EDITAL DE PREGÃO ELETRÔNICO N.º 03/2014

PROCESSO N.º 8518394-63.2013.8.06.0000

PREZADOS SENHORES,

O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, por intermédio do(a) Pregoeiro(a) e dos membros da equipe de apoio designadas pela portaria de n.º 172/2014, publicado no DJE, em 03/02/2014, com sede na Av. Gen. Afonso Albuquerque Lima s/n, - Cambeba, CEP – 60822-325, torna público para conhecimento de todos os interessados, que, no dia e hora abaixo indicados, será realizada licitação na modalidade Pregão Eletrônico, do tipo **MENOR PREÇO GLOBAL POR LOTE**, que será regido pela Lei Federal Nº 10.520, de 17/07/2002, com aplicação subsidiária da Lei Federal N.º 8.666/93 e suas alterações, pelas Resoluções Nº 04 de 06/03/2008 e Nº 08 de 08/07/2009 do TJCE, além das demais disposições legais aplicáveis e do disposto no presente Edital, com intuito de atender as necessidades deste Tribunal.

OBJETO: Contratação de serviços especializados, sob demanda, de administração, gerenciamento, monitoramento, tratamento de resposta a incidentes de segurança e estruturação da segurança da informação do TJCE, com o fornecimento de software da GRC – Governança, Riscos e Compliance, para automatizar a Gestão de Segurança da Informação, incluindo levantamentos, inventários, diagnósticos, análises, avaliações, testes, e tratamento dos ativos, com a gestão da continuidade de negócios e elaboração dos planos de contingência, com divulgação, planejamento, treinamento, elaboração e revisão dos normativos para sua implementação, para atender as necessidades do Poder Judiciário do Estado do Ceará, em conformidade com o disposto neste edital e seus anexos.

RECEBIMENTO DAS PROPOSTAS ATÉ: 24/02/2014 às 14:00 horas (Horário de Brasília).

ABERTURA DAS PROPOSTAS: 24/02/2014 às 14:00 horas (Horário de Brasília).

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: 25/02/2014 às 14:00 horas (Horário de Brasília).

FORMALIZAÇÃO DE CONSULTAS: Observando o prazo legal, o fornecedor poderá formular consultas por fone/fax ou e-mail, conforme números e endereço abaixo, informando o número da licitação.

Fone/Fax: (85) 3207-7098/3207-7100

E-mail: cpl.tjce@tjce.jus.br

REFERÊNCIA DE TEMPO: Para todas as referências de tempo será observado o horário de Brasília/DF.

Constituem Anexos deste Edital e dele fazem parte:
ANEXO 01 – TERMO DE REFERÊNCIA
ANEXO 02 – ORÇAMENTO DETALHADO
ANEXO 03 – MODELO DE APRESENTAÇÃO DA PROPOSTA
ANEXO 04 – TERMO DE RECEBIMENTO PROVISÓRIO
ANEXO 05 – TERMO DE RECEBIMENTO DEFINITIVO
ANEXO 06 – MODELO DE ORDEM DE SERVIÇO
ANEXO 07 – PLANO DE MUDANÇA E LIBERAÇÃO - PML
ANEXO 08 – TERMO DE CIÊNCIA
ANEXO 09 – TERMO DE COMPROMISSO
ANEXO 10 – RECIBO DE RETIRADA DO EDITAL PELA INTERNET
ANEXO 11 – MODELO DE DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE
ANEXO 12 – MODELO DE DECLARAÇÃO DE QUE NÃO EMPREGA MENOR

ANEXO 13 – MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATOS IMPEDITIVOS SUPERVENIENTE À HABILITAÇÃO
ANEXO 14 - MODELO DE DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA
ANEXO 15 - MINUTA DO CONTRATO (LOTE 1)
ANEXO 16 - MINUTA DO CONTRATO (LOTE 2)

1. DISPOSIÇÕES PRELIMINARES

1.1. O Pregão Eletrônico será realizado em sessão pública, por meio da *INTERNET*, mediante condições de segurança - criptografia e autenticação - em todas as suas fases;
1.2. Os trabalhos serão conduzidos por funcionário do Tribunal de Justiça do Estado do Ceará, denominado(a) pregoeiro(a), mediante a inserção e monitoramento de dados gerados ou transferidos para o aplicativo "Licitações" constante da página eletrônica do Banco do Brasil S.A, no endereço eletrônico www.licitacoes-e.com.br.
1.3. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subseqüente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação do Pregoeiro em contrário, no site: www.licitacoes-e.com.br, campo "Consultar Mensagens" referente ao presente pregão eletrônico, sendo de responsabilidade do(s) licitante(s): verificar a(s) referida(s) mensagem(ns) e, ainda, os respectivos ônus por não consultá-la(s).

2. RECEBIMENTO E ABERTURA DAS PROPOSTAS E DATA DO PREGÃO

2.1. O fornecedor deverá observar as datas e os horários limites previstos para a abertura da proposta, atentando também para a data e horário para início da disputa.

3. CONDIÇÕES PARA PARTICIPAÇÃO

3.1. Poderão participar desta Licitação, toda e qualquer firma individual ou sociedade, regularmente estabelecida no País, que seja especializada e credenciada no objeto desta licitação e que satisfaça todas as exigências, especificações e normas contidas neste Edital e seus Anexos;
3.2. É vedada a participação de pessoa física ou jurídica nos seguintes casos:
a) Sob a forma de consórcio, qualquer que seja a sua constituição;
b) Que estejam em estado de insolvência civil, sob processo de falência, concordata, recuperação judicial ou extrajudicial, dissolução, fusão, cisão, incorporação e liquidação;
c) Que estejam cumprindo penas de suspensão temporária de participar de licitações e impedimento de contratar com a Administração;
d) Que tenham sido declaradas inidôneas pela Administração Pública;
e) Empresas estrangeiras que não tenham autorização para funcionar no País;
f) Servidor público ou empresas cujos dirigentes, gerentes, sócios ou componentes de seu quadro técnico sejam funcionários ou empregados públicos da Administração Pública Estadual Direta ou Indireta.
g) Que seja autor do projeto básico ou executivo;
3.3. O licitante deverá manifestar, **em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação,** e que sua proposta está em conformidade com as exigências do instrumento convocatório, nos termos do art. 20, inciso XIII da Resolução nº 04 de 06/03/2008 do TJCE;
3.4. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas neste edital.

4. REGULAMENTO OPERACIONAL DO CERTAME

4.1. O certame será conduzido pelo(a) pregoeiro(a), que terá, em especial, as seguintes atribuições:
a) coordenar o processo licitatório;
b) conduzir os trabalhos da equipe de apoio;
c) receber, examinar e decidir as impugnações e consultas ao edital, apoiado pela área responsável pela elaboração do Termo de Referência;
d) receber as propostas de preços;
e) abrir e examinar as propostas de preços e classificar os proponentes;
f) verificar a conformidade das propostas com os requisitos estabelecidos no instrumento convocatório;
g) desclassificar propostas indicando os motivos;
h) conduzir os procedimentos relativos aos lances e à escolha da proposta do lance de menor preço;
i) receber a documentação de habilitação;
j) verificar e julgar as condições de habilitação;
k) declarar o vencedor;
l) receber, examinar e decidir sobre a pertinência dos recursos, encaminhando-os à autoridade superior,

quando mantiver sua decisão;
m) elaborar e publicar a ata da sessão;
n) encaminhar o processo devidamente instruído à autoridade superior e propor a homologação;
o) abrir processo administrativo para apuração de irregularidades visando à aplicação de penalidades previstas na legislação.

CREDENCIAMENTO NO APLICATIVO LICITAÇÕES

4.2. Para acesso ao sistema eletrônico, os interessados em participar do Pregão deverão dispor de chave de identificação e senha pessoal (intransferíveis), obtidas junto às Agências do Banco do Brasil S.A., sediadas no País;
4.3. As pessoas jurídicas ou firmas individuais deverão credenciar representantes, mediante a apresentação de procuração por instrumento público ou particular, com firma reconhecida, atribuindo poderes para formular lances de preços e praticar todos os demais atos e operações no *licitações-e*;
4.4. Em sendo sócio, proprietário, dirigente (ou assemelhado) da empresa proponente, deverá apresentar cópia do respectivo Estatuto ou Contrato Social, no qual estejam expressos seus poderes para exercerem direitos e assumir obrigações em decorrência de tal investidura;
4.5. A chave de identificação e a senha terão validade de 01 (um) ano e poderão ser utilizadas em qualquer pregão eletrônico, salvo quando canceladas por solicitação do credenciado ou por iniciativa do Banco, devidamente justificado;
4.6. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao Banco do Brasil S.A. a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros;
4.7. O credenciamento do fornecedor e de seu representante legal junto ao sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico.

PARTICIPAÇÃO

4.8. A participação no Pregão Eletrônico se dará por meio da digitação da senha pessoal e intransferível do representante credenciado e subsequente encaminhamento da proposta de preços, exclusivamente por meio do sistema eletrônico, observados data e horário e limite estabelecidos.
Obs.: a informação dos dados para acesso deve ser feita na página inicial do site *www.licitacoes-e.com.br*, opção "Acesso Identificado";
4.9. O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. O fornecedor será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances;
4.10. O licitante que desejar utilizar-se das prerrogativas da **Lei Complementar 123, de 14/12/2006**, deverá declarar no campo específico do sistema;
4.11. No preenchimento da proposta eletrônica o licitante deverá informar o valor total de sua proposta, conforme instruções contidas no Anexo 02 deste Edital e poderá mencionar, no campo "INFORMAÇÕES ADICIONAIS", as principais características dos serviços ofertados, **VEDADA A IDENTIFICAÇÃO DO LICITANTE, SOB PENA DE DESCLASSIFICAÇÃO**;
4.12. A validade da proposta será de no mínimo **60(sessenta) dias**, contados a partir da data da sessão pública do Pregão;
4.13. Caberá ao fornecedor acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

ABERTURA DAS PROPOSTAS E FORMULAÇÃO DOS LANCES

4.14. A partir do horário previsto no sistema, terá início a sessão pública do pregão eletrônico, com a divulgação das propostas de preços recebidas, passando o(a) pregoeiro(a) a avaliar a aceitabilidade das propostas. Caso ocorra alguma desclassificação, esta deverá ser fundamentada e registrada no sistema;
4.15. Os preços deverão ser expressos em reais, com até 2 (duas) casas decimais em seus valores globais;
4.16. O sistema ordenará automaticamente as propostas classificadas pelo(a) pregoeiro(a), e somente estas participarão da etapa de lances;
4.17. Aberta a etapa competitiva, na data e horário determinados neste Edital, os representantes dos fornecedores deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor;
4.18. Para efeito de lances, será considerado o valor global:
4.18.1. Os licitantes poderão ofertar lances sucessivos, desde que inferiores ao seu último lance registrado no sistema, ainda que este seja maior que o menor lance já ofertado por outro licitante.
4.18.2. Em caso de dois ou mais lances de igual valor, prevalece aquele que for recebido e registrado em primeiro lugar.
4.19. Durante o transcurso da sessão pública, os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais participantes;

4.20. No caso de desconexão com o(a) pregoeiro(a), no decorrer da etapa competitiva do Pregão Eletrônico, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o(a) pregoeiro(a), quando possível, sua atuação no certame, sem prejuízos dos atos realizados;
4.21. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão será suspensa, sendo reiniciada somente após comunicação expressa do(a) pregoeiro(a) aos participantes, através de mensagem no sistema, divulgando data e hora da reabertura da sessão. Caberá ao licitante a responsabilidade por qualquer ônus decorrente da perda de negócio diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão;
4.22. A etapa inicial de lances da sessão pública será encerrada pelo(a) pregoeiro(a), seguida do tempo randômico, que poderá ser de 1 (um) segundo a 30 (trinta) minutos, aleatoriamente determinado pelo sistema eletrônico;

4.22.1. Face imprevisão do tempo extra, as Empresas participantes deverão estimar o seu valor mínimo de lance a ser ofertado, evitando assim, cálculos de última hora, que poderá resultar em uma disputa frustrada por falta de tempo hábil.

4.23. Transcorrido o tempo randômico, o sistema detectará a existência de situação de empate ficto. Em cumprimento ao que determina a Lei Complementar nº 123/2006, a microempresa e a empresa de pequeno porte que ofertou lance de até 5% (cinco por cento) superior ao menor preço da arrematante que não se enquadre nessa situação de empate, será convocada pelo(a) pregoeiro(a), na sala de disputa, para, no prazo de 5 (cinco) minutos, utilizando-se do direito de preferência, ofertar novo lance inferior ao melhor lance registrado, sob pena de preclusão.

4.23.1. Os procedimentos descritos no subitem 4.23 somente serão aplicados se a melhor oferta inicial (menor lance ou proposta de menor valor) não tiver sido apresentada por microempresa ou empresa de pequeno porte;

4.23.2. Todos esses procedimentos acontecerão na sala de disputa, estando essas informações disponíveis para os demais participantes do pregão e também para toda a sociedade;

4.24. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa e lances ou, quando for o caso, após negociação e decisão pelo(a) pregoeiro(a) acerca da aceitação do lance de menor valor;
4.25. O(a) pregoeiro(a) poderá negociar exclusivamente pelo sistema, em campo próprio, a fim de obter melhor preço, encaminhando, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado lance mais vantajoso, para que seja obtida a melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no edital;
4.26. Encerrada a etapa de lances da sessão pública, o(a) pregoeiro(a) verificará também, o cumprimento às demais exigências para habilitação contidas neste Edital;
4.27. Se a proposta ou o lance de menor valor não for aceitável, ou se o fornecedor desatender às exigências habilitatórias, o(a) pregoeiro(a) examinará a proposta ou o lance subsequente, verificando a sua compatibilidade e a habilitação do participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda o Edital. Também nessa etapa o(a) pregoeiro(a) poderá negociar com o participante para que seja obtido preço melhor;
4.28. Caso não sejam apresentados lances, será verificada a conformidade entre a proposta de menor preço e valor estimado para a contratação, inclusive quanto aos preços unitários;
4.29. Constatando o atendimento das exigências fixadas no Edital, o objeto será adjudicado ao autor da proposta ou lance de menor preço;
4.30. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante toda a sessão pública do pregão e etapas posteriores, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

5. PROPOSTA E FORNECIMENTO

5.1. A Proposta de Preços da Empresa vencedora deverá ser entregue na Comissão Permanente de Licitação do TJCE, **no prazo máximo de 2 (dois) dias úteis**, a contar do encerramento da etapa de lances da sessão pública, com os preços ajustados ao menor lance, em papel timbrado da empresa, folhas originais rubricadas e a última assinada pelo Representante Legal da Empresa, em linguagem clara e concisa, sem emendas, rasuras ou entrelinhas, contendo Razão Social, CNPJ, CGF, endereço e com especificação detalhada dos serviços a serem prestados, etc.;

5.1.1. O não cumprimento da entrega da documentação, dentro dos prazos estabelecidos neste Edital, acarretará desclassificação/inabilitação, bem como poderá acarretar a aplicação das sanções estabelecidas no art. 7º, da Lei Federal nº 10.520/02, e no art. 31, da Resolução nº 04/08, sendo convocado o licitante subsequente, e assim sucessivamente, observada a ordem de classificação.

5.1.2. Caso o arrematante venha a ser desclassificado ou inabilitado, o(a) pregoeiro(a) convocará os demais participantes, seguindo a ordem de classificação, devendo suas propostas de preços serem entregues **no prazo máximo de 2 (dois) dias úteis**, contados da sua convocação realizada por meio do sistema de licitações.

5.2. A proposta deverá explicitar:

5.2.1. O prazo de validade que não poderá ser inferior a **60(sessenta)** dias, contados a partir da data da sua emissão, de acordo com o previsto no art. 6° da Lei Federal n° 10.520/02, razão pela qual a não manutenção das propostas no decorrer de seu prazo de validade poderá ensejar as sanções previstas no art. 81 da Lei n° 8.666/93 e no art. 31, inciso II, alínea "c", da Resolução n° 04/2008 do TJCE;

5.2.2. Valores unitários por item e valor total, em moeda corrente nacional, com até 02(duas) casas decimais, conforme Anexo 02 do Edital, devendo o valor total da proposta ser escrito em numeral e por extenso;

5.2.3. Demais condições da proposta de preço, conforme itens 20.1 – Lote 1 e 18.1 – Lote 2 do Anexo 01 – Termo de Referência deste Edital.

5.3. Ocorrendo discordância entre os valores numéricos e por extenso prevalecerão estes últimos.

5.4. **Os critérios para prestação dos serviços estão estabelecidos no Lote 1 - item 4 e Lote 2 - item 2, do Anexo 01 (Termo de Referência) deste Edital.**

6. CRITÉRIOS DE JULGAMENTO

6.1. Para julgamento será adotado o critério de **MENOR PREÇO GLOBAL POR LOTE**, observados os prazos para fornecimento, as especificações técnicas, parâmetros mínimos de desempenho e de qualidade e demais condições definidas neste Edital;

6.1.1. A proposta final para o lote não poderá conter item com valor unitário superior ao estimado pela Administração, descritos no Anexo 02, sob pena de desclassificação, independente do valor total do lote.

6.2. Após a apresentação da proposta não caberá desistência;

6.3. Se a proposta de menor preço não for aceitável, ou ainda, se o licitante desatender às exigências habilitatórias, o(a) pregoeiro(a) examinará a proposta subsequente, verificando sua compatibilidade e a habilitação do participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda a este edital;

6.4. O licitante remanescente que esteja enquadrado no percentual estabelecido no art. 44, § 2º, da Lei Complementar nº 123/2006, no dia e hora designados pelo(a) pregoeiro(a), será convocado na ordem de classificação, no "*chat* de mensagem", para ofertar novo lance inferior ao melhor lance registrado no lote, para, no prazo de 5 (cinco) minutos, utilizar-se do direito de preferência;

6.5. Serão desclassificadas as propostas que conflitem com as normas deste Edital ou da Legislação em vigor;

6.6. Serão rejeitadas as propostas que:

6.6.1. Sejam incompletas, isto é, não contenham informação(ões) suficiente(s) que permita(m) a perfeita identificação do serviço licitado;

6.6.2. Contiverem qualquer limitação ou condição substancialmente contrastante com o presente Edital, ou seja, manifestamente inexequíveis, por decisão do(a) PREGOEIRO(A);

6.6.3. Contiverem preços superiores aos praticados no mercado, ou comprovadamente inexeqüíveis;

6.7. A desclassificação será sempre fundamentada e registrada no sistema;

6.8. Da sessão, o sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

6.9. **De conformidade com parecer da CPL, não constituirá causa de desclassificação do(a) proponente a irregularidade formal que não afete o conteúdo ou a idoneidade da proposta e/ou documentação.**

7. HABILITAÇÃO

7.1. Efetuados os procedimentos previstos no item 4 deste Edital, o licitante detentor da proposta ou do lance de menor valor, deverá entregar, no **prazo máximo de 2 (dois) dias úteis**, contados do encerramento da etapa de lances da sessão pública, a documentação de habilitação prevista abaixo, para o Tribunal de Justiça do Estado do Ceará, Comissão Permanente de Licitação, na Av. Gen. Afonso Albuquerque Lima, s/n, 2º andar - Cambeba, Cep – 60822-325;

7.1.1. O não cumprimento da entrega da documentação dentro do prazo estabelecido acarretará a inabilitação da licitante, bem como poderá acarretar a aplicação das sanções estabelecidas no art. 7º, da Lei Federal nº 10.520/2002 e no art. 31, da Resolução nº 04/2008, sendo convocado o licitante subsequente, e assim sucessivamente, observada a ordem de classificação, devendo suas documentações de habilitação serem entregues **no prazo máximo de 2(dois) dias úteis**, contados das suas convocações realizadas por meio do sistema de licitações.

7.2. Os licitantes deverão apresentar os seguintes documentos de habilitação para participar do presente certame:

7.2.1. No caso de licitante CADASTRADO, o Certificado de Registro Cadastral (CRC) emitido pela Secretaria do Planejamento e Gestão (SEPLAG), do Estado do Ceará, compatível com o ramo do objeto licitado.

7.2.1.1. A Comissão Permanente de Licitação do TJCE verificará eletronicamente a situação do licitante no Certificado de Registro Cadastral. Caso o mesmo esteja com algum documento vencido,

deverá apresentá-lo juntamente com os documentos de habilitação, sob pena de inabilitação, salvo os documentos de Regularidades Fiscal e Trabalhista acessíveis para consultas em *sítios* oficiais que poderão ser consultados pelo(a) pregoeiro(a).

7.2.2. O licitante NÃO CADASTRADO no CRC junto à SEPLAG/CE deverá apresentar os documentos relacionados na opção "Informações sobre Cadastramento de Fornecedores" disponíveis no *sítio:* **www.portalcompras.ce.gov.br**.

7.2.3. Certidão Negativa de Falência ou Concordata ou, se for o caso, Certidão de Recuperação Judicial, expedida pelo Cartório Distribuidor da sede da pessoa jurídica;

7.2.4. Declaração do licitante, se couber, tratar-se de Microempresa ou empresa de pequeno porte, **conforme modelo no Anexo 11**.

7.2.5. Ato constitutivo, estatuto ou contrato social em vigor, caso o representante legal da empresa integre seu quadro societário;

7.2.6. Procuração, juntamente com o ato constitutivo, estatuto ou contrato social em vigor, no caso do representante legal da empresa ser procurador.

7.2.7. Declaração que não possui, em seu quadro funcional, menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, menores de 16 (dezesseis) anos em trabalho algum, salvo na condição de aprendiz a partir de 14 (quatorze) anos, **conforme ANEXO 12 do Edital**;

7.2.8. Declaração, sob pena de incidir nas punições cabíveis, relativamente aos documentos exigidos nesta licitação, caso exista após a data de sua emissão, algum **fato superveniente** que impeça sua habilitação, na forma do § 2º, Art. 32, da Lei n.º 8.666/93, **conforme ANEXO 13 do Edital**;

7.2.9. Declaração de Elaboração Independente de Proposta, conforme modelo **constante no Anexo 14 do Edital**;

QUALIFICAÇÃO TÉCNICA

7.3. O licitante deverá satisfazer às condições de qualificação técnica descritas no item 20.2 - Lote 01 e item 18.2 – Lote 2 do ANEXO 01 (Termo de Referência) do Edital.

VISITA TÉCNICA

7.4. A vistoria técnica se dará conforme o item 19 – Lote 1 e item 17 – Lote 2 do ANEXO 01 (Termo de Referência) do Edital.

7.5. Os documentos de habilitação deverão ser apresentados da seguinte forma:

7.5.1. Obrigatoriamente, da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos tanto para matriz como para todas as filiais. A contratação será celebrada com a sede que apresentou a documentação.

7.5.2. Se apresentados em qualquer processo de fotocópia, deverão ser, obrigatoriamente, autenticados em Cartório oficial, sob pena de não o fazendo, serem consideradas inabilitadas no presente processo licitatório, conforme Provimento n.º 006/97 do Tribunal de Justiça do Estado do Ceará.

7.5.3. Os documentos obtidos através de *sítios* oficiais, que estejam condicionados à aceitação via internet, terão sua autenticidade verificada pelo(a) pregoeiro(a). Os documentos de habilitação disponibilizados pelos Órgãos competentes, emitidos por meio eletrônico através da rede mundial de computadores (internet), para fins de julgamento, serão considerados originais, não necessitando de autenticação notarial. Outrossim, se os mesmos forem apresentados através de cópias xerográficas, estas deverão obrigatoriamente ser autenticadas em cartório;

7.5.4. Caso haja documentos redigidos em idioma estrangeiro, os mesmos somente serão considerados se acompanhados da versão em português, firmada por tradutor juramentado.

7.5.5. Dentro do prazo de validade. Na hipótese de no documento não constar expressamente o prazo de validade, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre sua validade. Na ausência de tal declaração ou regulamentação, o documento será considerado válido pelo prazo de 30 (trinta) dias, contados a partir da data de sua emissão.

7.6. O(A) Pregoeiro(a) poderá também, solicitar originais de documentos já autenticados para fins de verificação, sendo a empresa obrigada a apresentá-los no prazo **de 48(quarenta e oito) horas**, contados a partir da solicitação, sob pena de não o fazendo, ser inabilitada;

7.7. Todas as certidões negativas apresentadas deverão comprovar a quitação com os tributos pertinentes, as que se encontram positivas, só serão acatadas se tiverem o mesmo valor das negativas;

7.8. Em se tratando de microempresa ou empresa de pequeno porte, esta deverá apresentar todos os documentos exigidos para efeito de comprovação da regularidade fiscal, mesmo que estes apresentem alguma restrição, conforme determina o art. 43, da Lei Complementar 123, de 14/12/2006;

7.8.1. Havendo alguma restrição na comprovação da regularidade fiscal da microempresa ou empresa de pequeno porte, será assegurado o prazo de 2(dois) dias úteis, contados da data em que o proponente foi declarado vencedor do certame, prorrogável por igual período, a critério da Administração, para a regularização da situação que deu causa à restrição;

7.8.2. A não regularização no prazo previsto no subitem anterior, implicará a decadência do direito à contratação, sem prejuízo das sanções previstas neste Edital;

7.9. Constatando o atendimento das exigências previstas no Edital, o licitante será declarado vencedor,

sendo-lhe adjudicado o objeto da licitação pelo(a) próprio(a) pregoeiro(a), na hipótese de inexistência de recursos administrativos, ou pela Autoridade Superior, na hipótese de existência de recursos administrativos;
7.10. Se o licitante desatender às exigências previstas neste Item 7, o(a) pregoeiro(a) examinará a oferta subsequente na ordem de classificação, verificando a sua aceitabilidade e procedendo a sua habilitação, repetindo esse procedimento sucessivamente, se for necessário, até a apuração de uma proposta que atenda ao Edital, sendo o respectivo licitante declarado vencedor.

8. PEDIDOS DE ESCLARECIMENTOS E IMPUGNAÇÕES AO EDITAL

8.1. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao(à) pregoeiro(a), até 3 (três) dias úteis anteriores à data fixada para abertura das propostas, informando o número deste pregão no sistema do Banco do Brasil e o órgão interessado.
8.2. Até 2 (dois) dias úteis anteriores a data fixada para abertura das propostas, qualquer pessoa poderá impugnar o presente edital, mediante petição por escrito, protocolizada no Tribunal de Justiça do Estado do Ceará, no endereço constante no preâmbulo deste Edital.

8.2.1. Não serão conhecidas as impugnações apresentadas fora do prazo legal e/ou subscritas por representante não habilitado legalmente.

8.3. Caberá ao(à) pregoeiro(a), auxiliado(a) pela área interessada, quando for o caso, decidir sobre a petição de impugnação no prazo de 24 (vinte e quatro) horas.
8.4. Acolhida a impugnação contra este edital, será designada nova data para a realização do certame, exceto se a alteração não afetar a formulação das propostas.

9. RECURSOS ADMINISTRATIVOS

9.1. Declarado o vencedor, o proponente que desejar recorrer contra decisões do(a) Pregoeiro(a), poderá fazê-lo de imediato e motivadamente, no prazo de até **24(vinte e quatro) horas**, manifestando sua intenção com o registro da síntese das suas razões, exclusivamente no âmbito do sistema eletrônico, sendo-lhe concedido o prazo de **3 (três) dias** para apresentar por escrito as razões do recurso, conforme o artigo 4º, inciso XVIII da Lei Federal nº 10.520 de 17/07/2002. Os demais licitantes ficam, desde logo, intimados a apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo do recorrente;
9.2. A falta de manifestação imediata e motivada importará a decadência do direito de recurso;
9.3. Fica assegurada aos licitantes vista imediata dos autos do Pregão, com a finalidade de subsidiar a preparação de recursos e de contrarrazões. Os referidos Autos estarão disponíveis na sala da Comissão de Licitação do TJCE;
9.4. Não serão conhecidos os recursos intempestivos, nem acolhidas razões ou contrarrazões enviadas via fax símile, e-mail e/ou telegrama;
9.5. Não serão conhecidos os recursos apresentados fora do prazo legal ou subscritos por representante não habilitado legalmente ou não identificado no processo para responder pelo proponente;
9.6. Não será concedido prazo para recursos sobre assuntos meramente protelatórios ou quando não justificada a intenção de interpor o recurso pelo proponente;
9.7. O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento;
9.8. A decisão em grau de recurso será definitiva e dela dar-se-á conhecimento aos interessados, por meio de comunicação via fac-símile/e-mail.

10. SANÇÕES ADMINISTRATIVAS

10.1. Nos termos do art. 7º, da Lei Federal nº 10.520/2002, os proponentes que, convocados dentro do prazo de validade de suas propostas, não celebrarem o contrato, deixarem de entregar ou apresentarem documentação falsa exigida neste edital, ensejarem o retardamento da execução do seu objeto, não mantiverem a proposta, falharem ou fraudarem na execução do contrato, comportarem-se de modo inidôneo ou cometerem fraude fiscal, ficarão impedidos de licitar e contratar com o Estado do Ceará e serão descredenciados do Cadastro Geral de Fornecedores do Estado do Ceará da SEPLAG/CE pelo prazo de até 05 (cinco) anos, sem prejuízo das demais sanções previstas neste edital e das demais cominações legais.
10.2. A LICITANTE VENCEDORA, uma vez contratada, sujeitar-se-á, em caso de inadimplemento de suas obrigações, definidas neste Instrumento ou em outros que o complementem, **às sanções e penalidades administrativas, conforme previsão nos itens 17 – Lote 1 e 15 – Lote 2, Anexo 01 – Termo de Referência, deste Edital**, sem prejuízo das sanções legais, descritas nos Arts. 86 a 88 da Lei 8.666/93 e responsabilidades civil e criminal;
10.3. As multas, a que se referem o item anterior, não impedem que a Administração rescinda unilateralmente o contrato e aplique outras sanções, tudo conforme previsão na Lei nº 8.666/93 e a Lei nº 10.520/2002;
10.4. O TJCE poderá deduzir o valor da multa aplicada da garantia contratual apresentada e, caso não seja suficiente, descontá-la dos pagamentos eventualmente devidos à CONTRATADA, os valores correspondentes à aplicação contratual ou, se for o caso, efetuar cobrança judicial;
10.5. Nenhuma sanção será aplicada sem o devido processo administrativo, oportunizando-se defesa prévia

ao interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vistas ao processo.

11. PAGAMENTO

11.1. Os prazos e condições de pagamento estão descritos nos itens 11 – Lote 1 e 9 – Lote 2 do Anexo 01 – Termo de Referência deste Edital.

12. REAJUSTAMENTO E RECURSOS FINANCEIROS

12.1. Reajustamento: Os preços oferecidos serão fixos e irreajustáveis pelo período mínimo de 01(um) ano;
12.2. Após 12 meses da data de apresentação da proposta e o contrato sendo prorrogado, a CONTRATADA, mediante justificativa, poderá solicitar reajuste com base na variação do IPCA.
12.3. Ficará a critério do TJCE concordar ou não, integral ou parcialmente, com o reajuste de preços propostos.
12.4. Os recursos financeiros correrão por conta do Fundo Especial de Reaparelhamento e Modernização Judiciária – FERMOJU, tendo como Fonte dos recursos – Recursos Diretamente Arrecadados. Na seguinte dotação orçamentária:

04200001.02.061.500.21360.01.33903900.70.1.20

13. DOS PRAZOS

13.1. O prazo de vigência do contrato para o Lote 1 será de 12 (doze) meses, contados a partir de sua assinatura, podendo ser prorrogado, conforme descrito no item **18.1 – Lote 1 do ANEXO 01 – TERMO DE REFERÊNCIA**.
13.2. O prazo de vigência do contrato para o Lote 2 será de 24 (vinte e quatro) meses, contados a partir de sua assinatura, conforme descrito no item **16.1 – Lote 2 do ANEXO 01 – TERMO DE REFERÊNCIA**.

14. DO CONTRATO

14.1. A contratação se efetivará através de contrato - minuta constante dos Anexos 15 e 16 deste Edital, e deverá ser assinado pela PROPONENTE VENCEDORA no prazo de 05 (cinco) dias úteis, contados da data da convocação expedida pelo TJCE para este fim;
14.2. Tal Contrato terá suas cláusulas e condições reguladas pela Lei 8.666/93 e suas atualizações;
14.3. Farão parte do contrato todos os elementos apresentados pelo licitante vencedor, que tenham servido de base para o julgamento, bem como as condições estabelecidas neste Pregão e em seus anexos, independentemente de transcrição;
14.4. Caso a proponente, declarada vencedora, não queira ou não possa assinar o contrato respectivo, dentro do prazo de validade da proposta, poderá o TJ-CE, sem prejuízo de aplicação de penalidades à desistente, optar pela contratação das proponentes remanescentes, na ordem de classificação, se, alternativamente, o TJ-CE não preferir revogar a presente licitação.

15. DAS OBRIGAÇÕES DO CONTRATANTE

15.1. As obrigações do Contratante estão estabelecidas nos itens 6 – Lote 1 e 4 – Lote 2 do Termo de Referência, constante no Anexo 01 deste Edital.

16. DAS OBRIGAÇÕES DA CONTRATADA

16.1. As obrigações da Contratada estão estabelecidas nos itens 7 – Lote 1 e 5 – Lote 2 do Termo de Referência, constante no Anexo 01 deste Edital.

17. DA GARANTIA CONTRATUAL

17.1. Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive pagamento de multas eventualmente aplicadas, a licitante prestará garantia no percentual de 5% (cinco por cento) do valor total do contrato, podendo a CONTRATADA optar por qualquer das modalidades previstas no art. 56 da Lei 8.666/93, a saber:

17.1.1. Caução em dinheiro ou títulos da dívida pública, cuja exigibilidade não seja contestada pelo TJCE;
17.1.2. Quando se tratar de caução em dinheiro, deverá ser recolhido na Secretaria de Finanças do TJCE;
17.1.3. Seguro garantia;
17.1.4. Fiança bancária.

17.2. Em se tratando de fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil;
17.3. Se o valor da garantia for utilizado em pagamento de qualquer obrigação, a CONTRATADA deverá re-integralizar o seu valor, no prazo não superior a 10 (dez) dias corridos, contados da data em que for notificada;

17.4. A não apresentação da garantia até a assinatura contratual significará recusa à assinatura do contrato, ensejando aplicação das sanções previstas;
17.5. No caso de rescisão do contrato, a garantia se presta a cobrir prejuízos comprovados;
17.6. A garantia ofertada deverá cobrir multas aplicadas, bem como obrigações trabalhistas e previdenciárias, não deverá ser proporcional ao tempo de vigência do contrato, garantindo sua totalidade durante todo o período de vigência. Não será aceita cláusula que preveja a realização do contrato por terceiros, bem como cláusula que preveja a subrogação da seguradora nos créditos da segurada. Deve, também, ser concedido pela seguradora, prazo mínimo de 30(trinta) dias para comunicação pelo TJCE das falhas cometidas pela segurada.

20. DISPOSIÇÕES FINAIS

18.1. A presente licitação não importa necessariamente em contratação, podendo o Tribunal de Justiça do Estado do Ceará revogá-la, no todo ou em parte, por razões de interesse público, derivada(s) de fato(s) superveniente(s) comprovado(s) ou anulá-la por ilegalidade, de ofício ou por provocação mediante ato escrito e fundamentado disponibilizado no sistema para conhecimento dos participantes da licitação. O Tribunal de Justiça do Estado do Ceará poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas ou para sua abertura;
18.2. O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato ou do pedido de compra, sem prejuízo das demais sanções cabíveis;
18.3. É facultado à(ao) Pregoeira(o) ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo licitatório, vedada a inclusão posterior de documentos que deveriam constar obrigatoriamente na proposta e na documentação de habilitação não previstos neste Edital serão decididos pela(o) Pregoeira(o);
18.4. Os proponentes intimados para prestar quaisquer esclarecimentos adicionais deverão fazê-lo no prazo determinado pela(o) Pregoeira(o), sob pena de desclassificação/inabilitação;
18.5. O desatendimento de exigências formais não essenciais não importará no afastamento do proponente, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta;
18.6. As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação;
18.7. As decisões referentes a este processo licitatório poderão ser comunicadas aos proponentes por qualquer meio de comunicação que comprove o recebimento ou, ainda, mediante publicação no Diário da Justiça do Estado do Ceará;
18.8. Na contagem dos prazos estabelecidos neste edital excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. Os prazos estabelecidos neste edital se iniciam e se vencem somente em dia de expediente no Tribunal de Justiça do Estado do Ceará;
18.9. **A participação do licitante nesta licitação implica em aceitação de todos os termos deste Edital, e a inobservância de qualquer dos itens descritos nele é de total responsabilidade dos participantes;**
18.10. Qualquer informação fornecida por telefone, não terá caráter formal;
18.11. O foro designado para julgamento de quaisquer questões judiciais resultantes deste Edital será o de Fortaleza, Capital do Estado do Ceará, considerado aquele a que está vinculada(o) a(o) Pregoeira(o).
18.12. O(A) Pregoeiro(a) atenderá aos interessados no horário de 08:00 às 18:00 horas, de segunda a sexta-feira, exceto feriados, na Sala da Comissão Permanente de Licitação, 2º Andar, do Tribunal de Justiça do Estado do Ceará, para melhores esclarecimentos;
18.13. É vedado ao servidor dos órgãos e entidades da Administração Pública Estadual, inclusive Fundações instituídas e/ou mantidas pelo Poder Público, participar como licitante, direta ou indiretamente, por si ou por interposta pessoa, dos procedimentos licitatórios disciplinados pela Lei Nº 10.880, de 29/12/83;
18.14. De acordo com a resolução nº 7, de 18 de outubro de 2005, do CNJ, não contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao respectivo Tribunal (CONTRATANTE);
18.15. A documentação apresentada para fins de habilitação da Empresa vencedora, fará parte dos autos da licitação e não será devolvida ao proponente.
18.16. Os casos omissos e não previstos neste Edital serão resolvidos pelo(a) Pregoeiro(a) do TJCE, nos termos da Legislação pertinente.

Fortaleza-CE, aos 07 de fevereiro de 2014.

Georgeanne Lima Gomes Botelho
PRESIDENTE DA COMISSÃO PERMANENTE DE LICITAÇÃO

ANEXO 01

TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

Contratação de serviços especializados, sob demanda, de administração, gerenciamento, monitoramento, tratamento de resposta a incidentes de segurança e estruturação da segurança da informação do TJCE, com o fornecimento de software de GRC – Governança, Riscos e Compliance, para automatizar a Gestão de Segurança da Informação, incluindo levantamentos, inventários, diagnósticos, análises, avaliações, testes, e tratamento dos ativos, com a gestão da continuidade de negócios e elaboração dos planos de contingência, com divulgação, planejamento, treinamento, elaboração e revisão dos normativos para sua implementação, conforme detalhamento técnico e especificações constantes deste Termo de Referência.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Quantitativos

2.1.1. Os quantitativos especificados na tabela do **LOTE 01** foram baseados nas quantidades de soluções de segurança de tecnologia da informação atualmente em uso como também já previstos a serem adquiridas pelo TJCE. Os quantitativos também estão definidos no item **10** neste documento;

2.1.2. Os quantitativos especificados na tabela do **LOTE 02** foram baseados nas necessidades de prestação de serviços de gestão de segurança de tecnologia da informação do TJCE como também tendo como base pesquisa mercadológica de serviços prestados e praticados atualmente no mercado.

LOTE 01

ID	Demanda Prevista	Unidade de Medida	Quantitativo a ser Contratado
SERVIÇO DE ADMINISTRAÇÃO, GERENCIAMENTO E MONITORAMENTO DOS ATIVOS DE SEGURANÇA			
1	Gerenciamento de appliance Firewall/VPN no site principal do tipo CISCO ASA 5550	Unidade	03
2	Gerenciamento de appliance firewall/VPN nos sites remotos do tipo CISCO ASA 5505	Unidade	26
3	Gerenciamento de appliance firewall/VPN nos sites remotos do tipo a ser adquirido pelo TJCE	Unidade	190
4	Gerenciamento de appliance IPS no site principal do tipo CISCO IPS-4260	Unidade	02
5	Gerenciamento de appliance SIEM no site principal do tipo CISCO Mars	Unidade	01
SERVIÇO DE TRATAMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA			
6	Tratamento de Respostas a incidente - Firewall/VPN do tipo CISCO ASA 5550/5505	Solução	01
7	Tratamento de Respostas a incidente - IPS no site principal do tipo CISCO IPS-4260	Solução	01
8	Tratamento de Respostas a incidente - SIEM do tipo CISCO Mars	Solução	01

9	Tratamento de Respostas a incidente - Mail Security do tipo CISCO Ironport C160	Solução	01
10	Tratamento de Respostas a incidente - Web Security tipo McAfee Web Gateway	Solução	01
11	Tratamento de Respostas a incidente - EndPoint Security do tipo Kaspersky Security Center	Solução	01

LOTE 02

ID	Demanda Prevista	Unidade de Medida	Quantitativo a ser Contratado
FORNECIMENTO E IMPLANTAÇÃO DE FERRAMENTAS PARA AUTOMATIZAR A GESTÃO DA SEGURANÇA DA INFORMAÇÃO			
1	Software de gestão de segurança da informação	Unidade	01
2	Serviço de suporte, manutenção e atualização de software	Unidade	01
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO			
3	Metodologia de gestão de risco documentada	Unidade	01
4	Piloto para validação da metodologia de gestão de riscos	Unidade	01
5	PLANO DE TRABALHO	Unidade	01
6	RELATÓRIOS DE ACOMPANHAMENTO	Projeto	01
7	APRESENTAÇÃO INICIAL	Unidade	01
SERVIÇO DE ANÁLISE DE RISCOS E VULNERABILIDADES EM SEGURANÇA DA INFORMAÇÃO			
8	Relatório Análise do Faltante (Gap Analisys)	Unidade	01
9	Relatório de Inventário de Ativos de Informação	Unidade	01
10	Relatório Gerencial de Riscos	Unidade	01
11	Relatório de Ocorrência de Riscos Identificados e Recomendações	Unidade	01
12	Relatório de Mitigação de Riscos	Unidade	01
13	Plano de Tratamento de Riscos	Unidade	01
14	Plano de Tratamento de Riscos Anual	Unidade	01
15	Relatório Trimestral de Riscos dos Ativos	Unidade	04
16	Relatório Consolidado de Riscos	Unidade	01
17	PLANO DE TRABALHO	Unidade	01
18	RELATÓRIOS DE ACOMPANHAMENTO	Projeto	01
19	APRESENTAÇÃO INICIAL	Unidade	01
SERVIÇO DE TESTES DE INVASÃO INTERNOS E EXTERNOS			
20	PLANO DE TESTE DE INVASÃO	Unidade	01
21	RELATÓRIO DE DESCOBERTA DE TESTE DE INVASÃO	Unidade	01

22	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO	Unidade	01
23	RELATÓRIO DE RETORNO SOBRE INVESTIMENTO	Unidade	01
24	RELATÓRIO DA SEGURANÇA FÍSICA	Unidade	01
25	RELATÓRIO DA SEGURANÇA TÉCNICO ADMINISTRATIVA	Unidade	01
26	PLANO DE TESTE DE INVASÃO anual	Unidade	01
27	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO mensal	Unidade	12
28	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO trimestral	Unidade	04
29	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO semestral	Unidade	02
30	PLANO DE TRABALHO	Unidade	01
31	RELATÓRIOS DE ACOMPANHAMENTO	Projeto	01
32	APRESENTAÇÃO INICIAL	Unidade	01
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO			
33	Modelo de Gestão de Resposta a Incidentes	Unidade	01
34	Proposta de Implantação	Unidade	01
35	Documento com Missão da ETIR	Unidade	01
36	Documento de constituição da ETIR	Unidade	01
37	Documento com detalhamento de tipos de serviços, tarefas e ações da ETIR	Unidade	01
38	Política de classificação de incidentes computacionais	Unidade	01
39	Modelo de formulário para reporte de incidentes computacionais	Unidade	01
40	Proposta de utilização de ferramentas para limpeza completa de dados	Unidade	01
41	Procedimento de comunicação da ETIR do TJCE em caso de indícios de ilícitos criminais	Unidade	01
42	Proposta de treinamento	Unidade	01
43	Treinamento para os membros do ETIR	Turma	01
44	PLANO DE TRABALHO	Unidade	01
45	RELATÓRIOS DE ACOMPANHAMENTO	Projeto	01
46	APRESENTAÇÃO INICIAL	Unidade	01
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DO MODELO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO			
47	Relatório com análise da estruturação e atuação do Comitê	Unidade	01
48	Relatório de Propostas de Melhoria	Unidade	01
49	Definições de infraestrutura de Segurança da Informação	Unidade	01

50	Modelo de gestão documentado	Unidade	01
51	PLANO DE TRABALHO	Unidade	01
52	RELATÓRIOS DE ACOMPANHAMENTO	Projeto	01
53	APRESENTAÇÃO INICIAL	Unidade	01
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO			
54	Relatório com Análise das Normas vigentes	Unidade	01
55	Relatório de Propostas de Melhoria das Normas vigentes	Unidade	01
56	Documento de Política de Segurança da Informação, com o novo conjunto de normativos	Unidade	01
57	Documento para formalização e aprovação por parte da autoridade máxima responsável	Unidade	01
58	Dicionário dos termos técnicos utilizados nos documentos	Unidade	01
59	Sumário executivo para apresentação à alta Administração	Unidade	01
60	Guia de consulta rápida	Unidade	01
61	PLANO DE TRABALHO	Unidade	01
62	RELATÓRIOS DE ACOMPANHAMENTO	Projeto	01
63	APRESENTAÇÃO INICIAL	Unidade	01
SERVIÇO DE ELABORAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL			
64	Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE)	Unidade	01
65	RELATÓRIO INICIAL para o TJCE	Unidade	01
66	PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	Unidade	01
67	PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS	Unidade	01
68	PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA)	Unidade	01
69	PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	Unidade	01
70	PLANO DE RECUPERAÇÃO DE OPERAÇÕES	Unidade	01
71	PLANO DE TESTES E EXERCÍCIOS	Unidade	01
72	PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE	Unidade	01
73	PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL	Unidade	01
74	PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS	Unidade	01
75	Treinamento das equipes de recuperação de desastres	Turma	01
76	Relatórios de testes realizados	Unidade	01

77	Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE) - anual	Unidade	01
78	PLANO DE TRABALHO	Unidade	01
79	RELATÓRIOS DE ACOMPANHAMENTO	Projeto	01
80	APRESENTAÇÃO INICIAL	Unidade	01
SERVIÇO DE ELABORAÇÃO DO PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO			
81	Relatório técnico com as necessidades que a nova arquitetura de Segurança de TI do TJCE precisará satisfazer	Unidade	01
82	Documento com objetivos de evolução da rede corporativa do TJCE	Unidade	01
83	Documento com ajustes necessários no núcleo básico da arquitetura de segurança	Unidade	01
84	Relatório do Plano Diretor de Segurança da Informação	Unidade	01
85	Cronograma de Trabalho anexo ao relatório	Unidade	01
86	Relatório do Plano Diretor de Segurança da Informação – anual.	Unidade	01
87	PLANO DE TRABALHO	Unidade	01
88	RELATÓRIOS DE ACOMPANHAMENTO	Projeto	01
89	APRESENTAÇÃO INICIAL	Unidade	01
SERVIÇO DE DIVULGAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO			
90	Plano de Divulgação e Treinamento	Unidade	01
91	Palestras da Semana da Segurança da Informação	Projeto	01
92	Palestras do Seminário de Segurança da Informação	Projeto	01
93	Treinamentos do Corpo Técnico de TI da SETIN - Gestão de continuidade de negócios	Participantes	10
94	Treinamentos do Corpo Técnico de TI da SETIN – Sistemas de gestão de segurança da informação	Participantes	10
95	Treinamentos do Corpo Técnico de TI da SETIN - Gestão de riscos em TI	Participantes	10
96	Treinamentos do Corpo Técnico de TI da SETIN – Diretrizes para gestão da segurança da informação para organizações de telecomunicações	Participantes	10
97	Treinamento dos integrantes do Comitê de Segurança da Informação - Sistemas de gestão de segurança da informação	Turma	01
98	Workshop para a alta Administração do TJCE	Unidade	01
99	PLANO DE TRABALHO	Unidade	01
100	RELATÓRIOS DE ACOMPANHAMENTO	Projeto	01
101	APRESENTAÇÃO INICIAL	Unidade	01

2.2. Motivação

Conforme Lei n.º 8.666, de 21/06/93, art. 3º, caput, a licitação destina-se a garantir o princípio constitucional

da isonomia e a selecionar a proposta mais vantajosa para a Administração. Neste aspecto, o presente termo de referencia foi elaborado observando-se diversos aspectos;

A qualificação técnica da contratada em projetos aderentes aos listados no presente termo de referência, agregando conhecimento técnico especializado e experiência a execução dos serviços;

Qualificação da equipe técnica a participar da elaboração dos produtos aqui especificados;

Ateste de fornecimento e instalação de solução, aderente ao especificado neste termo de referência, que demonstre o pleno funcionamento da solução;

No aspecto econômico a adoção da forma do pregão eletrônico permitirá pleno acesso a fornecedores de qualquer parte do país.

Em função do ambiente normativo da necessidade de proteção adequada das informações do TJCE, seja como proprietário ou custodiante, o presente projeto tem em seu conteúdo perfeitamente aderente, pois proporcionará automatizar o processo de GRC – Governança, Riscos, Compliance e Segurança da Informação com o fornecimento de um software especializado, com consultoria para implementação de serviços especializados de Administração, Gerenciamento e Monitoramento das soluções de riscos e de segurança, possibilitando:

- Implementação de serviços especializados de Administração, Gerenciamento e Monitoramento das soluções de segurança;
- Implementação de serviços de Tratamento de Resposta a Incidentes de segurança;
- Inventário dos ativos envolvidos de TIC – Ambientes, Pessoas, Sistemas, Processos e Pessoas;
- Análises e testes dos ativos envolvidos de TIC – Ambientes, Pessoas, Sistemas, Processos e Pessoas;
- Avaliações dos ativos envolvidos de TIC – Ambientes, Pessoas, Sistemas, Processos e Pessoas;
- Tratamento das recomendações oriundas das análises dos ativos envolvidos de TIC – Ambientes, Pessoas, Sistemas, Processos e Pessoas;
- Implementação de um modelo de gestão de riscos;
- Implementação de um software de continuidade de TI;
- Implementação de um software de dashboard, com geração automática de relatórios e gráficos;
- Implementação de um software de workflow para acompanhamento das não conformidades e implementações das recomendações originadas;
- Implementação de um software de Políticas, Normas e Procedimentos;
- Implementação, atualização e adequação do conjunto normativo de segurança da informação e comunicações;
- Implementação de um sistema de continuidade de TI;
- Internalização de método para a governança, riscos e conformidade do ambiente de TI;
- Implementação de um processo de resposta a incidentes;
- Internalização de conhecimento, métodos e ferramenta, através de treinamento em segurança da informação.

2.3. Resultados a serem Alcançados com a Contratação

A padronização, automatização dos processos de GRC e o uso de boas práticas e metodologias para os processos relacionados à Segurança da Informação e Comunicações visam mitigar os riscos no ambiente tecnológico do TJCE, bem como planejar ações de resposta a incidentes de segurança e situações de desastres possibilitando as equipes a adoção de respostas rápidas reduzindo significativamente as interrupções dos processos relacionados com as atividades criticas do Tribunal. A aquisição em questão visa ainda possibilitar a recuperação de dados e a elaboração de planos de continuidade de negócio que trazem os seguintes benefícios diretos;

- Um ambiente centralizado, apoiado pelo software, não só para o inventário, coletas, análises e avaliações, mas principalmente para o efetivo acompanhamento e tratamento das ações corretivas e/ou preventivas que devam ser adotadas;
- Preservação da imagem do Órgão perante a população, com respostas e prestação de contas;
- Diminuição de esforços relacionados à Governança, Gestão dos Riscos, Conformidade e Gestão de Segurança da Informação e Comunicações devida à automatização de grande parte dos processos e projetos;
- Atendimento a regulamentações, com aderência e conformidade;
- Os projetos visam também a consolidação das ações relacionadas a Segurança da Informação e Comunicações por meio de uso de software e a padronização das análises e avaliações de riscos por meio do uso das bases de conhecimento nativas no software. Tais ações trazem como resultado os seguintes benefícios ao TJCE:
- Melhoria na qualidade e confiabilidade dos indicadores gerados para controle das ações;
- Melhoria na comunicação entre as áreas de tecnologia, no que diz respeito ao tratamento de pontos críticos relacionados à segurança;
- Método confiável e padronizado para coleta de informações de risco e conformidade;

- Geração de relatórios padronizados com confiabilidade referente ao quantitativo de ações, eventos, atividades e indicadores de riscos;
- Indicadores que possam subsidiar o TJCE nas tomadas de decisão;
- Definição de Estratégias para a Continuidade do Negócio;
- Definição da criticidade dos Ativos/Sistemas para priorização (análise de impacto);
- Definição de uma Política de Continuidade de Negócio;
- Plano de Recuperação de Desastres para reconstrução do ambiente tecnológico em caso de:
  - Incêndio;
  - Enchentes;
  - Falta de Energia;
  - Roubo ou Furto de equipamentos;
  - Outros.
- Planos de Administração de Crises para priorização de ações de continuidade durante uma situação de desastres;
- Planos de Gerenciamento de Incidentes para respostas a incidentes no intuito de evitar desastres;
- Planos de Continuidade Operacional no intuito de possibilitar a continuidade das operações críticas durante um desastre;

2.4. Justificativa Técnica da Solução Escolhida

O Conselho Nacional de Justiça – CNJ divulgou as Diretrizes para a implantação da Gestão de Segurança da Informação (GSI) no Poder Judiciário, visando à proteção, principalmente, dos ativos críticos de negócio.

Tais orientações devem ser devidamente compreendidas como linhas mestras de conduta e adotadas em todos os níveis pelos órgãos do Judiciário Brasileiro e tem como objetivo a preservação dos aspectos de confidencialidade, integridade e disponibilidade das informações, bem como contribuir para que a missão do Judiciário seja cumprida.

Toda a manutenção da segurança das informações do Tribunal de Justiça do Estado do Ceará é realizada pela mesma equipe que cuida da infraestrutura de TIC. É fundamental a existência de um sistema que automatize o processo de GRC – Governança, Riscos, Compliance e de Gestão de segurança da informação devidamente implementado e que possa automatizar todos os processos de Riscos e Continuidade de negócios.

Os desafios da segurança da informação aumentam de tamanho a cada dia. São tantos os problemas que os profissionais da área tem uma imensa dificuldade de se manterem atualizados dada a quantidade de novas vulnerabilidades e as necessidades constantes de correção dos sistemas. Some-se a isso os problemas de roubo de identidades, o uso de técnicas de phishing cada vez mais efetivas, que perseguem sistemas mundo afora. Esses e muitos outros exemplos demandam que revisemos constantemente os conceitos básicos de segurança com o objetivo de mantermos nossa perspectiva e foco.

Precisamos aplicar sólidos princípios de gestão de riscos para que possamos focar nossos recursos nas áreas problemáticas mais críticas. Com os riscos mais importantes priorizados e as proteções apropriadas selecionadas, podemos estar confiantes que os maiores incidentes de segurança serão evitados ou, pelo menos, reduzidos.

A base de um programa sólido de segurança da informação são as políticas. Elas servem para garantir que toda a organização esteja focada na mesma direção quanto aos princípios de segurança e que os colaboradores se reúnam em um esforço centralizado para oferecer uma frente coesa contra todo tipo de intrusos.

O TJCE possui dois Sites (Data Center´s) um localizado no Centro de Documentação e Informática – CDI e o outro no Fórum Clóvis Beviláqua – FCB, sendo que o Tribunal ainda não possui os procedimentos de contingência dos serviços de TI em caso de desastres.

A gestão da continuidade de TI pode garantir que a área de TI da organização seja capaz de voltar a operar caso algum desastre aconteça. A alta gerência não pode se permitir acreditar que algo nunca acontecerá à organização. Tudo que eles precisam é olhar ao redor e ver exemplos do que aconteceu aos outros.

Boas práticas de governança corporativa e riscos são metas perseguidas por todas as organizações, incluindo a administração pública. Assim, o Tribunal de Justiça do Estado do Ceará - TJCE na busca constante pela excelência na prestação dos serviços e relacionamento transparente com a sociedade, procura aperfeiçoar o gerenciamento de seus objetivos quando se depara com riscos e obstáculos crescentes, especialmente na busca da adequação das operações às leis e regulamentações aplicáveis.

O TJCE vem buscando constantemente a efetiva melhora em seus processos de gestão de segurança das informações e comunicações, e este termo de referência tem por objetivo especifico analisar e avaliar conformidade com as diversas normativas tendo como referência ainda, as boas práticas de mercado para executar ações de melhorias que se façam necessárias para o funcionamento pleno dos dispositivos implantados.

2.5. Justificativa para Parcelamento do Objeto

Devido ao fato de que o fornecimento dos serviços contidos na tabela **LOTE I** especificada no item **2.1**, podem ser realizados por empresas que não fornecem os serviços contidos na tabela **LOTE II** especificada no item **2.1**, é de fundamental importância para a competitividade do certame o parcelamento do objeto.

2.6. Justificativa do Serviço por demanda para o LOTE 01

O serviço por demanda pode ser entendido como o uso de uma quantidade de serviços alocada a um intervalo definido de tempo para atender a um objetivo específico. Uma forma de contratação que estabelece o "quanto", "quando" e "quem" realizará o serviço, bem como os padrões de qualidade e aceitação dos serviços realizados.

Para atender às exigências legais, este Termo de Referência foi elaborado a partir de conceitos atuais e recomendações de melhores práticas, com instrumentos de controle capazes de aferir se a demanda foi efetivamente atendida, tendo como elementos balizadores a definição prévia e adequada dos serviços. Foi prevista também a avaliação dos resultados e o pagamento após a emissão do atesto conferencial dos serviços desenvolvidos.

Entre as vantagens deste tipo de contratação está o fato de não haver caracterização de locação exclusiva de mão de obra, uma vez que a forma básica para a solicitação do serviço por demanda é "o próprio serviço". Adicionalmente, ficam excluídos da presente contratação todo e qualquer reembolso, tais como salários, diárias, passagens ou quaisquer outros insumos, vetados por lei, que possam caracterizar a subordinação dos prestadores de serviços à administração do TJCE.

Ainda, quanto à abordagem referente à sua economicidade, a presente contratação visa estabelecer exatamente quais demandas deverão ser atendidas, evitando que sejam desperdiçados recursos financeiros com alocações indevidas, desnecessárias e onerosas.

Os serviços serão demandados, considerando-se o tempo necessário para sua execução, além de exigir da CONTRATADA o produto na qualidade, prazo e forma previamente pactuados.
A contratação por demanda, descrita neste Termo de Referência, visa garantir a contratação unicamente dos serviços efetivamente necessários ao TJCE.

LOTE 01

3. DESCRIÇÃO DA SOLUÇÃO

3.1. OBJETIVO

3.1.1. Serviços especializados de Administração, Gerenciamento e Monitoramento das soluções de segurança do TJCE.
3.1.2. Serviços especializados de Tratamento de Resposta a Incidentes de segurança das soluções do TJCE.

3.2. FIREWALL/VPN – MATRIZ

3.2.1. 03 (três) appliances Firewall/VPN do tipo CISCO ASA-5550;
3.2.2. Os appliances estão implantados e em funcionamento nos Data Centers do TJCE na cidade de Fortaleza/CE;
3.2.3. Deve ser considerada a revisão das configurações e regras atuais da solução;
3.2.4. Durante a vigência do contrato poderá haver mudança da solução em virtude do fim do contrato de suporte, devendo a CONTRATADA manter as funcionalidades contratadas na nova solução.

3.3. FIREWALL/VPN – LOCALIDADES REMOTAS

3.3.1. 216 (duzentos e dezesseis) appliances de Firewall/VPN em localidades remotas do tipo CISCO ASA-5505, sendo;
3.3.1.1. 26 firewalls já estão implantados e em funcionamento em prédios do TJCE na cidade de Fortaleza/CE;
3.3.1.2. 190 firewalls estão como previsão de aquisição para serem implantados nas comarcas do interior do Estado;
3.3.2. Deve ser considerada a revisão das configurações e regras atuais da solução;
3.3.3. Durante a vigência do contrato poderá haver mudança da solução em virtude do fim do contrato de suporte, devendo a CONTRATADA manter as funcionalidades contratadas na nova solução.

3.4. IPS – INTRUSION PREVENT SYSTEM

3.4.1. 02 (dois) appliances IPS do tipo CISCO IPS-4260;
3.4.2. Os appliances estão implantados e em funcionamento nos Data Centers do TJCE na cidade de Fortaleza/CE;
3.4.3. Deve ser considerada a revisão das configurações e regras atuais da solução;
3.4.4. Durante a vigência do contrato poderá haver mudança da solução em virtude do fim do contrato de suporte, devendo a CONTRATADA manter as funcionalidades contratadas na nova solução.

3.5. SIEM – SECURITY INFORMATION AND EVENT MANAGEMENT

3.5.1. 01 (um) appliance SIEM do tipo CISCO MARS;
3.5.2. O appliance está implantado e em funcionamento no Data Center do TJCE na cidade de Fortaleza/CE;
3.5.3. Deve ser considerada a revisão das regras atuais e implantação de todas as soluções compatíveis em funcionamento no TJCE para monitoração do SIEM, incluindo Firewalls, Controladores de domínio do tipo Active Diretory, IPS, MAIL security, WEB security, Endpoint security, WOP, WLAN, etc.
3.5.4. Durante a vigência do contrato poderá haver mudança da solução em virtude do fim do contrato de suporte, devendo a CONTRATADA manter as funcionalidades contratadas na nova solução.

3.6. MAIL SECURITY
3.6.1. 01 (uma) solução de Mail Security no site principal do tipo CISCO Ironport C160;
3.6.2. A solução protege 1.000 (um mil) caixas postais;
3.6.3. A solução já está implantada e em funcionamento no prédio principal do TJCE na cidade de Fortaleza/CE.
3.6.4. Durante a vigência do contrato poderá haver mudança da solução em virtude do fim do contrato de suporte, devendo a CONTRATADA manter as funcionalidades contratadas na nova solução.

3.7. WEB SECURITY
3.7.1. 01 (uma) solução de Web Security no site principal do tipo McAfee Web Gateway;
3.7.2. A solução protege 1.500 (um mil e quinhentos) usuários;
3.7.3. A solução já está implantada e em funcionamento no prédio principal do TJCE na cidade de Fortaleza/CE.
3.7.4. Durante a vigência do contrato poderá haver mudança da solução em virtude do fim do contrato de suporte, devendo a CONTRATADA manter as funcionalidades contratadas na nova solução.

3.8. ENDPOINT SECURITY
3.8.1. 01 (uma) solução de EndPoint Security no site principal do tipo Kaspersky Security Center;
3.8.2. A solução protege 5.500 (cinco mil e quinhentos) usuários;
3.8.3. A solução já está implantada e em funcionamento no prédio principal do TJCE na cidade de Fortaleza/CE.
3.8.4. Durante a vigência do contrato poderá haver mudança da solução em virtude do fim do contrato de suporte, devendo a CONTRATADA manter as funcionalidades contratadas na nova solução.

3.9. DESCRIÇÃO DETALHADA DOS SERVIÇOS DE ADMINISTRAÇÃO, GERENCIAMENTO E MONITORAMENTO DOS ATIVOS DE SEGURANÇA

3.9.1. A CONTRATADA deverá prestar serviço de Administração, Gerenciamento e Monitoramento para as soluções abaixo, no formato 24x7x365 dias:
3.9.1.1. Firewall/VPN – Matriz;
3.9.1.2. Firewall/VPN – Localidades Remotas;
3.9.1.3. IPS – Intrusion Prevent System;
3.9.1.4. SIEM – Security Information and Event Management;
3.9.2. A CONTRATADA deverá realizar configuração, ajustes, testes dos hardwares e softwares relacionados para as soluções descritas;
3.9.3. A instalação dos equipamentos do tipo concentrador para ativação da solução de monitoração devem ser realizadas nos Data Centers do CONTRATANTE, localizado em Fortaleza/CE;
3.9.4. Todas as atividades envolvidas serão acompanhadas e apoiadas por analistas e técnicos da CONTRATANTE;
3.9.5. A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades realizadas após o expediente (horários noturnos ou em finais de semana e feriados);
3.9.6. Todas as soluções deste lote devem ser revisadas na etapa de ativação das soluções (inicial) e revisões periódicas, validando regras/políticas das soluções, garantindo proteção da rede e usuários que trafegam na rede;
3.9.7. A CONTRATADA deverá instalar e incluir um link de dados dedicado a ser instalado no Data Center da CONTRATANTE (ponta A) tendo na outra extremidade o SOC da CONTRATADA (ponta B) com throughput suficiente para a realização dos serviços de gerenciamento, às custas da CONTRATADA,
3.9.8. A CONTRATADA deverá instalar e incluir uma Conexão VPN (Virtual private Network), compatível com a solução atualmente usada pelo Tribunal, usada como redundância da conexão dedicada, para caso haja indisponibilidade do link de dados.
3.9.9. O atendimento deverá ser realizado por central de serviços da própria CONTRATANTE e/ou telefone;
3.9.10. Não sendo possível registrar o atendimento/chamado na central de serviços da CONTRATANTE, a CONTRATADA deverá disponibilizar a sua própria central de serviços para realização dos serviços;
3.9.11. Os serviços deverão ser prestados remotamente, a partir de Centros de Atendimento próprios, localizados no Brasil, estritamente de acordo com as especificações deste documento;
3.9.12. Para suporte técnico remoto: suporte prestado por meio de Central de Atendimento 0800 ou equivalente à ligação local, web, e-mail e fax;
3.9.13. Esclarecimento de dúvidas relacionadas à prestação dos serviços, políticas e regras implementadas,

funcionalidade da solução, deverão ser de atendimento imediato;
3.9.14. Suporte técnico local: atendimento in-loco, prestados por técnicos capacitados para a solução de problemas relacionados aos equipamentos e softwares. Este suporte poderá ser solicitado pela CONTRATANTE sempre que necessário;
3.9.15. Visitas técnicas, quando necessárias, estarão restritas às instalações da Secretaria de Tecnologia da Informação do TJCE;
3.9.16. Os recursos humanos envolvidos na implantação e prestação do serviço de suporte deverão estar capacitados na solução envolvida. Entende-se por capacitação: certificados profissionais emitidos pelos fabricantes das soluções que serão ofertadas;
3.9.17. O TJCE é responsável pelo envio dos equipamentos de sua propriedade para o fabricante em caso de manutenção;
3.9.18. Os chamados abertos somente poderão ser fechados após autorização de funcionário designado pelo TJCE.
3.9.19. O fechamento por parte da contratada que não tenha sido previamente autorizado pelo TJCE poderá ensejar aplicação de multa a CONTRATADA no valor conforme termo de contrato do valor mensal pelos serviços por ocorrência;
3.9.20. O TJCE informará as pessoas autorizadas a abrir e fechar chamados junto a CONTRATADA, bem como o meio pelo qual a autorização de fechamento será formalizada;
3.9.21. Os serviços contemplam os seguintes itens:
3.9.21.1. Regras das soluções (de acesso, NAT, alertas, etc.) – inclusão, exclusão e alteração;
3.9.21.2. Usuários – inclusão, exclusão e alteração;
3.9.21.3. Configuração das soluções;
3.9.21.4. Mudança das soluções;
3.9.21.5. Logs (configurações, armazenamento, organização e recuperação);
3.9.21.6. Criação e manutenção de regras para os ativos de segurança do escopo;
3.9.21.7. Criação e manutenção de contas e grupos de VPN;
3.9.21.8. A correta alocação de recursos necessários para restaurar a operação com a maior brevidade possível;
3.9.21.9. Elaboração de análise crítica para cada inclusão/exclusão/alteração de regras nos ativos de segurança do escopo, a fim de garantir a gestão de mudanças no ambiente da CONTRATANTE;
3.9.21.10. Análise de logs dos ativos de segurança do escopo, com geração mensal de relatórios operacionais e gerenciais para a CONTRATANTE, classificando todos os eventos por nível de criticidade com descrição detalhada dos eventos e recomendações de ações;
3.9.21.11. Atualização de patches e novas versões de firmware nos equipamentos;
3.9.21.12. Nos serviços de Firewall, a CONTRATADA deverá se responsabilizar pela gravação de dados para auditoria, de forma detalhada para cada conexão efetivada, incluindo a origem, serviço, hora de conexão, destino e ação executada;
3.9.21.13. Condução e resolução remota de incidentes e requisições de serviço relacionadas à segurança das informações do TJCE;
3.9.21.14. Aplicação das mais recentes versões, patches e hotfixes nos ativos;
3.9.21.15. Backup das soluções;
3.9.21.16. Realização de testes de segurança periódicos nos ativos (auditoria/análise de segurança);
3.9.21.17. Otimização periódica bimestral de regras, baseada na utilização de regras, protocolos, usuários, etc.);
3.9.21.18. Documentação das soluções;

3.10. DESCRIÇÃO DETALHADA DOS SERVIÇOS DE TRATAMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA

3.10.1. A CONTRATADA deverá prestar serviço de Tratamento de Resposta a Incidentes de Segurança para as soluções abaixo, no formato 24x7x365 dias:
3.10.1.1. Firewall/VPN;
3.10.1.2. IPS – Intrusion Prevent System;
3.10.1.3. SIEM – Security Information and Event Management;
3.10.1.4. Mail Security
3.10.1.5. Web Security
3.10.1.6. Endpoint Security
3.10.2. Se o TJCE ainda não possuir o seu modelo de Tratamento de Resposta a Incidentes de Segurança, a CONTRATADA deverá apresentar o seu modelo de identificação de ocorrências, registro, ações de medidas corretivas e atualização dos chamados para o acompanhamento e resolução de incidentes;
3.10.3. Durante a fase de ativação, deve ser definido em conjunto, pelo TJCE e pela CONTRATADA, o plano de tratamento de resposta a incidentes, que incluirá detalhes deste processo.
3.10.4. A CONTRATADA deve dispor de um modelo deste plano, que deverá ser discutido e aprovado pelo TJCE.
3.10.5. A CONTRATADA deve estabelecer com o TJCE um plano de comunicação entre a CONTRATADA e

o TJCE, garantindo a oficialização dos meios de comunicação e a matriz de escalonamento;
3.10.6. Os serviços de tratamento de resposta a incidentes de segurança contemplam os seguintes itens:
3.10.6.1. Geração de eventos de segurança;
3.10.6.2. Coleta;
3.10.6.3. Armazenamento;
3.10.6.4. Análise;
3.10.6.5. Reação;
3.10.6.6. Detectar incidentes através das soluções de monitoramento do SOC, informativos, reclamações de órgãos oficiais externos, solicitação do TJCE;
3.10.6.7. Receber informações relativas a incidentes, criar registro, e encaminhar o incidente em questão para resolução;
3.10.6.8. Comunicar o status dos incidentes ao TJCE conforme se faça necessário;
3.10.6.9. Fornecer ao TJCE as atualizações regulares do status dos incidentes;
3.10.6.10. Abrir processo de gerência de mudança, com aprovação do TJCE, para solucionar um incidente, caso necessário;
3.10.6.11. Encerrar o registro dos incidentes, de acordo com os procedimentos estabelecidos.
3.10.6.12. Monitoramento e análise remota das informações dos incidentes de segurança registrados, incluindo os itens afetados por eles;
3.10.6.13. Investigação e diagnóstico remoto de incidentes de segurança registrados, incluindo resolução dos mesmos, sempre que possível;
3.10.6.14. O envolvimento da equipe de TI da CONTRATANTE, bem como especialistas de 3º nível da CONTRATADA, no tratamento do incidente;
3.10.6.15. Monitoração em tempo real de eventos de risco (intrusão, disponibilidade, falhas de acesso importantes etc.), com processo previamente formalizado de resposta a incidentes originados da Internet;
3.10.6.16. Análise e Correlação dos Logs, através de SIEM (Security information and event management), utilizando a solução da CONTRATANTE;
3.10.6.17. Resposta aos alertas de segurança;
3.10.6.18. Categorizar os níveis de alertas;

3.11. DESCRIÇÃO DETALHADA DOS SERVIÇOS DE PORTAL DE ATENDIMENTO

3.11.1. A CONTRATADA deverá disponibilizar um portal de atendimento e abertura de chamados;
3.11.2. A CONTRATADA deve assegurar que os chamados, eventos e/ou incidentes de rede e/ou segurança sejam transferidos para outros técnicos ou grupos de solucionadores conforme suas especialidades, com acompanhamento total de passos, histórico de registros, datas, horários e consumo de tempo;
3.11.3. Deverá armazenar os relatórios periódicos, permitindo que o TJCE realize download dos seus relatórios mensais (mês corrente e anteriores);
3.11.4. A CONTRATADA deve fornecer uma visão que permite observar o gerenciamento da fila de atendimento, utilizada pelos analistas, onde é apresentada a ordem em que os chamados devem ser atendidos, bem como, possibilita contínuo monitoramento de tempo e volume por chamados em fila;
3.11.5. A CONTRATADA deve utilizar uma Interface Web, permitindo com que os seus técnicos possam executar funções de abrir, escalar, atualizar o andamento do chamado e encerrá-lo;
3.11.6. A solução da CONTRATADA deve ser integrada com a solução do TJCE, prevista para ser contratada durante o período do contrato.
3.11.7. A contratada deve garantir a integração entre os componentes, funcionalidades ou aplicações de diferentes fabricantes por meio de Web Services ou Linha de Comando ou e-mail.

3.12. DESCRIÇÃO DETALHADA DO NMS (ACORDO DE NÍVEL MÍNIMO DE SERVIÇO)

3.12.1. A CONTRATADA deverá disponibilizar as atualizações e patches de segurança de cada produto contratado durante 24 (vinte e quatro) horas por dia, 07 (sete) dias da semana.
3.12.2. A CONTRATADA deverá prover as atualizações de "releases" e de versões dos produtos licenciados durante a vigência do contrato, sendo que estas atualizações deverão passar também a estarem cobertas pelas garantias, níveis de serviços e demais termos deste serviço de manutenção.
3.12.3. A CONTRATADA deverá garantir os serviços de suporte a customização, parametrização e configuração voltadas à atualização e utilização de funcionalidades disponibilizadas nos produtos licenciados ou em versões superiores que sejam lançadas durante a vigência do contrato, para todos os produtos fornecidos e disponibilizados pelo TJCE no ambiente de produção. Este suporte, customização, parametrização e configuração deverão ser efetuadas no prazo máximo de 10 (dez) dias úteis, contados a partir da abertura do chamado;
3.12.4. A CONTRATADA deverá resolver os atendimentos, em pelo menos 90% (noventa por cento) das solicitações, nos seguintes prazos máximos:
3.12.4.1. Dúvidas ou alteração de configuração (P3): 30 minutos, contados a partir da abertura do chamado;

- Prioridade (P3) - Ocorrência de baixo impacto na utilização da Solução de Segurança para resolver problemas de funcionamento ou resposta a incidentes que não ocasionem paradas nas aplicações/ativos que deles fazem uso.

3.12.4.2. Serviço com performance inadequada (P2): 1:30 horas, contadas a partir da abertura do chamado;

- Prioridade (P2) - Ocorrência de médio impacto/Falha verificada em uma determinada funcionalidade da Solução de Segurança que impeça a obtenção do resultado esperado, mas a solução ou serviço permanecem funcionando para outras finalidades;

3.12.4.3. Serviço indisponível (P1): 2 horas, contadas a partir da abertura do chamado.

- Prioridade (P1) - Ocorrência de alto impacto/Falha verificada em um componente da Solução de Segurança que ocasione parada total ou parcial das atividades do ambiente da CONTRATANTE;

3.12.5. A CONTRATADA deverá garantir o atendimento e suporte para um número ilimitado de solicitações.

3.12.6. A CONTRATADA deverá garantir Suporte on-site no caso de impossibilidade de resolução do problema remotamente em horário comercial, exceto para solicitações (P1) que poderá ser na modalidade de 24 (vinte e quatro) horas, 7 (sete) dias da semana, apenas aos equipamentos concentradores, instalados no Datacenter do TJCE na cidade de Fortaleza/CE.

3.12.7. A CONTRATADA deverá garantir o serviço de suporte aos softwares contratados que deverá ser executado obrigatoriamente, por especialistas em resolução de problemas, na modalidade de atendimento 24 (vinte e quatro) horas, 7 (sete) dias da semana.

3.12.8. A CONTRATADA deverá trabalhar, ininterruptamente, na solução dos problemas críticos (P1) até que a solução contratada esteja novamente operando em regime normal de produção. Caso a solução do problema reportado exija a presença de técnicos(s) da CONTRATADA, mesmo fora do horário comercial, este(s) deverá (ão) ficar dedicado(s) a resolução do problema até que ele esteja resolvido.

3.12.9. Os indicadores de desempenho deverão ser monitorados e servirão de base para a avaliação mensal da CONTRATADA no "Relatório de Acompanhamento de Execução do Contrato", onde será possível verificar a efetividade do atendimento e permitir a depuração do processo.

3.12.10. Os NMS's devem ser considerados e entendidos pela CONTRATADA como um compromisso de qualidade que assumirá junto a CONTRATANTE.

3.12.11. A análise dos resultados destas avaliações pela CONTRATANTE resultará em advertências ou penalizações caso a CONTRATADA, não cumpra com os seus compromissos de qualidade e desempenho.

3.13. DESCRIÇÃO DETALHADA DOS RELATÓRIOS

3.13.1. Durante a Etapa de Ativação do Serviço, a CONTRATANTE e a CONTRATADA definirão os tipos de relatórios técnicos que deverão ser gerados e enviados mensalmente.

3.13.2. A CONTRATADA deverá emitir até o 10º (décimo) dia útil do mês subsequente ao período analisado os seguintes relatórios gerenciais:

3.13.2.1. Atendimentos realizados no período;

3.13.2.2. Percentual do NMS de atendimento consumido;

3.13.2.3. Percentual do NMS de solução consumido;

3.13.2.4. Gráfico e análise das maiores origens/destinos/portas de tráfego no período;

3.13.2.5. Gráfico e análise dos maiores acessos de usuários VPN no período;

3.13.2.6. Tabela e análise dos maiores eventos das soluções no período;

3.13.2.7. Informações sobre atualização dos equipamentos;

3.13.2.8. Informações sobre a disponibilidade dos ativos;

4. DA PRESTAÇÃO DOS SERVIÇOS

4.1. Do Local:

4.1.1. TJCE: na Av. General Afonso Albuquerque Lima, S/N. - Cambeba CEP: 60822-325, Fortaleza-CE, na Secretaria de Tecnológica da Informação – SETIN.

4.2. Forma de Fornecimento:

4.2.1. Todo o fornecimento deverá estar de acordo com os critérios estabelecidos nos itens deste Termo de Referência;

4.2.2. A Contratada deverá implementar rigorosa gerência de projeto, com observância às regras a seguir além de adotar a Metodologia de Gerenciamento de Projetos – MGP da SETIN;

4.2.3. Para a inicialização do projeto, a empresa Contratada deverá executar:

4.2.3.1. Abertura do projeto: deverá ser elaborado e apresentado **Termo de Abertura do Projeto**;

4.2.3.2. Apresentação do escopo do serviço: deverá ser elaborado e apresentado **Declaração de Escopo do Projeto**;

4.2.3.3. Pré-planejamento do projeto: deverá ser elaborado e apresentado Plano de Gerenciamento do Projeto;

4.2.3.4. A Contratada deverá apresentar Cronograma de Execução, constando atividades, subatividades e marcos, contemplando todas as ações previstas para a execução dos serviços, datas de entrega de documentação, datas das reuniões de ponto de controle, dentre qualquer outro evento que se julgar relevante e necessário;

4.2.3.5. A Contratada deverá agendar reunião ("kick-off meeting") junto aos responsáveis técnicos da Contratante, objetivando dar início ao acompanhamento da execução do Contrato;

4.2.3.6. Na reunião de "kick-off", a Contratada deverá apresentar sua equipe de trabalho, composta, no

mínimo, por 01 (um) Gerente de Projeto e Equipe de Técnicos Especialistas;
4.2.3.7. Para apoio ao Gerente de Projeto, deverão ser alocados todos os técnicos necessários para a execução dos serviços;
4.2.3.8. Caberá ao Gerente de Projeto coordenar e orientar todo o processo de planejamento e execução dos serviços do Contrato, respeitando os prazos estabelecidos, atestando a qualidade dos serviços executados;
4.2.3.9. Deverá ser elaborada e apresentada Lista de Contatos do Projeto;
4.2.3.10. Definição das regras para execução do serviço;
4.2.3.11. Definição das responsabilidades de cada um dos envolvidos;
4.2.4. A contar da 1ª reunião do projeto, deverão ser executadas reuniões de controle do projeto ("Status do Projeto") entre as equipes técnicas envolvidas, onde o Gerente de Projeto posicionará os responsáveis do CONTRATANTE sobre o andamento do projeto e apresentando os documentos pertinentes;
4.2.5. As reuniões de status poderão ser realizadas semanalmente, quinzenalmente ou conforme a demanda, a critério da CONTRATANTE;
4.2.6. O Gerente será responsável pela elaboração e entrega de relatórios de progresso e ou situação do projeto ("Relatório de Acompanhamento"), onde deverão ser descritas as atividades pertinentes ao período, além de destacar as pendências e solicitações de mudança do projeto, dentre outros tópicos;
4.2.7. Os relatórios de progresso e ou situação do projeto deverão ser fornecidos por período, semanalmente, quinzenalmente ou conforme a demanda, a critério da CONTRATANTE;
4.2.8. Todas as reuniões do projeto deverão ser registradas em "Ata", a qual será de inteira responsabilidade do Gerente;
4.2.9. As atas deverão ser entregues em no máximo 48 (quarenta e oito) horas após a realização da reunião para verificação e revisão por parte do TJCE, para posterior emissão de aceite por ambas as partes;
4.2.10. Após a apresentação e aprovação dos documentos relacionados ao plano de projeto, a equipe do projeto dará início às demais Fases do cronograma;
4.2.11. Produtos da fase para entrega ao TJCE:
4.2.11.1. Documentação inicial do projeto, incluindo termo de abertura, declaração de escopo, plano de gerenciamento, cronograma de trabalho, matriz de responsabilidade e lista de contatos dos participantes;
4.2.11.2. Documentos de acompanhamento do projeto, incluindo relatórios de situação e atas de reunião;
4.2.11.3. Termo de Aceitação;

4.3. Oficialização da demanda dos serviços por meio da emissão de "Ordem de Serviço – OS":

4.3.1. A execução será sempre precedida da emissão pelo TJCE da competente "Ordem de Serviço – OS", contendo no mínimo: descrição do serviço, quantitativo, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço esperados;
4.3.2. A "Ordem de Serviço – OS" será emitida, assinada e autorizada pelo Fiscal do Contrato;
4.3.3. Toda "Ordem de Serviço – OS" deverá ser assinada pelo Gerente do Projeto / Preposto, representante da CONTRATADA perante o TJCE, declarando a concordância da CONTRATADA em executar as atividades descritas na "Ordem de Serviço – OS", de acordo com as especificações estabelecidas pelo TJCE;
4.3.4. Os serviços deverão estar sempre de acordo com as especificações constantes nas "Ordens de Serviços – OS";
4.3.5. O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução – quando a "Ordem de Serviço – OS" é emitida pelo TJCE, durante a execução – com o acompanhamento e supervisão de responsáveis do TJCE, e ao término da execução – com o fornecimento de "Relatório de Serviços" pela Contratada e atesto dos mesmos por responsáveis do TJCE;
4.3.6. Todos os serviços prestados pela Contratada deverão ser necessariamente documentados (passo-a-passo), registrados e entregues ao TJCE pela mesma, em cópias impressas e gravadas em meio magnético, complementarmente ao "Relatório de Serviços";

4.4. Do Recebimento

4.4.1. Todos os serviços terão suas métricas medidas a cada mês após a emissão da primeira ordem de serviço – OS;
4.4.2. A CONTRATANTE atestará o recebimento dos mesmos, mensalmente, através da validação do Relatório de Níveis de Serviços.
4.4.3. Para aceite do recebimento e posterior encaminhamento ao pagamento, deverão ser apresentados os seguintes documentos:
4.4.3.1. Ordem de Serviços emitida e assinada, Relatório de Serviços e demais Documentos Técnicos pertinentes e comprobatórios de execução do serviço;
4.4.4. A frequência de aferição e avaliação dos níveis de serviços será mensal, devendo, a CONTRATADA, elaborar relatório gerencial de serviços, apresentando-o, à CONTRATANTE, até o 5º. (quinto) dia útil do mês subsequente ao da prestação dos serviços.
4.4.5. Devem constar desse relatório, dentre outras informações, os indicadores/metas de níveis de serviços definidos e alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e

demais informações relevantes para a gestão contratual.
4.4.6. O conteúdo detalhado e a forma do relatório gerencial serão definidos pelas partes.
4.4.7. Independentemente da aceitação no recebimento, a Contratada deverá garantir a qualidade do serviço executado pelo prazo estabelecido nas especificações e nas condições constantes deste Termo de Referência, obrigando-se a corrigir aquele que apresentar inconsistência no prazo estabelecido pelo TJCE.
4.4.8. Os Fiscais do Contrato verificarão a conformidade dos serviços e/ou da entrega e da documentação requerida e, no caso de estarem conformes, atestará a Nota Fiscal e encaminhará para pagamento. No caso de não estarem conformes, as devolverá, com as ressalvas devidas, no prazo de até 10 (dez) dias da apresentação, para a Contratada providenciar a sua conformidade e novo encaminhamento para o TJCE.
4.4.9. No caso dos serviços em não conformidade, a contagem dos prazos aqui estabelecidos será reiniciada a contar da data do saneamento das ressalvas pela CONTRATADA, devidamente certificadas pelo Fiscal do Contrato.
4.4.10. O TJCE rejeitará, no todo ou em parte, os serviços executados em desacordo com o disposto. Se, após o recebimento, constatar-se que os serviços foram executados em desacordo com o especificado, com defeito ou incompleto, os responsáveis do TJCE notificarão, por escrito, à CONTRATADA, interrompendo-se os prazos de recebimento e ficando suspenso o pagamento até que seja sanada a situação.
4.4.11. Os valores da(s) NF(s) / Fatura(s) deverão ser os mesmos consignados na Nota de Empenho, sem o que não será liberado o respectivo pagamento. Em caso de divergência, será estabelecido prazo para a Contratada fazer a substituição desta(s) NF(s) / Fatura(s).
4.4.12. São critérios de mensuração dos serviços prestados para controle dos pagamentos:

Item	Métrica	Indicador	Valor
Serviços técnicos	Unidade	Serviço Especificado na OS	100% executado

4.5. Os Serviços estarão passíveis de recusa quando:

4.5.1. Apresentarem especificações técnicas diferentes das estabelecidas neste Termo e nos seus anexos;
4.5.2. Em casos de impactos insatisfatórios no ambiente. Os ajustes necessários no procedimento de execução dos serviços deverão ocorrer no prazo não superior a 48 (quarenta e oito) horas corridas contadas do momento da comunicação do ocorrido através de documento emitido pelos setores responsáveis pela contratação;
4.5.3. Os ajustes referentes aos serviços ora autorizados pelo TJCE e executados pela Contratada deverão ocorrer por conta da mesma sem gerar qualquer ônus ao Tribunal de Justiça do Estado do Ceará, sem isentar a CONTRATADA de qualquer sanção prevista neste documento.

4.6. Do Prazo

4.6.1. Os serviços deverão ser executados a partir de notificação para fornecimento dos serviços a ser emitida pelo TJCE posterior à assinatura do contrato;
4.6.2. Em até 10 (dez) dias corridos a partir da data de emissão da notificação para fornecimento dos serviços pelo TJCE, a empresa CONTRATADA deverá efetuar a inicialização do projeto;
4.6.3. Efetuada a inicialização do projeto, com o competente aceite de abertura do projeto, todos os serviços contemplados pelo Objeto deverão estar disponíveis para demanda do TJCE via emissão de Ordem de Serviços – OS;

4.7. Tabela de Acordo de Níveis Mínimos de Serviços

Descrição	Definição	Cálculo	Aferição	Tempo de Atendimento	Glosa	Meta
DISPONIBILIDADE DA SOLUÇÃO DE GERNCIAMENTO e TRATAMENTO DE RESPOSTAS A INCIDENTES	É o tempo em que a solução de gerenciamento deverá estar operacional com todos as ferramentas disponíveis, inclusive link de dados, interface WEB, DASHBORD e central 0800	∑ Minutos Disponíveis ----------x100 ∑ Minutos Contratados	Verificado através dos tickets de indisponibilidade da solução de gerenciamento registrados na solução de service desk e disponibilizados na Solução;	NA	1% do valor da parcela mensal do serviço a cada ponto percentual abaixo de 99%	99%
Dúvidas ou alteração de configuração (P3);	É o tempo para registro e abertura de incidente no Service Desk da CONTRATANTE /	∑ Chamados Registrados dentro do tempo	Verificado através dos tickets registrados na solução de Service	90% dos atendimentos realizados em até 30	1% do valor da parcela mensal do serviço a	90%

	CONTRATADA e identificar a causa raiz, tomando as medidas para a resolução do incidente (troubleshooting)em conformidade com os processos de incidente e mudança do CONTRATANTE e potencial de impacto na disponibilidade do serviço.	acordado ---------x100 ∑ Chamados Registrados	Desk para cada solução;	minutos	cada ponto percentual abaixo de 90%	
Serviço com performance inadequada (P2);				90% dos atendimentos realizados em até 1 hora e 30 minutos		90%
Serviço indisponível (P1);				90% dos atendimentos realizados em até 2 horas		90%

5. ELEMENTOS PARA GESTÃO DO CONTRATO

5.1. Papeis e Responsabilidade

ID	Papel	Entidade	Responsabilidade
1	Fiscal Técnico	SETIN – Diretor(a) da Divisão de Segurança da Informação	Confecção e assinatura do Termo de Recebimento Provisório, quando da entrega do objeto resultante de cada Ordem de Serviço ou de Fornecimento de Bens; Avaliação da qualidade dos serviços realizados ou dos bens entregues e justificativas, de acordo com os Critérios de Aceitação definidos em contrato; Identificação de não conformidade com os termos contratuais; Verificação da manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica. Verificação de manutenção das condições elencadas no Plano de Sustentação (Documento elaborado no planejamento da contratação, que visa garantir a continuidade do negócio durante e após a entrega da Solução de Tecnologia da Informação, bem como após o encerramento do contrato); Comunicar por escrito ao gestor do contrato qualquer falta cometida pela empresa contratada, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão levar a aplicação de sanção ou à rescisão contratual; Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato; Realizar pessoalmente a medição dos serviços contratados; Recusar serviço ou fornecimento irregular ou em desacordo com condições previstas em edital, na proposta da contratada e no contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados; Averiguar se é o contratado quem executa o contrato e certificar-se de que não existe cessão ou subcontratação fora das hipóteses legais; Verificar o cumprimento das normas trabalhistas por parte do contratado, a exemplo da jornada de trabalho, limitações de horas extras, descanso semanal, bem como da obediência às normas de segurança do trabalho, a fim de evitar acidentes com agentes administrativos, terceiros e empregados do contrato; Atestar a efetiva realização do objeto contratado para fins de pagamento das faturas correspondentes; Acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle da qualidade dos materiais, serviços e equipamentos a serem aplicados nos serviços.
2	Fiscal Requisitante do Contrato	SETIN – Chefia do Suporte Técnico	Avaliação da qualidade dos serviços realizados ou dos bens entregues e justificativas, de acordo com os Critérios de Aceitação definidos em contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Identificação de não conformidade com os termos contratuais, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato;

			Verificação da manutenção da necessidade, economicidade e oportunidade da contratação; Verificação de manutenção das condições elencadas no Plano de Sustentação (Documento elaborado no planejamento da contratação, que visa garantir a continuidade do negócio durante e após a entrega da Solução de Tecnologia da Informação, bem como após o encerramento do contrato), em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle da qualidade dos materiais, serviços e equipamentos a serem aplicados nos serviços, em conjunto com o Fiscal Técnico; Verificar o cumprimento das normas trabalhistas por parte do contratado, a exemplo da jornada de trabalho, limitações de horas extras, descanso semanal, bem como da obediência às normas de segurança do trabalho, a fim de evitar acidentes com agentes administrativos, terceiros e empregados do contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Comunicar por escrito ao gestor do contrato qualquer falta cometida pela empresa contratada, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão levar a aplicação de sanção ou à rescisão contratual, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato.
3	Fiscal Administrativo	SETIN – Diretor(a) da Divisão de Apoio da Secretaria de Tecnologia da Informação	Certificar-se do correto cálculo e recolhimento das obrigações trabalhistas, previdenciárias, e tributárias decorrentes do contrato; Proceder à obrigatória liquidação da despesa, mediante fatura de serviço devidamente atestada pelo fiscal técnico, para fins de apuração da origem e do objeto do que se deve pagar, da importância exata a ser paga e a quem se deve pagar para extinguir a obrigação, com base no contrato, na nota de empenho e nos comprovantes de entrega do material ou da efetiva prestação do serviço, em conformidade com o disposto nos arts. 62 e 63 da Lei nº 4.320, de 18 de março de 1964; Efetuar o controle da vigência, realizando comunicado ao fiscal técnico em tempo hábil, uma vez que este deverá controlar os prazos de execução, necessidades de prorrogações ou nova contratação, ficando o fiscal administrativo o controle da época de reajustamento dos preços contratados, tomando as providências cabíveis em tempo hábil junto à Divisão Central de Contratos e Convênios do TJCE, quando necessário; Verificar se a empresa contratada cumpriu com a garantia prevista no contrato.
4	Gestor do Contrato	SETIN – Secretário(a) de Tecnologia da Informação	Manter registro próprio, atualizado, das ocorrências relacionadas à execução do contrato; Acompanhar o cumprimento do cronograma de execução e dos prazos previstos; Determinar à contratada a regularização das falhas ou defeitos observados, assinalando prazo para correção; Relatar, por escrito, ao titular do órgão responsável, a inobservância de cláusulas contratuais ou quaisquer ocorrências que possam trazer dificuldades, atrasos, defeitos e prejuízos à execução da avença, em especial os que ensejarem a aplicação de penalidades; Comunicar ao titular do órgão responsável, apresentando as devidas justificativas, a eventual necessidade de acréscimos ou supressões de serviços, materiais ou equipamentos, identificadas no curso das atividades de fiscalização; Solicitar à contratada a substituição de empregado ou preposto da contratada e aprovar, previamente, mediante termo juntado ao processo, a substituição de iniciativa da contratada, quando assim exigir o contrato; Receber, definitivamente, por meio de ateste na nota fiscal/fatura ou

			documento equivalente, devidamente discriminado, obras, serviços e materiais; Acompanhar o prazo de vigência do contrato e manifestar-se, quando provocado pela Administração, sobre os aspectos de oportunidade, conveniência, razoabilidade e economicidade administrativa de realizar-se alteração, prorrogação ou rescisão do contrato, anexando, quando for o caso, documentação comprobatória;

6. DEVERES E RESPONSABILIDADES DA CONTRATANTE

6.1. Proporcionar todas as facilidades para a Contratada executar o fornecimento do objeto do presente Termo de Referência, permitindo o acesso dos profissionais da Contratada às suas dependências. Esses profissionais ficarão sujeitos a todas as normas internas do TJCE, principalmente as de segurança, inclusive àquelas referentes à identificação, trajes, trânsito e permanência em suas dependências;
6.2. Promover o acompanhamento e a fiscalização da execução do objeto do presente Termo de Referência, sob o aspecto quantitativo e qualitativo, anotando em registro próprio as falhas detectadas;
6.3. Comunicar prontamente à CONTRATADA qualquer anormalidade na execução do objeto, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no presente Termo de Referência;
6.4. Fornecer à Contratada todo tipo de informação interna essencial à realização dos fornecimentos e dos serviços;
6.5. Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando esta estiver em conformidade com os padrões de informação e qualidade exigidos;
6.6. Homologar os serviços prestados, quando estes estiverem de acordo com o especificado no Termo de Referência;
6.7. Efetuar o pagamento à CONTRATADA;

7. DEVERES E RESPONSABILIDADES DA CONTRATADA

7.1. Atender a todas as condições descritas no presente Termo de Referência e respectivo Contrato;
7.2. Manter as condições de habilitação e qualificação exigidas durante toda a vigência do Contrato;
7.3. Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, contribuições previdenciárias, impostos e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que estes não têm nenhum vínculo empregatício com o TJCE;
7.4. Responsabilizar-se pelo fornecimento do objeto deste Termo de Referência, respondendo civil e criminalmente por todos os danos, perdas e prejuízos que, por dolo ou culpa sua, de seus empregados, prepostos, ou terceiros no exercício de suas atividades, vier a, direta ou indiretamente, causar ou provocar à TJCE;
7.5. Obter todas as autorizações, aprovações e franquias necessárias à execução dos serviços, pagando os emolumentos prescritos por lei e observando as leis, regulamentos e posturas aplicáveis. É obrigatório o cumprimento de quaisquer formalidades e o pagamento, à sua custa, das multas porventura impostas pelas autoridades, mesmo daquelas que, por força dos dispositivos legais, sejam atribuídas à Administração Pública;
7.6. Não ceder ou transferir, total ou parcialmente, parte alguma do contrato. A fusão, cisão ou incorporação só será admitida com o consentimento prévio e por escrito do TJCE;
7.7. Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades objeto do Contrato, sem prévia autorização do TJCE;
7.8. Dar ciência, imediatamente e por escrito, de qualquer anormalidade que verificar na execução do objeto bem como prestar esclarecimentos que forem solicitados pelo TJCE;
7.9. Manter sigilo absoluto sobre informações, dados e documentos provenientes da execução do Contrato e também às demais informações internas do TJCE a que a Contratada tiver conhecimento;
7.10. Não deixar de executar qualquer atividade necessária ao perfeito fornecimento do objeto, sob qualquer alegação, mesmo sob pretexto de não ter sido executada anteriormente qualquer tipo de procedimento;
7.11. Somente desativar hardware, software e qualquer outro recurso computacional relacionado à execução do objeto mediante prévia autorização do TJCE;
7.12. Prestar qualquer tipo de informação solicitada pelo TJCE sobre os serviços contratados bem como fornecer qualquer documentação julgada necessária ao perfeito entendimento do objeto deste Termo de Referência;
7.13. Elaborar e apresentar documentação técnica dos fornecimentos e serviços executados nas datas aprazadas, visando sua homologação pelo TJCE;
7.14. Alocar profissionais devidamente capacitados e habilitados para os serviços contratados;
7.15. Providenciar a substituição imediata dos profissionais alocados ao serviço que, eventualmente, não

atendam aos requisitos deste Termo de Referência ou por solicitação do TJCE devidamente justificada;
7.16. Implementar rigorosa gerência de contrato com observância a todas as disposições constantes deste Termo de Referência;
7.17. Em até 10 (dez) dias após a assinatura do contrato, a CONTRATADA disporá de profissionais com capacidade técnica suficiente e necessária ao desempenho dos serviços Objeto do Contrato, exigindo-se:
7.17.1. Todos os profissionais deverão possuir experiência mínima comprovada de 03 (três) anos na área de Segurança da Informação e terem participado de projetos similares;
7.17.2. A equipe de profissionais envolvida para exercer as funções, deve possuir as seguintes certificações ou equivalentes:
7.17.2.1. 01 (uma) Certificação CISSP (Certified Information Systems Security Professional);
7.17.2.2. 01 (uma) Certificação PMI-PMP Project Management Professional ou PMI-ACP - Profissional Certificado em Métodos Ágeis, práticas e ferramentas e técnicas através de metodologias ágeis.
7.17.2.3. 01 (uma) Certificação em alguma solução de mercado em Firewall/VPN;
7.17.2.4. 01 (uma) Certificação em alguma solução de mercado em IPS – Intrusion Prevent System;
7.17.2.5. 01 (uma) Certificação em alguma solução de mercado em SIEM – Security Information and Event Management;
7.17.2.6. 01 (uma) Certificação em alguma solução de mercado em Mail Security;
7.17.2.7. 01 (uma) Certificação em alguma solução de mercado em Web Security;
7.17.2.8. 01 (uma) Certificação em alguma solução de mercado em Endpoint Security;
7.17.3. A comprovação de que os profissionais compõem o quadro permanente da licitante se fará mediante a apresentação de cópia da Carteira de Trabalho (CTPS) ou do contrato social da licitante, no caso de sócio, ou contrato de prestação de serviços pelo prazo de vigência do contrato.
7.17.4. A comprovação de que os profissionais são detentores de experiência se dará com o fornecimento de Atestado(s) de Capacidade Técnica (fornecido(s) por pessoa jurídica de direito público ou privado, em documento timbrado) e a comprovação de que os profissionais são detentores de conhecimento com apresentação de documentos comprobatórios de diplomas e das certificações exigidas.
7.18. Da Visita Técnica ao ambiente da CONTRATADA:
7.18.1. Em até 15 (quinze) dias, após a assinatura do contrato, 02 (dois) representantes da equipe de servidores do TJCE realizarão vistoria técnica ao ambiente do SOC da CONTRATADA, de forma a averiguar o atendimento aos requisitos do **IITEM 20.3** e seus subitens deste termo. Caso não esteja em conformidade a empresa terá o contrato rescindido.
7.18.2. Todos os custos da visita ao ambiente da CONTRATADA com passagens (FORTALEZA/DESTINO/FORTALEZA), estadia, translados e qualquer outro que seja necessário será da CONTRATADA, devendo ser considerado 02 (dois) participantes da CONTRATANTE para a realização da vistoria no ambiente.

8. FORMA DE ACOMPANHAMENTO DO CONTRATO

8.1. O acompanhamento e a fiscalização da execução do Contrato serão realizados por servidores do TJCE e designados como Fiscais do Contrato, os quais obedecerão às disposições de normas e resoluções internas do Tribunal, assim como o artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010.
8.2. Conforme alínea “a” do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, caberá à fiscalização providenciar elaboração do Plano de Inserção da contratada.
8.3. Conforme alínea “b” do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, deverá ser realizada reunião inicial com participação dos Fiscais do Contrato, do Representante Legal da Contratada (apresentando o Preposto da mesma) e demais intervenientes identificados.
8.4. Conforme item 2 da alínea “b” do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, entrega, por parte da Contratada, a pauta da reunião mencionada acima contemplará a entrega do Termo de Compromisso e do Termo de Ciência.
8.5. É importante informar que este Termo de Referência é fruto da sequência de trabalhos da etapa de Planejamento da Contratação conforme a INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, a qual dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional.
8.6. Conforme a instrução normativa acima, os documentos de planejamento (Análise de Viabilidade, Plano de Sustentação, Análise de Riscos e Estratégia de Contratação) foram devidamente elaborados e se encontram aprovados.

9. METODOLOGIA DE AVALIAÇÃO DA QUALIDADE

9.1. Todo o trabalho realizado pela CONTRATADA estará sujeito à avaliação técnica, sendo homologado quando estiver de acordo com o padrão de qualidade exigido pelo Órgão e de acordo com os prazos definidos;

9.2. A documentação técnica gerada deverá seguir o padrão definido pelo TJCE ou pelo CONTRATANTE, sendo devidamente verificada por responsável técnico e atestada pelo Fiscal do Contrato. O padrão de documentação técnica deverá ser informado na reunião inicial entre a CONTRATANTE e a CONTRATADA. A reunião inicial ocorrerá em até 07 (sete) dias corridos após o TJCE emitir a ordem de fornecimento.

10. LEVANTAMENTO DE QUANTITATIVOS

Bem/Serviço	Estimativa	Forma de Estimativa
Gerenciamento de appliance Firewall/VPN no site principal do tipo CISCO ASA 5550	03	Quantidade de dispositivos a serem gerenciados por mês
Gerenciamento de appliance firewall/VPN nos sites remotos do tipo CISCO ASA 5505	26	Quantidade de dispositivos a serem gerenciados por mês
Gerenciamento de appliance firewall/VPN nos sites remotos do tipo a ser adquirido pelo TJCE	190	Previsão da quantidade de dispositivos a serem adquiridos durante o prazo contratual.
Gerenciamento de appliance IPS no site principal do tipo CISCO IPS-4260	02	Quantidade de dispositivos a serem gerenciados por mês
Gerenciamento de appliance SIEM no site principal do tipo CISCO Mars	01	Quantidade de dispositivos a serem gerenciados por mês
Tratamento de Respostas a incidente - Firewall/VPN do tipo CISCO ASA 5550/5505	01	Quantidade de soluções a serem tratadas quanto a respostas a incidente por mês
Tratamento de Respostas a incidente - IPS no site principal do tipo CISCO IPS-4260	01	Quantidade de soluções a serem tratadas quanto a respostas a incidente por mês
Tratamento de Respostas a incidente - SIEM do tipo CISCO Mars	01	Quantidade de soluções a serem tratadas quanto a respostas a incidente por mês
Tratamento de Respostas a incidente - Mail Security do tipo CISCO Ironport C160	01	Quantidade de soluções a serem tratadas quanto a respostas a incidente por mês
Tratamento de Respostas a incidente - Web Security tipo McAfee Web Gateway	01	Quantidade de soluções a serem tratadas quanto a respostas a incidente por mês
Tratamento de Respostas a incidente - EndPoint Security do tipo Kaspersky Security Center	01	Quantidade de soluções a serem tratadas quanta a respostas a incidente por mês

11. CONDIÇÕES PARA PAGAMENTO

11.1. Os faturamentos dos serviços, executados pela CONTRATADA, serão efetuados conforme abaixo;
11.1.1. A CONTRATANTE deverá emitir ordem de serviço para cada atividade a ser iniciada, conforme a quantidade das unidades discriminadas na Ordem de Serviço;
11.1.2. Os serviços poderão ser faturados após a solicitação de pagamento por parte da CONTRATADA e entrega/aceite do Relatório de Níveis de Serviços;
11.1.3. Quando houver divergência entre a solicitação de pagamento apresentada e a prestação dos serviços verificada pela CONTRATANTE, a parte incontrovérsia poderá ser faturada ficando a parte controversa para ser discutida e COMPENSADA na fatura posterior.
11.2. As notas fiscais deverão ser emitidas em nome do Fundo de Especial de Reaparelhamento e Modernização do Judiciário – FERMOJU, CNPJ nº. 41.655.846/0001-47;
11.3. O pagamento será realizado através de depósito bancário nas agências do BANCO BRADESCO S/A, devendo as faturas ou notas fiscais, referentes à execução dos serviços previamente autorizadas, serem entregues até o dia 10 (dez) do mês subsequente à prestação dos mesmos, e estas deverão ser pagas, sem quaisquer acréscimos e atualização monetária, até o último dia útil do referido mês, devidamente atestado pelo(s) setor(es) competente(s) deste Tribunal de Justiça;
11.4. O valor do pagamento será aquele apresentado na Nota Fiscal, conforme definido no contrato e devidamente atestado, descontadas as glosas, conforme definido neste Termo de Referência;
11.5. O Tribunal de Justiça reserva-se o direito de recusar o pagamento, no ato da ATESTAÇÃO, caso o objeto não esteja em conformidade com as condições deste instrumento;
11.6. Nenhum pagamento será efetuado à empresa vencedora do certame antes de paga à multa que por ventura lhe tenha sido aplicada;
11.7. Nenhum pagamento será efetuado à CONTRATADA na pendência de qualquer uma das situações abaixo especificadas, sem que isso gere direito a alteração de preços ou compensação financeira: Apresentação da Certidão Negativa de Débito da Previdência Social – CND; Apresentação de Certidão Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida Ativa da União; Apresentação de Certidão Negativa de Débitos junto aos Governos Estadual e Municipal; Apresentação de Certificado de Regularidade do FGTS – CRF; Certidão Negativa de Débitos Trabalhistas.
11.8. Caso existam penalidades a serem aplicadas a CONTRATADA será notificada, conforme especificado no item **MECANISMOS FORMAIS DE COMUNICAÇÃO**, sendo o prazo do atesto da respectiva ORDEM DE SERVIÇO interrompido até a entrega das justificativas pela CONTRATADA;

12. GARANTIA CONTRATUAL

12.1. Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive pagamento de multas eventualmente aplicadas, a licitante prestará garantia no percentual de 5% (cinco por cento) do valor total do contrato, podendo a CONTRATADA optar por qualquer das modalidades previstas no art. 56 da Lei 8.666/93, a saber:
12.1.1. Caução em dinheiro ou títulos da dívida pública, cuja exigibilidade não seja contestada pelo TJCE;
12.1.2. Quando se tratar de caução em dinheiro, deverá ser recolhido na Secretaria de Finanças do TJCE;
12.1.3. Seguro garantia;
12.1.4. Fiança bancária.
12.2. Em se tratando de fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil;
12.3. Se o valor da garantia for utilizado em pagamento de qualquer obrigação, a CONTRATADA deverá re-integralizar o seu valor, no prazo não superior a 10 (dez) dias corridos, contados da data em que for notificada;
12.4. A não apresentação da garantia até a assinatura contratual significará recusa à assinatura do contrato, ensejando aplicação das sanções previstas;
12.5. No caso de rescisão do contrato, a garantia se presta a cobrir prejuízos comprovados;

13. PROPRIEDADE, SIGILO, RESTRIÇÕES

13.1. A contratada cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do art. 111, da Lei Federal N.º 8.666/93, combinado com o art. 4.º, da Lei Federal N.º 9.609/98, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência dos serviços contratados, entendendo-se por resultados quaisquer estudos, relatórios, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presenta contratação, em papel ou em mídia eletrônica;
13.2. Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a CONTRATADA, zelar por si, por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados;
13.3. A obrigação assumida de Confidencialidade permanecerá válida durante o período de vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA, previstas no CONTRATO e na legislação pertinente;
13.4. Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados, a qualquer título, da equipe executante do Objeto deste Termo de Referência, a assinatura do ANEXO 09 - TERMO DE COMPROMISSO, bem como a assinatura do ANEXO 08 – TERMO DE CIÊNCIA onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.

14. MECANISMOS FORMAIS DE COMUNICAÇÃO

Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade
Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Através de telefone, e-mail, presencial, relatórios, documentos de texto, planilhas, slides, e-mail, sítios da internet, PDF (*Portable Document Format*): documento em formato portável.	Quando necessário
Comunicações oficiais	Contratada/ Contratante	Contratante/ Contratada	Ofício por correspondência	Quando necessário

15. ESTIMATIVA DOS PREÇOS UNITÁRIOS

ITEM	UND	QTD	DESCRIÇÃO	VALOR UNIT. (R$)	VALOR TOTAL MENSAL (R$)	VALOR TOTAL ANUAL (R$)
SERVIÇO DE ADMINISTRAÇÃO, GERENCIAMENTO E MONITORAMENTO DOS ATIVOS DE SEGURANÇA						
1	UND	03	Gerenciamento de appliance Firewall/VPN no site principal do tipo CISCO ASA 5550	R$ 4.221,62	R$ 12.664,86	R$ 151.978,32
2	UND	26	Gerenciamento de appliance firewall/VPN nos sites remotos do tipo CISCO ASA 5505	R$ 84,07	R$ 2.185,82	R$ 26.229,84

3	UND	190	Gerenciamento de appliance firewall/VPN nos sites remotos do tipo a ser adquirido pelo TJCE	R$ 84,07	R$ 15.973,30	R$ 191.679,60
4	UND	02	Gerenciamento de appliance IPS no site principal do tipo CISCO IPS-4260	R$ 3.458,14	R$ 6.916,28	R$ 82.995,36
5	UND	01	Gerenciamento de appliance SIEM no site principal do tipo CISCO Mars	R$ 8.078,89	R$ 8.078,89	R$ 96.946,68
SERVIÇO DE TRATAMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA						
6	SOL	01	Tratamento de Respostas a incidente - Firewall/VPN do tipo CISCO ASA 5550/5505	R$ 13.180,48	R$ 13.180,48	R$ 158.165,76
7	SOL	01	Tratamento de Respostas a incidente - IPS no site principal do tipo CISCO IPS-4260	R$ 2.688,51	R$ 2.688,51	R$ 32.262,12
8	SOL	01	Tratamento de Respostas a incidente - SIEM do tipo CISCO Mars	R$ 3.856,18	R$ 3.856,18	R$ 46.274,16
9	SOL	01	Tratamento de Respostas a incidente - Mail Security do tipo CISCO Ironport C160	R$ 4.888,83	R$ 4.888,83	R$ 58.665,96
10	SOL	01	Tratamento de Respostas a incidente - Web Security tipo McAfee Web Gateway	R$ 11.557,30	R$ 11.557,30	R$ 138.687,60
11	SOL	01	Tratamento de Respostas a incidente - EndPoint Security do tipo Kaspersky Security Center	R$ 13.327,83	R$ 13.327,83	R$ 159.933,96
					TOTAL	**R$ 1.143.819,36**

Obs: Valores obtidos através da média de 03 propostas da pesquisa mercadológica. Valores arrendondados em função das divisões.

16. ADEQUAÇÃO ORÇAMENTÁRIA

Fonte	**Ação**	**PPA - 2012/2015**
Fundo Especial de Reaparelhamento e Modernização do Poder Judiciário do Estado do Ceará (FERMOJU)	**Manutenção e funcionamento de TI**	**Iniciativa 00001 - Ampliação e Modernização da infraestrutura do Tribunal de Justiça do Estado do Ceará**
Gerenciamento de appliance Firewall/VPN no site principal do tipo CISCO ASA 5550		**Serviço**
Gerenciamento de appliance firewall/VPN nos sites remotos do tipo CISCO ASA 5505		**Serviço**
Gerenciamento de appliance firewall/VPN nos sites remotos do tipo a ser adquirido pelo TJCE		**Serviço**
Gerenciamento de appliance IPS no site principal do tipo CISCO IPS-4260		**Serviço**
Gerenciamento de appliance SIEM no site principal do tipo CISCO Mars		**Serviço**
Tratamento de Respostas a incidente - Firewall/VPN do tipo CISCO ASA 5550/5505		**Serviço**
Tratamento de Respostas a incidente - IPS no site principal do tipo CISCO IPS-4260		**Serviço**
Tratamento de Respostas a incidente - SIEM do tipo CISCO Mars		**Serviço**
Tratamento de Respostas a incidente - Mail Security do tipo CISCO Ironport C160		**Serviço**
Tratamento de Respostas a incidente - Web Security tipo McAfee Web Gateway		**Serviço**
Tratamento de Respostas a incidente - EndPoint Security do tipo Kaspersky Security Center		**Serviço**
Código do Projeto		**PJSETIN2012028**
Código Financeiro		**1112012028**
Regionalização da Despesa		**Fortaleza/CE**
Exercício 2013/2014		**R$ 1.143.819,36**

17. SANÇÕES ADMINISTRATIVAS

17.1. Atendendo ao Art. 15, inciso III, alínea "h" da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010 e conforme os Arts. 86, 87 e 88 da Lei No 8.666 de 1993, seguem, abaixo, definições claras e detalhadas das sanções administrativas a serem aplicadas a esta contratação com vinculação por Termo de Contrato.
17.2. Pela inexecução total ou parcial do objeto definido neste Termo de Referência, o TJCE poderá, garantida a prévia defesa, aplicar à Contratada, as sanções a seguir, de acordo com o grau do prejuízo causado pelo descumprimento das respectivas obrigações:
17.2.1. Advertência escrita quando se tratar de infração leve, a juízo da fiscalização, no caso de descumprimento das obrigações e responsabilidades assumidas no contrato ou ainda no caso de outras ocorrências que possam acarretar prejuízos ao TJCE desde que não caiba a aplicação de sanção mais grave;
17.2.2. 0,3% (três décimos por cento) por dia sobre o valor dos serviços entregues com atraso, até o percentual de 8% (oito por cento). Decorridos 30 (trinta) dias de atraso o TJCE poderá decidir pela rescisão, em razão da inexecução total.
17.2.3. 1% (um por cento) por dia sobre o valor da garantia contratual, pela não apresentação/atualização, até o percentual de 10% (dez por cento)no prazo estabelecido neste instrumento, da garantia de execução contratual.
17.2.4. 0,5% (meio por cento) por evento sobre o valor global atualizado do contrato, pela não manutenção das condições de habilitação e qualificação exigidas no instrumento convocatório.
17.2.5. 10 % (dez por cento) sobre o valor do contrato, nas hipóteses de rescisão contratual por inexecução total do contrato.
17.2.6. Suspensão temporária de participar em licitação e impedimento de contratar com a Administração, pelo prazo não superior a 5 (cinco) anos;
17.2.7. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos que determinaram sua punição ou até que seja promovida a sua reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.
17.3. As eventuais penalidades por descumprimento de Acordos de Níveis Mínimos de Serviços (NMS's) serão calculadas de acordo com o **ITEM 4.7 - Tabela de Acordo de Níveis Mínimos de Serviços** e abatidas na fatura do mês da prestação de serviços, conforme a validação do Relatório de Níveis de Serviços.

18. DA VIGÊNCIA CONTRATUAL E REAJUSTE

18.1. Da Vigência Contratual

18.1.1 O contrato deverá ter vigência iniciando-se na data de sua assinatura e vigorará por 12 meses, podendo ser prorrogado, tudo em conformidade com o disposto no Art. 57, inciso II, da Lei Federal n° 8.666/1993, por ser considerado pela CONTRATANTE, serviço de natureza contínua.

18.2. Do Reajuste dos Preços

18.2.1 Após 12 meses da data de apresentação da proposta e o contrato sendo prorrogado, a CONTRATADA, mediante justificativa, poderá solicitar reajuste com base na variação do IPCA.
18.2.2 Ficará a critério do TJCE concordar ou não, integral ou parcialmente, com o reajuste de preços propostos.

19. DA VISTORIA TÉCNICA PRÉVIA AO AMBIENTE DA CONTRATANTE

19.1. A licitante deverá realizar vistoria técnica nas instalações do Tribunal, em dias úteis durante o horário de 09:00 às 17:00 horas.
19.2. A vistoria se faz necessária e obrigatória, pois a licitante obterá informações extremamente importantes e sigilosas sobre o atual Tratamento de Incidentes de Segurança da Informação do Tribunal de Justiça onde deverá se inteirar de todos os aspectos referentes à execução dos serviços para apresentação de sua proposta.
19.3. A licitante deverá manter sigilo absoluto sobre informações, dados e documentos provenientes da vistoria técnica e também às demais informações internas do TJCE a que a licitante tiver conhecimento.
19.4. O agendamento da vistoria deverá ser previamente efetuado nos telefones de contatos do TJCE, mencionando as informações de contato da Empresa (razão social, endereço e telefone) e de seu representante (nome completo e telefone) o qual efetuará a vistoria.
19.4.1. TJCE: na Av. General Afonso Albuquerque Lima, S/N. - Cambeba CEP: 60822-325, Fortaleza-CE, por meio dos telefones: (85) 3207-7756 / 6850, na Secretaria de tecnologia da Informação.
19.5. A vistoria deverá ser agendada e realizada em no máximo 02 (dois) dias úteis antes da abertura das propostas.

19.6. Durante a vistoria, será dado acesso às dependências do Tribunal.
19.7. Para todos os efeitos, considerar-se-á que a Empresa tem pleno conhecimento da natureza e do escopo dos serviços, não se admitindo, posteriormente, qualquer alegação de desconhecimento desses elementos de contratação.
19.8. Efetuada a vistoria será Lavrado, por representante da equipe técnica do TJCE designado para tanto, o respectivo Atestado de Vistoria, conforme modelo, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação.

20. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

20.1. Da Proposta de Preço

20.1.1. A proposta deverá conter obrigatoriamente os seguintes elementos:
20.1.1.1. Preço unitário por item, em moeda corrente nacional, cotados com apenas duas casas decimais, expressos em algarismos e por extenso, sendo que, em caso de divergência entre os preços expressos em algarismos e por extenso, serão levados em consideração os últimos;
20.1.1.2. Não deve conter cotações alternativas, emendas, rasuras ou entrelinhas;
20.1.1.3. Deve fazer menção ao número do pregão e do processo licitatório;
20.1.1.4. Deve ser datada e assinada na última folha e rubricadas nas demais, pelo representante legal da empresa;
20.1.1.5. Deve conter na última folha o número do CNPJ da empresa;
20.1.1.6. Deve informar o prazo de validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, contados da data de entrega da mesma;
20.1.1.7. Indicação do nome do banco, número da agência, número da conta-corrente, para fins de recebimento dos pagamentos;
20.1.2. A proposta de preços deverá vir acompanhada, ainda, de:
20.1.2.1. Atestado de Capacidade Técnica e Declaração que disporá dos profissionais com capacidade técnica conforme **ITEM 7.17** após a assinatura do contrato.

20.2. Da Qualificação Técnica

20.2.1. A licitante será habilitada a participar do certame com a apresentação de Atestado de Vistoria a ser fornecido pelo TJCE e Atestado(s) de Capacidade Técnica, a ser(em) fornecido(s) por pessoa jurídica de direito público ou privado, em documento timbrado, e que comprove(m) a aptidão da licitante para desempenho de atividade pertinente e compatível com o objeto da licitação, contendo:
20.2.1.1. Serviços de natureza e vulto compatíveis com o objeto ora licitado e que façam explícita referência pelo menos às parcelas de maior relevância técnica e valor significativo, que permitam estabelecer, por comparação, proximidade de características funcionais técnicas, dimensionais, quantitativas e qualitativas com o objeto da presente licitação, mencionando explicitamente os seguintes serviços:
20.2.1.2. Serviços de SOC – Security Operation Center (Centro de Operações de Segurança).
20.2.1.3. Serviços gerenciados de segurança para Firewall/VPN, IPS, SIEM;
20.2.1.4. Serviços de Tratamento de Respostas a Incidente de Segurança para Firewall/VPN, IPS, SIEM, Mail Security, Web Security, EndPoint Security;
20.2.2. Serão aceitos o somatório de atestados para comprovação;
20.2.3. A Administração se resguarda no direito de diligência junto à pessoa jurídica do Atestado/Declaração de Capacidade Técnica, visando obter informação sobre o serviço prestado e cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatórios do conteúdo declarado.

20.3. Do Ambiente da Contratada

20.3.1. A CONTRATADA, após a assinatura do contrato, deverá comprovar possuir infraestrutura de alta disponibilidade e tolerância a falhas com, no mínimo, 01 (um) SOC – Security Operation Center (Centro de Operações de Segurança), localizados no Brasil. O SOC deverá ser capaz de lidar isoladamente com todos os clientes da CONTRATADA e atender aos seguintes requisitos mínimos:
20.3.1.1. Estar localizado em prédio comercial que possua gerador de energia para as áreas privativas. O gerador deve ser acionado automaticamente em casso de falta de energia e fornecer energia estabilizada em até 2 minutos após a partida. Os geradores devem suportar a demanda das instalações por até 12 horas sem necessidade de reabastecimento;
20.3.1.2. Efetue registro dos visitantes com identificação individual e controle digital de entrada e saída;
20.3.1.3. Possua circuito interno de registro e gravação de imagem em todas as áreas de circulação;
20.3.1.4. Esteja localizado próximo a vias de grande circulação com acesso imediato a transportes públicos de mais de uma modalidade;
20.3.1.5. Funcione em regime 24 x7;
20.3.1.6. Possua sistema de refrigeração de conforto central;
20.3.1.7. Registrar todas as entradas e saídas mantendo o registro armazenado para consulta por mais de 90 dias;
20.3.1.8. Filmar permanentemente toda a área armazenada mantendo as imagens armazenadas por mais

de 90 dias;
20.3.1.9. Possuir UPS que suporte todos os equipamentos essenciais ao funcionamento por, pelo menos, 30 minutos;
20.3.1.10. Estar conectado ao Data Center que hospeda os sistemas de suporte técnico, monitoramento, administração e gerenciamento através de múltiplas conexões de rede local ou WAN, de forma que a falha de uma conexão isoladamente não afete o acesso aos mesmos;
20.3.1.11. Possuir estrutura central para visualização dos painéis dos sistemas de suporte técnico, monitoramento, administração e gerenciamento que permita que todos os profissionais visualizem eventos relevantes simultaneamente.
20.3.1.12. Possuir dispositivos redundantes para fornecer energia elétrica e controle de temperatura. Cada um destes dispositivos deve ter capacidade para manter a operação isoladamente em caso de manutenção planejada ou falha. Os dispositivos que devem ser considerados nessa especificação são:
20.3.1.12.1. Transformadores isoladores;
20.3.1.12.2. UPS;
20.3.1.12.3. Geradores;
20.3.1.12.4. Torres de refrigeração;
20.3.1.12.5. Chillers;
20.3.1.12.6. CRAC units;
20.3.1.12.7. Roteadores;
20.3.1.12.8. Swicthes de core;
20.3.1.12.9. Swicthes de distribuição.
20.3.1.13. Possuir caminhos de distribuição de energia elétrica, fluidos e gases para refrigeração e conexões de rede local redundantes de modo que um caminho permaneça ativo e o outro possa ser utilizado como alternativa em caso de manutenção planejada ou falha. Os sistemas de distribuição que devem ser considerados nessa especificação são:
20.3.1.13.1. Cabine para recebimento de energia externa;
20.3.1.13.2. Cabeamento de transmissão de energia;
20.3.1.13.3. Quadros de distribuição;
20.3.1.13.4. Dutos de água gelada;
20.3.1.13.5. Cabos para conexões de rede.
20.3.1.14. Possuir múltiplas entradas independentes para fornecimento de energia elétrica. Cada entrada para fornecimento de energia elétrica deve ser capaz de isoladamente suportar a operação do Data Center;
20.3.1.15. Possuir múltiplas conexões independentes para acesso à Internet. Cada conexão para acesso à Internet deve ser capaz de isoladamente suportar a operação do Data Center;
20.3.1.16. Os ativos de TI empregados no monitoramento (servidores, rede, software, etc.) deverão estar hospedados em ambiente com as seguintes características mínimas:
20.3.1.16.1. Possuir sistemas redundantes para armazenamento de dados e alimentação de energia;
20.3.1.16.2. Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o prazo do CONTRATO. Após este período deverão ser disponibilizadas para o TJCE, em mídia magnética ou via rede, e em seguida eliminadas da base de dados da LICITANTE;
20.3.1.16.3. Estar configurados de forma que a falha de nenhum dos equipamentos isoladamente interrompa o funcionamento dos sistemas;

20.4. Modalidade de Licitação

20.4.1. A modalidade de licitação sugerida deve ser o Pregão Eletrônico, considerando se tratar de bem e serviço comuns, nos termos da lei Federal n° 10.520/2002.

20.5. Tipo de Licitação

20.5.1. A licitação será do tipo menor preço global. Os valores máximos aceitáveis, tanto unitários quanto global, estão descritos no item **ESTIMATIVA DE PREÇO.**

20.6. Condições de Participação

20.6.1. Não será admitida a participação de dois ou mais LICITANTES em regime de consórcio.

LOTE 02

1. DESCRIÇÃO DA SOLUÇÃO

1.1 OBJETIVO

1.1.1 Estruturação da segurança da informação do TJCE, com o fornecimento de software de GRC – Governança, Riscos e Compliance, para automatizar a Gestão de Segurança da Informação, incluindo levantamentos, inventários, diagnósticos, análises, avaliações, testes, e tratamento dos ativos, com a gestão da continuidade de negócios e elaboração dos planos de contingência, com divulgação, planejamento, treinamento, elaboração e revisão dos normativos para sua implementação.

1.2 FORNECIMENTO E IMPLANTAÇÃO DE SOFTWARE de GRC – GOVERNANÇA, RISCOS E COMPLIANCE PARA AUTOMATIZAR A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

1.2.1 Implementar ferramentas para automatizar a gestão da segurança da informação, integrando as ações, permitindo o inventário dos processos, indicadores, documentos das normas, processos, políticas, análises, avaliação e tratamento de riscos, geração de recomendações e planos de ação e acompanhamento através de workflow para gestão de incidentes, tratamento das não conformidades e gestão de alertas.
1.2.2 Os softwares deverão ter interfaces e manuais no idioma Português (Brasil), permitindo a customização dos relatórios.
1.2.2.1 O software deverá ser instalado no ambiente a ser disponibilizado pelo TJCE.
1.2.2.2 Deverão ser entregues como produtos da instalação os seguintes itens:
1.2.2.2.1 Relatório de instalação do Software.
1.2.2.2.2 Documento que comprove a licença de uso do software.
1.2.2.2.3 CD de instalação do software.
1.2.2.2.4 Manual do Software em Português (Brasil).

1.2.3 BENEFÍCIOS:

1.2.3.1 Conduzir de forma otimizada projetos de análise de Gaps em Governança, Riscos e Compliance.
1.2.3.2 Criar Risk Scorecard, fornecendo visão executiva dos Riscos, incluindo índices e métricas que facilitam estabelecer critérios e apoiar a tomada de decisões.
1.2.3.3 Obter resultados precisos no processo de conformidade com normas e regulamentações internacionais e de mercado.
1.2.3.4 Consolidar os Riscos permitindo priorizar investimentos conforme a importância de cada ativo para a organização Acompanhar a evolução dos Riscos.
1.2.3.5 Gerenciar de forma centralizada Riscos e Compliance, incluindo a evolução histórica.
1.2.3.6 Realizar auditorias mais eficientes e com menores custos.
1.2.3.7 Gerenciar os requisitos de segurança em múltiplas auditorias, eliminando custos redundantes e controles desnecessários.
1.2.3.8 Apoiar a implementação dos requisitos de Certificação para SOx, PCI DSS, ISO 27002, ISO 27001, BS 25999, CobiT, Basiléia II, BITS/FISAP e outros.
1.2.3.9 Apoiar a gestão de Planos de Continuidade facilitando a manutenção e recuperação rápida das informações e procedimentos, alinhada à norma ABNT NBR ISO 22301:2013.
1.2.3.10 Facilitar a Gestão de Eventos e Incidentes.

1.2.4 REQUISITOS DO SOFTWARE

1.2.4.1 Os requisitos do software serão avaliados conforme a sua capacidade de atender aos quesitos da estrutura de implementação dos processos automatizados de Segurança da Informação.
1.2.4.2 Deve ser baseado em padrões e normas internacionais, como: ABNT ISO 27000, ABNT ISO/IEC Guia 73:2005, ABNT ISO 27005, ABNT 15999, NBR ISO 31000:2009 e ABNT NBR ISO 22301:2013.
1.2.4.3 Deve possuir recurso de auditoria das atividades realizadas e permitir a proteção de dados com criptografia.
1.2.4.4 Deve ser totalmente web não requerendo instalações de agentes ou clientes nas estações de trabalho.
1.2.4.5 Todas as mensagens devem ser no idioma Português (Brasil).
1.2.4.6 Deve possuir suporte web integrado ao software em idioma Português (Brasil).
1.2.4.7 Deve possuir área dedicada ao usuário, onde sejam possíveis:
1.2.4.7.1 Consultar pendências.
1.2.4.7.2 Receber corporativas administradas pelos gestores.
1.2.4.7.3 Visualizar perfis e acessos aos sistemas.
1.2.4.8 Deve inventariar os processos de SI, os indicadores recomendados de SI, os documentos das normas processos e políticas de SI e os ativos críticos de TI e de SI.
1.2.4.9 Deve realizar a gestão de ativos considerando: pessoas, equipamentos, edificações, processos de

negócio e ativos definidos pelos usuários. Deve permitir a criação de atributos conforme os tipos de ativos.
1.2.4.10 Deve possuir definição de política de senha como: tamanho, tipo de caracteres que deverão ser utilizados, validade, tempo para time-out e número de tentativas inválidas para que o usuário seja bloqueado.
1.2.4.11 Deve possuir mecanismos de concessão de permissões na solução com base nos perfis e papéis exercidos pelos usuários.
1.2.4.12 Deve possuir perfis de acesso por usuários com funções de gestão, administrativas e operacionais.
1.2.4.13 Deve ter a capacidade para realização do gerenciamento dos elementos da organização, considerando:
1.2.4.13.1 Visualizar, inserir, editar e excluir elementos do inventário e seus atributos.
1.2.4.13.2 Visualizar com estruturação em árvore e os ativos cadastrados.
1.2.4.13.3 Possuir consultas para todas as informações registradas no inventário.
1.2.4.13.4 Integrar os ativos com os processos de negócios a eles vinculados.
1.2.4.14 Deve permitir a gestão dos ativos cadastrados, sendo capaz de:
1.2.4.14.1 Incluir, editar ou deletar as áreas físicas da organização ou lógicas, processos, grupos de sistemas, dentre outras visões que permitam a organização dos componentes de informação.
1.2.4.15 Definir os responsáveis, por cada área da estrutura funcional, obtendo ainda, o cadastro do e-mail, telefone, função, dentre os outros aspectos relevantes.
1.2.4.16 Definir os responsáveis por área da estrutura funcional, com a finalidade de perfil de acesso.
1.2.4.17 Incluir os componentes de informação tecnológicos, humanos, processuais e ambientais em cada área da estrutura funcional.
1.2.4.18 Definir os valores de grau de importância em cada item inventariado.
1.2.4.19 Deve gerar informações consolidadas sobre análise de riscos e conformidade originadas das análises, fiscalizações, inspeções e auditorias.
1.2.4.20 Possuir base de conhecimento que permite realizar análise de riscos nos ativos de tecnologia da informação possuindo as bases de conhecimento devendo conter no mínimo 30 controles relacionados para cada um dos itens relacionais a seguir.
1.2.4.20.1 Ativos envolvidos: processos, pessoas, tecnologias e ambientes.
1.2.4.21 Deve permitir o monitoramento das respostas às análises de forma consolidada, possuindo:
1.2.4.21.1 A situação das respostas aos itens inventariados.
1.2.4.21.2 Situação dos dados dessas análises (índice de respostas, indicadores e controle).
1.2.4.22 Deve permitir a automatização da análise de controles do TJ-CE através da criação de questionários que sejam aplicados pela estrutura de controle ou encaminhada manualmente por email para as áreas.
1.2.4.23 Deve permitir atribuição de responsabilidades sobre análises efetuadas.
1.2.4.24 Deve permitir a visualização dos percentuais de completude da gestão de riscos.
1.2.4.25 Deve permitir a visualização gráfica do “status” da gestão de riscos.
1.2.4.26 Deve permitir a criação de filtros dinâmicos aos itens da gestão de riscos.
1.2.4.27 Deve permitir avaliação das não conformidades identificadas nas análises, decidindo se deverão ser encaminhados para tratamento.
1.2.4.28 Deve permitir que os itens em tratamento possam ser analisados por meio de gráficos e informações estatísticas.
1.2.4.29 Deve permitir o acompanhamento do tratamento dos itens e sua avaliação perante a simulação de tratamento.
1.2.4.30 Deve permitir a inserção de modelos de análises (normas, legislação, políticas, instruções) e sua associação aos itens criados nas bases de conhecimento.
1.2.4.31 Deve possuir bases de conhecimento de melhores práticas de análise de segurança física em datacenter e edificações que guardem ativos de tecnologia da informação.
1.2.4.32 Deve possuir bases de conhecimento com a análise de riscos das aplicações baseada na norma ISO 15403.
1.2.4.33 Deve permitir a análise integrada à avaliação de riscos em TI.
1.2.4.34 Deve permitir cadastrar os processos críticos.
1.2.4.35 Deve implementar o método de cálculo do BIA.
1.2.4.36 Deve possuir questionários automatizados ou manuais para que os usuários pesquisem a relevância.
1.2.4.37 Deve emitir o relatório de BIA (Análise de Impacto no Negócio).
1.2.4.38 Deve possuir recursos de armazenar as referências a informações consideradas críticas e vinculá-los a ativos.
1.2.4.39 Deve permitir que estes ativos sejam classificados conforme a política de classificação de informação.
1.2.4.40 Deve emitir relatórios e permitir consultas para que os usuários conheçam a classificação de cada informação.
1.2.4.41 Deve permitir a implementação dos recursos exigidos pela legislação de acesso a informação que

a TJ-CE deva atender.
1.2.4.42 Deve cadastrar os processos críticos definidos pela atividade de BIA.
1.2.4.43 Deve possuir recursos de gestão e aprovação de documentos por diferentes colaboradores através de workflow.
1.2.4.44 Deve permitir o armazenamento e consulta dos planos de continuidade de negócios, vinculando-os a ativos e processos.
1.2.4.45 Deve controlar a versão dos planos gerados.
1.2.4.46 Deve permitir a simulação dos planos a partir de testes de mesa automatizados em workflow.
1.2.4.47 Deve atender as exigências da norma ABNT 15999.
1.2.4.48 Deve realizar a gestão de incidentes através de workflow.
1.2.4.49 Deve armazenar os documentos de políticas e permitir consultas conforme o perfil dos usuários.
1.2.4.50 Deve permitir o armazenamento de conhecimento, procedimentos e práticas de testes de invasão do ambiente do TJ-CE.
1.2.4.51 Deve possuir recursos de workflow para encaminhamento e monitoramento da implementação das recomendações.
1.2.4.52 Implementar Workflow de Gestão de Incidentes.
1.2.4.53 Deve permitir o cadastro de ações com no mínimo os seguintes itens:
1.2.4.53.1 Descritivo da ação.
1.2.4.53.2 Resumo (Título).
1.2.4.53.3 Grau de urgência no tratamento da ação.
1.2.4.53.4 Grau de severidade para o processo.
1.2.4.53.5 Atribuição do responsável a ação.
1.2.4.54 Deve possuir controle de acesso para usuários e perfis.
1.2.4.55 Deve possuir a possibilidade de mensuração da ação conforme critérios do TJ-CE.
1.2.4.56 Definição de prazo de conclusão da ação.
1.2.4.57 Deve permitir o acompanhamento das ações, com os seguintes atributos:
1.2.4.57.1 Permitir incluir novas ações.
1.2.4.57.2 Possibilidade de fechar a ação.
1.2.4.57.3 Possibilidade de anexar arquivos como evidência.
1.2.4.58 Deve permitir filtros dinâmicos nas ações;
1.2.4.59 Deve permitir a geração dos seguintes relatórios das ações:
1.2.4.59.1 Por status da ação (aberta, fechada, etc.).
1.2.4.59.2 Por data (Dia de abertura, fechamento, atualização).
1.2.4.59.3 Pelo grau de urgência.
1.2.4.59.4 Por áreas associadas aos eventos.
1.2.4.59.5 Visualização rápida das ações mais urgentes.
1.2.4.60 Implementar workflow para tratamento das não conformidades.
1.2.4.61 Deve ser integrado à avaliação de riscos em TI.
1.2.4.62 Implementar Gestão de Alertas
1.2.4.63 Deve emitir alertas e trocar atributos conforme condições específicas.
1.2.4.64 Deve permitir a pontuação dos alertas.
1.2.4.65 Gerar Relatórios, Gerir Métricas, Praticar Melhoria Contínua.
1.2.4.66 Deve permitir a geração de relatórios, tabelas, gráficos, mapas e estatísticas dos inventários, análise e workflow.
1.2.4.67 Deve permitir a geração de relatórios e exportações nos formatos (xls, rtf, pdf) sem a necessidade de instalação de pacotes escritórios nas estações de trabalho.
1.2.4.68 Deve permitir a geração de relatório de nível estratégico contendo informações de toda a organização, de ameaças possíveis, risco para as macrodimensões, dimensões e os itens de inventário que os suportam, além de orientações para a gestão de riscos em tecnologia da informação.
1.2.4.69 Deve permitir a geração de relatório com a representação gráfica da interdependência de item do inventário com uma dimensão e sua macrodimensão, projetos, bem como os riscos encontrados no momento de fiscalização, inspeção e auditoria.
1.2.4.70 Deve permitir a geração de relatório de nível tático contendo informações gerais sobre as fiscalizações, inspeções e auditorias, mostrando os itens do inventário que foram analisados, bem como seus níveis de risco e possíveis estratégias de tratamento.
1.2.4.71 Deve permitir a geração de relatório de nível operacional visualizando os comentários realizados nas fiscalizações, inspeções e auditorias cada item do inventário, as boas práticas existentes, bem como os riscos encontrados.
1.2.4.72 Deve permitir a filtragem para todos os relatórios possibilitando que apenas parte da fiscalização, inspeção e auditoria seja avaliada.
1.2.4.73 Deve permitir a criação de gráficos a partir das análises realizadas.
1.2.4.74 Deve possibilitar filtros gráficos criados a partir de:
1.2.4.74.1 Risco encontrado.
1.2.4.74.2 Ativos.

1.2.4.74.3 Índice de conformidade.
1.2.4.74.4 Quantidade de elementos cadastrados no sistema.
1.2.4.74.5 Quantidade de questionamentos conformes.
1.2.4.74.6 Quantidade de questionamentos inconformidades.
1.2.4.75 Deve permitir agrupamentos dos gráficos em:
1.2.4.75.1 Ameaças aos elementos cadastrados.
1.2.4.75.2 Bases de conhecimentos geradas.
1.2.4.75.3 Elementos avaliados nas análises.
1.2.4.75.4 Responsável pelos elementos cadastrados.
1.2.4.76 Deve permitir a visualização em tipos distintos de gráficos, dentre eles:
1.2.4.76.1 Radar.
1.2.4.76.2 Pizza.
1.2.4.76.3 Barras.
1.2.4.76.4 Linhas.
1.2.4.77 Deve possibilitar a visualização gráfica do histórico das análises por:
1.2.4.77.1 Determinada época.
1.2.4.77.2 Série Histórica.
1.2.4.78 Deve permitir a inserção de filtros baseadas em:
1.2.4.78.1 Escolha por elementos cadastrados.
1.2.4.78.2 Responsável pelos elementos cadastrados.
1.2.4.78.3 Agrupamentos criados dentro das bases de conhecimento.
1.2.4.78.4 Nível do risco identificado.
1.2.4.78.5 Fontes potenciais de danos.
1.2.4.78.6 Causador da fonte potencial de dano.
1.2.4.79 Deve permitir o agrupamento dos gráficos criados em painéis de controles pré-selecionados.
1.2.4.80 Deve aumentar e/ou diminuir o nível de detalhamento dos gráficos, imergindo em um de seus componentes formadores.
1.2.4.81 Deve permitir a mudança do tipo de gráfico mesmo após sua definição inicial.
1.2.4.82 Deve mostrar legendas dos gráficos.

1.2.5 PRODUTOS ESPERADOS:

1.2.5.1 Software de gestão de segurança da informação instalado e em operação.
1.2.5.2 Serviço de suporte, manutenção e atualização de software durante todo o período de vigência do contrato.

1.2.6 PRAZO DE ENTREGA:

1.2.6.1 O fornecimento deverá ser executado em até 15 (quinze) dias corridos contados a partir da emissão de Ordem de Fornecimento – OF;

1.3 DESCRIÇÃO DETALHADA PARA ELABORAÇÃO DAS METODOLOGIAS DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO:

1.3.1 Elaborar e desenvolver metodologia de gestão de riscos em Segurança da Informação para o TJCE com base na análise, levantamento, mapeamento, consolidação e documentação de situações, ambientes, pessoas e processos que apresentem riscos relativos ao manuseio e circulação da informação institucional. No desenvolvimento e na consolidação da metodologia de gestão de riscos em questão deverá ser levando em consideração, no que couber, os seguintes normativos:
1.3.1.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.
1.3.1.2 NORMATIVOS ABNT: ABNT NBR ISO Guia 73:2005; ABNT NBR ISO/IEC 27005:2008; ABNT NBR ISO/IEC 27001:2006; ABNT NBR ISO/IEC 27002:2005 e ISO 31000;
1.3.1.3 Caso haja mudança dos normativos relacionados acima, estas deverão ser, necessariamente, observadas e aplicadas durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas demandas normativas apresentadas;
1.3.1.4 Caso os normativos acima sejam, em sua totalidade ou em parte, substituídos, os novos normativos deverão ser, necessariamente, observados e aplicados;
1.3.1.5 Durante a execução dos serviços, deverão ser observadas pela Contratada tantas mudanças quanto forem necessárias para adequar o TJCE aos novos normativos em vigência;
1.3.2 Deverão ser observados os seguintes aspectos na elaboração das metodologias:
1.3.2.1 Comunicação e consulta - Comunicar e consultar as partes envolvidas internas e externas, conforme apropriado, em cada etapa do processo de gestão de riscos e em relação ao processo como um todo.
1.3.2.2 Estabelecimento dos contextos - Estabelecer os contextos: externo, interno e da gestão de riscos nos quais se desenvolverá o restante do processo. Devem ser estabelecidos os critérios em relação aos quais os riscos serão avaliados e deverá ser definida a estrutura de análise.

1.3.2.3 Identificação de riscos - Identificar onde, quando, por que e como os eventos podem impedir, atrapalhar, atrasar ou melhorar a consecução dos objetivos.
1.3.2.4 Análise de riscos - Identificar e avaliar os controles existentes. Determinar as consequências e a probabilidade e, por conseguinte, o nível de risco. Tal análise deve considerar as diversas consequências potenciais e como elas podem ocorrer.
1.3.2.5 Avaliação de riscos - Comparar os níveis de risco estimados com os critérios estabelecidos previamente e considerar o balanço entre os benefícios potenciais e os resultados adversos. Isso possibilita que sejam tomadas decisões quanto à extensão, natureza dos tratamentos necessários e prioridades.
1.3.2.6 Tratamento de riscos - Desenvolver e implementar estratégias e planos de ação específicos e econômicos, para aumentar os benefícios potenciais e reduzir os custos potenciais.
1.3.2.7 Monitoramento e análise crítica – Deverá ser monitorada e demonstrada a real eficácia de todas as etapas do processo de gestão de riscos, com o objetivo de se garantir a manutenção das prioridades mapeadas, independentemente de alterações que envolvam o manuseio e trato das informações institucionais.

1.3.3 PRODUTOS ESPERADOS:

1.3.3.1 Metodologia de gestão de risco documentada (processos e responsabilidades): Comunicação e consulta, Estabelecimento dos contextos, Identificação e estimativa de Riscos, Análise, Avaliação e Tratamento do Risco, Monitoramento e análise crítica;
1.3.3.2 Piloto para validação da metodologia de gestão de riscos.

1.3.4 ATIVIDADES DE APOIO:

1.3.4.1 PLANO DE TRABALHO com o detalhamento do escopo da metodologia e cronograma de execução;
1.3.4.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;
1.3.4.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

1.3.5 PRAZO DE ENTREGA:

1.3.5.1 O serviço deverá ser executado em até 30 (trinta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

1.4 DESCRIÇÃO DETALHADA PARA ANÁLISE DE RISCOS E VULNERABILIDADES EM SEGURANÇA DA INFORMAÇÃO

1.4.1 Inventariar, analisar, avaliar e tratar os riscos relacionados aos ativos de informação do TJCE, determinando as consequências e probabilidades e, por conseguinte, o nível de risco, considerando, no que couber, os seguintes normativos:
1.4.1.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.
1.4.1.2 NORMATIVOS ABNT: ABNT NBR ISO Guia 73:2005; ABNT NBR ISO/IEC 27005:2008; ABNT NBR ISO/IEC 27001:2006; ABNT NBR ISO/IEC 27002:2005 e ISO 31000;
1.4.1.3 Caso haja mudança dos normativos relacionados acima, estas deverão ser, necessariamente, observadas e aplicadas durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas demandas normativas apresentadas;
1.4.1.4 Caso os normativos acima sejam, em sua totalidade ou em parte, substituídos, os novos normativos deverão ser, necessariamente, observados e aplicados;
1.4.1.5 Durante a execução dos serviços, deverão ser observadas pela Contratada tantas mudanças quanto forem necessárias para adequar o TJCE aos novos normativos em vigência;
1.4.2 Deverão ser observados os seguintes aspectos para a ANÁLISE DE RISCOS:
1.4.2.1 Análise do Faltante (GAP Analisys) de acordo com normativos e melhores práticas;
1.4.2.2 Deverão ser inventariados os ativos de tecnologia, sistemas e serviços de tecnologia da informação, pessoas e ambientes físicos.
1.4.2.3 Deverá ser gerado um relatório de inventário de ativos para validação por representante do TJCE, contendo:
1.4.2.4 Tipo de ativo (Ativos de Negócios do TJCE; Ativos de Segurança da Informação do TCJE);
1.4.2.5 Relevância do ativo para o atendimento da missão institucional do TJCE;
1.4.2.6 Deverão ser analisados os ativos inventariados considerando seus respectivos componentes constantes no relatório de inventário entregue e validado na etapa anterior.
1.4.2.7 Deverão ser gerados relatórios gerenciais, apresentando indicadores que possibilitem a avaliação por parte dos gestores do atual nível de risco do TJCE;
1.4.3 O RELATÓRIO GERENCIAL DE RISCOS demonstrando como foi avaliada cada situação de risco e como foram valorados os ativos de negócio, de segurança da informação, humanos, processuais e tecnológicos, obedecendo a seguinte relação entre os itens abaixo relacionados e a base normativa indicada:
1.4.3.1.1 Ativos (ISO/IEC 13335-1:2004 e ISO/IEC 27001:2006):

1.4.3.1.2 Tipo de ativo (ISO/IEC 27001:2006 e ISO/IEC 27005:2008):
1.4.3.1.3 Ativos de Negócios do TJCE;
1.4.3.1.4 Ativos de Segurança da Informação do TJCE
1.4.3.1.5 Relevância do ativo para o atendimento da missão institucional do TJCE;
1.4.3.1.6 Risco (ISO/IEC Guide 73, AS/NZS 4360 e ISO 31000):
1.4.3.1.7 Impacto [COSO (Risk Solutions, 2007)];
1.4.3.1.8 Evento [COSO (Risk Solutions, 2007 e ISO/IEC Guide 73:2002)];
1.4.3.1.9 Vulnerabilidade (ISO/IEC 13335-1:2004 e ISO 31000);
1.4.3.1.10 Efeito;
1.4.3.1.11 Ameaça (ISO/IEC 27000:2009):
1.4.3.1.12 Tipo de ameaça;
1.4.3.1.13 Agente da ameaça;
1.4.3.1.14 Tratamento de riscos (ISO 31000, ISO/IEC Guide 73:2002 e ISO/IEC 31010:2009):
1.4.3.1.15 Evitar o risco;
1.4.3.1.16 Reduzir o risco;
1.4.3.1.17 Transferir o risco;
1.4.3.1.18 Reter o risco;
1.4.3.1.19 Requisitos de segurança;
1.4.3.1.20 Controles:
1.4.3.1.21 Referência do controle;
1.4.3.1.22 Justificativa do controle;
1.4.3.1.23 Recomendações para a implementação do controle;
1.4.3.1.24 Custo/esforço aproximado para implementação do controle.
1.4.4 Os RELATÓRIOS DE OCORRÊNCIA DE RISCOS IDENTIFICADOS que tragam consigo recomendações para o tratamento das não conformidades acima identificadas, ainda que estas não possam ser tratadas.
1.4.5 O processo de análise de riscos deverá envolver profissionais especialistas em análise de riscos e especialistas no negócio do Tribunal (identificados pela contratada quando do levantamento dos ativos de segurança da informação do TJCE).
1.4.6 Entrevistas com os usuários e técnicos de TI do TJCE deverão ser realizadas e documentadas com o intuito de medir o nível de conscientização de cada um no que se refere a Segurança da Informação.
1.4.7 Deverão ser levantados, identificados, listados, documentados e quantificados os ambientes físicos sensíveis, onde gestores tratam informações confidenciais. Após o levantamento deverá ser realizada análise de risco detalhada de cada um dos mencionados ambientes levantados.
1.4.8 A análise dos insumos identificados no RELATÓRIO GERENCIAL DE RISCOS deverá contemplar, no mínimo, o quantitativo amostral abaixo relacionado. Caso o quantitativo em questão não consiga demonstrar, claramente, a situação de segurança atual do parque tecnológico do TJCE, nova análise deverá ser feita com agregação de tantos itens quanto necessário para demonstrar a real situação em comento:
1.4.8.1 Servidores de rede, físicos e virtuais: 150 itens de verificação;
1.4.8.2 Equipamentos / ativos de conectividade: 200 itens de verificação;
1.4.8.3 Estações de trabalho: 100 itens de verificação;
1.4.8.4 Pessoas (Gestores/Usuários/Técnicos): 250 itens de verificação. As entrevistas deverão refletir o nível de conhecimento dos colaboradores alocados em TODOS os setores do TJCE. Ademais, os detentores de cargo em comissão do TJCE deverão ser entrevistados e, particularmente, entrevistas pessoais deverão ser realizadas com TODOS os Secretários do Tribunal;
1.4.8.5 Ambientes Físicos (Escritórios/Datacenters);
1.4.9 Na análise deverão ser considerados, no mínimo, os seguintes ativos de tecnologia e respectivos desdobramentos:
1.4.9.1 Servidores
1.4.9.2 Sistema Operacional;
1.4.9.3 Aplicação de banco de dados;
1.4.9.4 Serviços de TI.
1.4.9.5 Estações de Trabalho
1.4.9.6 Sistema Operacional;
1.4.9.7 Aplicativos de Escritório;
1.4.9.8 Softwares de Comunicação.
1.4.9.9 Equipamentos de Conectividade.
1.4.9.10 Configurações de Segurança dos sistemas;
1.4.9.11 Regras de Segurança (Firewalls, IPS);
1.4.9.12 Disposição física.
1.4.9.13 Ambientes Físicos (Escritórios/Datacenters);
1.4.9.14 Boas práticas para Datacenters;
1.4.9.15 Boas práticas para Escritórios.
1.4.9.16 Sistemas.

1.4.9.17 Processo de Desenvolvimento (desenvolvimento seguro de aplicações).
1.4.9.18 Situações de risco.
1.4.9.19 Interferência eletromagnética, indisponibilidade de serviços ou informações, altas temperaturas ou umidade, falha de energia, falha de hardware, falha de software, queda de desempenho, código malicioso, acesso lógico não autorizado, fraude ou sabotagem, paralisação dos serviços ou informações, erros humanos, omissões ou uso indevido, acesso físico não autorizado, incêndio, furto ou roubo, falta de mão-de-obra essencial, falha em meios de comunicação, violação de propriedade intelectual, perda de rastreabilidade, multas, indenizações ou sanções legais, repúdio, não atendimento à regulamentação, dano a pessoas e instalações, perda de integridade de dados.
1.4.9.20 Quaisquer outras ameaças deverão ser consideradas nas análises de riscos quando necessárias à adequada execução dos serviços e/ou demandas do TJCE.
1.4.10 Com base nos resultados das análises mencionadas, deverá ser gerado o RELATÓRIO DE MITIGAÇÃO DE RISCOS, contendo soluções para cada item de insegurança levantado no "RELATÓRIO DE OCORRÊNCIAS DE RISCOS IDENTIFICADOS";
1.4.11 Nesta etapa, a Contratada deverá disponibilizar para a Equipe Técnica do TJCE um PLANO DE TRATAMENTO DE RISCOS, contemplando ações de controle de riscos e viabilidade de implantação, contendo no mínimo: Ações a serem implantadas; Prazos para Implantação; Áreas Funcionais responsáveis por implantar e manter controle sobre os riscos;
1.4.12 A Contratada deverá realizar Workshop(s) para prestar orientação e capacitação à Equipe Técnica do TJCE, visando o correto entendimento e a correta execução do PLANO DE TRATAMENTO DE RISCOS.
1.4.13 Durante a vigência do Contrato:
1.4.13.1 O acompanhamento do nível de risco dos ativos do TJCE deverá ser realizado pela Contratada de forma constante e por meio de um plano chamado "PLANO DE TRATAMENTO DE RISCOS ANUAL", a ser apresentado, previamente, ao TJCE, que o analisará e o aprovará antes de sua efetiva aplicação em ambiente de produção. Este plano deverá apresentar os índices de riscos esperados com base no tratamento sugerido pela Contratada.
1.4.13.2 A Contratada deverá atualizar os índices de riscos com base nas informações fornecidas pelo TJCE dos controles de riscos que forem sendo tratados. Os novos índices de riscos deverão ser apresentados trimestralmente aos gestores do TJCE. A empresa contratada deverá, a partir da atualização oficial de fontes normativas de pesquisa de risco que tragam novas vertentes identificadas de risco, adaptar sua metodologia de avaliação de risco para atender a esses novos indicativos normativos. Os ativos tecnológicos deverão ser analisados pela Contratada antes de sua entrada em ambiente de produção na Entidade. Deverá ser gerado um novo relatório de riscos do ativo analisado antes de sua entrada em ambiente de produção com as evidências de que os riscos foram tratados.
1.4.14 Os resultados das análises de riscos trimestrais deverão ser consolidados e apresentados por meio de relatórios, em formato gerencial e técnico, denominados:
1.4.14.1 RELATÓRIO TRIMESTRAL DE RISCOS DOS ATIVOS TECNOLÓGICOS DO TJCE;
1.4.14.2 RELATÓRIO CONSOLIDADO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO DO TJCE.
1.4.14.3 Os relatórios deverão compreender, no mínimo, informações sobre:
1.4.14.3.1 Avaliação de riscos dos ativos analisados, indicando os critérios, requisitos, metodologias e ponderações utilizadas;
1.4.14.3.2 As evidências necessárias apuradas;
1.4.14.3.3 As ameaças e vulnerabilidades encontradas;
1.4.14.3.4 A classificação de riscos e criticidades atribuídas;
1.4.14.3.5 A mensuração financeira estimada para auxiliar na decisão de tratamento do risco;
1.4.14.3.6 A identificação dos responsáveis e processos de negócio;
1.4.14.3.7 A análise de impactos;
1.4.14.3.8 Os controles propostos para a mitigação e tratamento do risco;
1.4.14.3.9 Indicadores quantitativos e qualitativos de riscos, dentre outras informações;
1.4.14.3.10 Observações pertinentes para o julgamento da análise.
1.4.15 Todo relatório/plano sobre análise de risco deverá identificar ações e definições para evitar, transferir, reter, reduzir ou mitigar os riscos apresentados. Também deverá identificar possíveis prejuízos, caso o Tribunal opte por não tratar os riscos previamente observados pela Contratada. Todo relatório, ao ser apresentado ao TJCE, deverá demonstrar a(s) metodologia(s) aplicada(s) bem como se esta(s) possui(em) aderência normativa ao compêndio identificado.

1.4.16 PRODUTOS ESPERADOS:

1.4.16.1 Na 1ª execução:
1.4.16.1.1 Relatório Análise do Faltante (Gap Analisys) com observância dos normativos;
1.4.16.1.2 Relatório de Inventário de Ativos de Informação com observância dos normativos;
1.4.16.1.3 Relatório Gerencial de Riscos;
1.4.16.1.4 Relatório de Ocorrência de Riscos Identificados e Recomendações;
1.4.16.1.5 Relatório de Mitigação de Riscos;
1.4.16.1.6 Plano de Tratamento de Riscos;

1.4.16.2 Nas demais execuções na vigência do contrato:
1.4.16.2.1 Plano de Tratamento de Riscos Anual;
1.4.16.2.2 Relatório Trimestral de Riscos dos Ativos;
1.4.16.2.3 Relatório Consolidado de Riscos;

1.4.17 ATIVIDADES DE APOIO:

1.4.17.1 PLANO DE TRABALHO com o detalhamento do escopo da análise e cronograma de execução;
1.4.17.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;
1.4.17.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

1.4.18 PRAZO DE ENTREGA:

1.4.18.1 Na 1ª execução: o serviço deverá ser executado em até 90 (noventa) dias corridos contados a partir da emissão de Ordem de Serviço – OS;
1.4.18.2 Nas demais execuções na vigência do contrato: o serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

1.5 DESCRIÇÃO DETALHADA PARA TESTES DE INVASÃO INTERNOS E EXTERNOS;

1.5.1 A atividade de Testes de Invasão Externos e Internos tem como objetivo principal identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica do TJCE. Estes testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações do TJCE.
1.5.2 Para a realização dos testes de invasão deverão ser observadas as orientações e técnicas emanadas pelos seguintes padrões internacionais, além de outros apresentados pela empresa contratada, caso haja, em seu portfólio, normativos que, comprovadamente, complementem os demonstrados abaixo:
1.5.2.1 OSSTMM 3 (The Open Source Security Testing Methodology Manual);
1.5.2.2 ISSAF/PTF (Information Systems Security Assessment Framework);
1.5.2.3 NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment);
1.5.2.4 NIST Special Publication 800-42 (Guideline on Network Security Testing);
1.5.2.5 OWASP TESTING GUIDE 3.0 - The Open Web Application Security Project.
1.5.3 O teste de invasão deverá obedecer às seguintes fases: 1ª) Planejamento; 2ª) Descoberta; 3ª) Ataque (exploração); 4ª) Relatório de recomendações;
1.5.4 A Contratada deverá observar que os testes, simulações de invasão ilícita e não autorizada a ativos e informações (Teste de Invasão), a serem executadas internamente (através da rede interna do TJCE) ou externamente (através da Internet), deverão ter duração máxima de até 20 (vinte) dias para cada simulação realizada.
1.5.5 Os alvos dos "Testes de Invasão" bem como as premissas e condições para realização dos mesmos serão, necessariamente, definidas e aprovadas pelo TJCE.
1.5.6 Todas as fases dos "Testes de Invasão" serão acompanhadas e supervisionadas pelo TJCE. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada ao TJCE, haja vista a necessidade de manter a disponibilidade dos ambientes ativos e serviços do Tribunal.
1.5.7 Deverá ser utilizada, pelo menos, 01 (uma) ferramenta de análise de vulnerabilidade comercial e 01 (uma) ferramenta de análise de vulnerabilidade gratuita. As ferramentas deverão ser apresentadas ao TJCE para ciência e aprovação em sua utilização, antes de sua efetiva utilização.
1.5.8 Deverá realizar análise de vulnerabilidades em até 1.000 (hum mil) endereços IPs do ambiente computacional do TJCE, sendo servidores, desktops, ativos de rede e outros equipamentos relacionados ao teste de vulnerabilidades.
1.5.9 Deverá ser elaborado o "PLANO DE TESTE DE INVASÃO", para cada teste que será realizado, contemplando as informações de PLANEJAMENTO do teste, tais como:
1.5.9.1 Objetivos, premissas e escopo do teste, datas e horas dos testes, metodologia de análise de vulnerabilidades, descrição das ações realizadas, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas.
1.5.9.2 Também na fase de planejamento, deverão ser atendidas e apresentadas, no mínimo, as seguintes informações:
1.5.9.2.1 Detalhes da infraestrutura alvo dos testes de invasão;
1.5.9.2.2 Equipamentos e recursos demandados para este teste;
1.5.9.2.3 Tipos de ataque;
1.5.9.2.4 Prazos (janelas de tempo para execução dos testes);
1.5.9.2.5 Pontos de contato da contratada (responsáveis para tratamento de questões não abordadas nos testes);
1.5.9.2.6 Tipos de testes a serem realizados pelos especialistas em segurança da informação, devendo-se

observar:
1.5.9.2.7 Quanto à abordagem:
1.5.9.2.7.1 Coletar informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas;
1.5.9.2.7.2 Técnica da caixa-preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista);
1.5.9.2.7.3 Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste);
1.5.9.2.7.4 Técnica da caixa cinza ou híbrida (conhecimento limitado sobre o alvo);
1.5.9.2.8 Quanto à forma de publicidade:
1.5.9.2.8.1 Teste informado (a equipe de segurança de TI do TJCE terá conhecimento dos testes);
1.5.9.2.8.2 Teste não informado (a equipe de segurança de TI do TJCE NÃO terá conhecimento dos testes);
1.5.9.3 Informações detalhadas dos testes em si;
1.5.9.4 Nesta fase de planejamento deverá ser obtido, formalmente:
1.5.9.4.1 A aprovação dos responsáveis do TJCE para o início dos testes, por meio de documentação chamada: TERMO DE AUTORIZAÇÃO PARA REALIZAÇÃO DE TESTES DE INVASÃO;
1.5.9.4.2 O preenchimento e a assinatura de TERMO DE CIÊNCIA de TODOS os técnicos da empresa contratada que atuarão nestes testes;
1.5.9.4.3 O preenchimento e a assinatura de TERMO DE COMPROMISSO do(s) representante (s) da contratada;
1.5.9.4.4 A especificação dos endereços IP a serem testados;
1.5.9.4.5 Restrição de ambiente computacional (ex: computadores, servidores, sistemas e sub-redes a NÃO serem testados);
1.5.9.4.6 Lista de técnicas de teste aplicáveis (engenharia social, DOS, etc) e ferramentas (decodificadores de senha, “sniffers” de rede, etc);
1.5.9.4.7 Momentos em que os testes serão conduzidos (ex. durante hora de trabalho, depois de horário de trabalho, etc);
1.5.9.4.8 Endereço IP das máquinas nas quais o teste de invasão será aplicado, de forma que os administradores possam diferenciar o legítimo ataque da empresa contratada dos ataques de hackers;
1.5.9.4.9 Forma de manuseio das informações coletadas pela equipe do teste de invasão.
1.5.10 Na fase da DESCOBERTA deverão ser atendidos os seguintes quesitos e apresentado “RELATÓRIO DE DESCOBERTA DE TESTE DE INVASÃO”, entre outros:
1.5.10.1 Coleta de informações, sendo classificadas em:
1.5.10.1.1 Coleta passiva, onde deverá ser utilizada, no mínimo, as seguintes técnicas:
1.5.10.1.1.1 Whois e nslookup (consultas DNS);
1.5.10.1.1.2 Sites de busca;
1.5.10.1.1.3 Listas de discussão;
1.5.10.1.1.4 Blogs de colaboradores;
1.5.10.1.1.5 Dumpster diving ou trashing;
1.5.10.1.1.6 Informações livres;
1.5.10.1.1.7 Packet sniffing “passive eavesdropping”;
1.5.10.1.1.8 Captura de banner.
1.5.10.1.2 Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas:
1.5.10.1.2.1 Port scanning (Mapeamento de rede);
1.5.10.1.2.2 Varredura de vulnerabilidade.
1.5.10.2 A varredura de vulnerabilidade deverá verificar/identificar, entre outros:
1.5.10.2.1 Hosts ativos na rede;
1.5.10.2.2 Portas e serviços em execução;
1.5.10.2.3 Serviços ativos e vulneráveis nos hosts;
1.5.10.2.4 Sistemas operacionais;
1.5.10.2.5 Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas;
1.5.10.2.6 Configurações feitas nos hosts sem observância de boas práticas em segurança computacional;
1.5.10.2.7 Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas;
1.5.10.2.8 Identificação de vetores de ataque e cenários para exploração;
1.5.10.2.9 Vulnerabilidades Detectadas (CVE);
1.5.10.2.10 Vulnerabilidades de Alto Risco;
1.5.10.2.11 Vulnerabilidades de Médio Risco;
1.5.10.2.12 Vulnerabilidades de Baixo Risco;
1.5.10.2.13 Informações a serem aplicadas na 3ª fase (fase de ataques);
1.5.10.2.14 Dos serviços e aplicações web:
1.5.10.2.14.1 Uso indevido de sistema de arquivos e arquivos temporários;
1.5.10.2.14.2 Evasão de informação por configurações default de tratamento de erros;
1.5.10.2.14.3 Tratamento indevido de entrada;
1.5.10.2.14.4 Problemas relacionados a má configuração dos serviços;
1.5.10.2.14.5 Gerenciamento inseguro de sessões web;

1.5.10.2.14.6 Verificação de trilhas de auditoria;
1.5.10.2.14.7 Escalação de privilégios;
1.5.10.3 Observa-se que a varredura em questão NÃO poderá:
1.5.10.3.1 Provocar paradas nos serviços prestados pelo ambiente computacional do TJCE;
1.5.10.3.2 Apresentar alta taxa de FALSO/POSITIVO;
1.5.10.3.3 Apresentar base de dados desatualizada (antes da realização de qualquer varredura, deverá ser apresentado ao TJCE provas de que a base de assinaturas das ferramentas utilizadas pela Contratada está atualizada com sua última versão).
1.5.10.4 Observa-se, ainda, que a varredura em questão deverá ser realizada em:
1.5.10.4.1 Redes corporativas autorizadas pelo TJCE;
1.5.10.4.2 Computadores autorizados pelo TJCE;
1.5.10.5 Mapeamento de rede, devendo ser verificado/identificado, entre outros:
1.5.10.5.1 Ativos conectados a rede corporativa do TJCE sem autorização;
1.5.10.5.2 Serviços vulneráveis;
1.5.10.5.3 Serviços autorizados que não estão em conformidade com a atual política de segurança da informação do Tribunal;
1.5.10.5.4 Fragilidades apresentadas pelos sistemas de IDS/IPS corporativos.
1.5.11 Na fase de ATAQUE deverão ser apresentadas, dentro do "RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO", as seguintes informações:
1.5.11.1 Confirmação ou refutação de a existência de vulnerabilidades;
1.5.11.2 Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade;
1.5.11.3 Obtenção de acesso e possível escalada de privilégios;
1.5.11.4 Deverão ser aplicados, no mínimo, os seguintes tipos de ataques:
1.5.11.4.1 Violações do protocolo HTTP;
1.5.11.4.2 SQL Injection;
1.5.11.4.3 LDAP Injection;
1.5.11.4.4 Cookie Tampering;
1.5.11.4.5 Cross-Site Scripting (XSS);
1.5.11.4.6 Directory Transversal;
1.5.11.4.7 Buffer Overflow;
1.5.11.4.8 OS Command Execution;
1.5.11.4.9 Command Injection;
1.5.11.4.10 Remote Code Inclusion;
1.5.11.4.11 Server Side Includes (SSI) Injection;
1.5.11.4.12 File disclosure;
1.5.11.4.13 Information Leak;
1.5.11.4.14 Zero day attacks;
1.5.11.4.15 DDos (Distribuited Denial of Service);
1.5.11.4.16 Dos (Denial of Service);
1.5.11.4.17 Contra protocolo TCP;
1.5.11.4.18 Ataques contra a aplicação.
1.5.11.5 Os ataques de negação de serviços, contra protocolo TCP e em nível da aplicação deverão, cada qual, explorar/demonstrar/utilizar as seguintes técnicas:
1.5.11.5.1 Para ataques de negação de serviços:
1.5.11.5.1.1 Bugs em serviços, aplicativos e sistemas operacionais;
1.5.11.5.1.2 SYN flooding;
1.5.11.5.1.3 Fragmentação de pacotes de IP;
1.5.11.5.1.4 Smurf e fraggle;
1.5.11.5.1.5 Teardrop, nuke e land.
1.5.11.5.1.6 Para ataques contra o protocolo TCP:
1.5.11.5.1.7 Seqüestro de conexões;
1.5.11.5.1.8 Prognóstico de número de seqüência do protocolo TCP;
1.5.11.5.1.9 Ataque de Mitnick;
1.5.11.5.1.10 Source routing.
1.5.11.5.1.11 Para ataques em nível da aplicação:
1.5.11.5.1.12 Buffer Overflow ;
1.5.11.5.1.13 Problemas com o SNMP;
1.5.11.5.1.14 Vírus, worms e cavalos de tróia.
1.5.12 Observa-se que, antes da utilização de qualquer técnicas acima, o TJCE abrirá janelas de manutenção em seu ambiente tecnológico.
1.5.13 Captura de Tráfego para testar se os algoritmos e protocolos utilizados na comunicação dos sistemas garantem a integridade e privacidade das informações em trânsito;
1.5.13.1 Quebra de Senha de perfis determinados pelo TJCE;

1.5.13.2 Injeção de Código;
1.5.13.3 Ataques XSS (Cross-site Script);
1.5.13.4 Comprometimento do acesso remoto do TJCE;
1.5.13.5 Manutenção de acesso;
1.5.13.6 Encobrimento de rastros da invasão.
1.5.14 Para testes de invasão direcionados, especificamente, aos serviços do TJCE prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados, no mínimo, os seguintes testes baseados na publicação OWASP TESTING GUIDE 3.0 (The Open Web Application Security Project):
1.5.14.1 Para testes de coleta de informações, aplicar padrão: OWASP-IG-001, OWASP-IG-002, OWASP-IG-003, OWASP-IG-004, OWASP-IG-005 e OWASP-IG-006;
1.5.14.2 Para testes de gerenciamento de configuração, aplicar padrão: OWASP-CM-001, OWASP-CM-002, OWASP-CM-003, OWASP-CM-004, OWASP-CM-005, OWASP-CM-006, OWASP-CM-007, OWASP-CM-008;
1.5.14.3 Para testes de autenticação, aplicar padrão: OWASP-AT-001, OWASP-AT-002, OWASP-AT-003, OWASP-AT-004, OWASP-AT-005, OWASP-AT-006, OWASP-AT-007, OWASP-AT-008, OWASP-AT-009 e OWASP-AT-010;
1.5.14.4 Para testes de gerenciamento de sessão, aplicar padrão: OWASP-SM-001, OWASP-SM-001, OWASP-SM-002, OWASP-SM-003, OWASP-SM-004, OWASPSM-005;
1.5.14.5 Para testes de autorização, aplicar padrão: OWASP-AZ-001, OWASP-AZ-002 e OWASP-AZ-003;
1.5.14.6 Para testes de negócio lógico, aplicar padrão: OWASP-BL-001;
1.5.14.7 Para testes de validação de dados, aplicar padrão: OWASP-DV-001; OWASPDV-002, OWASP-DV-003, OWASP-DV-004, OWASP-DV-005, OWASP-DV-006, OWASP-DV-007, OWASP-DV-008, OWASP-DV-009, OWASP-DV-010, OWASP-DV-011, OWASP-DV-012, OWASP-DV-013, OWASP-DV-014, OWASP-DV-015 e OWASP-DV-016;
1.5.14.8 Para testes de negação de serviços, aplicar padrão: OWASP-DS-001, OWASP-DS-002, OWASP-DS-003, OWASP-DS-004, OWASP-DS-005, OWASP-DS-006, OWASP-DS-007 e OWASP-DS-008;
1.5.14.9 Para testes de serviços web, aplicar padrão: OWASP-WS-001, OWASP-WS-002, OWASP-WS-003, OWASP-WS-004, OWASP-WS-005, OWASP-WS-006 e OWASP-WS-007.
1.5.15 Observa-se que o resultado de cada teste deverá vir acompanhado de relatórios contendo:
1.5.15.1 Referência-base (Whitepaper);
1.5.15.2 Ameaças encontradas;
1.5.15.3 Riscos levantados ao ambiente computacional;
1.5.15.4 Contramedidas para mitigar as ameaças achadas.
1.5.16 Observa-se que cada relatório contendo o resultado de testes deverá ser claro e conciso e fornecer ao TJCE completo entendimento sobre as ameaças e riscos encontrados. Também se observa a necessidade de a empresa apresentar os resultados em tabelas, seguindo o padrão apresentado abaixo:

Categoria	Número de Referência	Nome do Teste	Ameaças	Solução	Riscos

1.5.17 O "RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO" deverá apresentar todas as informações necessárias e completas para o correto entendimento de cada teste realizados em ambiente do TJCE, contemplando no mínimo:
1.5.17.1 Objetivos, premissas e escopo do teste;
1.5.17.2 Metodologia de análise de vulnerabilidades;
1.5.17.3 Descrição das ações realizadas;
1.5.17.4 Vulnerabilidades encontradas;
1.5.17.5 Categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades;
1.5.17.6 Apresentação das evidências apuradas;
1.5.17.7 Fontes de pesquisa, referências e ferramentas utilizadas.
1.5.18 Ao final dos trabalhos, a Contratada deve também apresentar um "RELATÓRIO DE RETORNO SOBRE INVESTIMENTO", onde deverão ser expostas todas as falhas, vulnerabilidades, riscos e ameaças de segurança da informação, identificadas em ambiente corporativo, com FOCO GERENCIAL, ou seja, contendo informações com vista à conscientização e tomada de decisão, pela alta Administração do Tribunal, sobre os riscos a que a instituição está exposta e os gastos necessários para se aumentar o nível de segurança da informação hoje praticado pelo Tribunal.
1.5.19 Deverão ser entregues:
1.5.19.1 Avaliação e relatório da SEGURANÇA FÍSICA do Tribunal, com a finalidade de indicar se o ambiente físico onde se encontram os sistemas críticos do TJCE é adequado e atende a normas e boas práticas internacionais de segurança física relacionadas a ambientes de alta criticidade computacional;
1.5.19.2 Avaliação e relatório da SEGURANÇA TÉCNICO-ADMINISTRATIVA do Tribunal, com a finalidade de indicar o nível de gerenciamento do corpo administrativo e técnico do TJCE com relação às ações de manutenção da proteção dos dados computacionais do Tribunal.
1.5.20 Por fim, a empresa contratada fica ciente de que:

1.5.20.1 Todas as fases dos “Testes de Invasão” deverão ser acompanhadas e supervisionadas a qualquer momento pelo TJCE;
1.5.20.2 A Contratada deverá fazer todo o possível para evitar comprometer o funcionamento normal da infraestrutura de TI do TJCE, bem com resguardar a confidencialidade, integridade e disponibilidade de todas as suas informações;
1.5.20.3 Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo corporativo deverá ser imediatamente reportada ao TJCE;
1.5.20.4 Caso ocorra algum efeito imprevisto na infraestrutura do TJCE em função dos testes, a Contratada deverá interromper os trabalhos, contatar a Equipe de TI do TJCE e trabalhar em conjunto com a mesma para acelerar a recuperação.
1.5.21 Durante a vigência do Contrato:
1.5.21.1 A Contratada deverá fornecer um “PLANO DE TESTES ANUAL”, com datas previstas para execução, conforme acordado com o TJCE.

1.5.22 PRODUTOS ESPERADOS:

1.5.22.1 Na 1ª execução:
1.5.22.1.1 PLANO DE TESTE DE INVASÃO: com exposição integral das informações e ações demandadas pela fase de PLANEJAMENTO (término da fase);
1.5.22.1.2 RELATÓRIO DE DESCOBERTA DE TESTE DE INVASÃO: com exposição integral das informações e ações demandadas pela fase de DESCOBERTA (término da fase);
1.5.22.1.3 RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO: com exposição integral das informações e ações demandadas pela fase de ATAQUES (término da fase);
1.5.22.1.4 RELATÓRIO DE RETORNO SOBRE INVESTIMENTO;
1.5.22.1.5 RELATÓRIO DA SEGURANÇA FÍSICA;
1.5.22.1.6 RELATÓRIO DA SEGURANÇA TÉCNICO-ADMINISTRATIVA;
1.5.22.2 Nas demais execuções durante a vigência do contrato:
1.5.22.2.1 PLANO DE TESTE DE INVASÃO ANUAL obedecendo aos mesmos moldes das demandas emanadas pelos PLANO DE TESTE DE INVASÃO e os relatórios da 1ª execução.
1.5.22.2.2 RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO – mensal, trimestral e semestral segundo o observado pelo PLANO DE TESTES ANUAL.

1.5.23 ATIVIDADES DE APOIO:

1.5.23.1 PLANO DE TRABALHO com o detalhamento do escopo dos testes e cronograma de execução;
1.5.23.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;
1.5.23.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

1.5.24 PRAZO DE ENTREGA:

1.5.24.1 Na 1ª execução: o serviço deverá ser executado em até 90 (noventa) dias corridos contados a partir da emissão de Ordem de Serviço – OS;
1.5.24.2 Nas demais execuções durante a vigência do contrato: o serviço deverá ser executado em até 45 (quarenta e cinco) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

1.6 DESCRIÇÃO DETALHADA PARA ELABORAÇÃO DAS METODOLOGIAS DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1.6.1 Definir processo e atividades para o correto tratamento de incidentes, com o foco na identificação, análise, avaliação, tratamento, dentre outras atividades, proporcionando como principal benefício a capacidade de resposta aos incidentes de forma unificada pelo TJCE, considerando, no que couber, os seguintes normativos:
1.6.1.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.
1.6.1.2 NORMATIVOS ABNT: ABNT NBR ISO/IEC 27001:2006;
1.6.1.3 NORMATIVOS NIST (National Institute of Standards and Technology): Handbook for Computer Security Incident Response Teams (CSIRTs) – HANDBOOK CMU/SEI-2003-HB-002; NIST Special Publication 800-61 Revision 1 (Computer Security Incident Handling Guide); NIST Special Publication 800-83 (Guide to Malware Incident Prevention and Handling); NIST Special Publication 800-86 (Guide to Integrating Forensic Techniques into Incident Response);
1.6.1.4 Caso haja mudança dos normativos relacionados acima, estas deverão ser, necessariamente, observadas e aplicadas durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas demandas normativas apresentadas;
1.6.1.5 Caso os normativos acima sejam, em sua totalidade ou em parte, substituídos, os novos normativos deverão ser, necessariamente, observados e aplicados durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas

demandas normativas apresentadas;
1.6.1.6 Durante a execução dos serviços, deverá ser observada pela Contratada tantas mudanças quanto forem necessárias para adequar o Tribunal aos novos normativos em vigência;
1.6.2 Deverá ser gerada uma proposta para implantação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR considerando a estrutura funcional do TJCE e estratégia para sua criação;
1.6.3 A empresa Contratada deverá, necessariamente, após análise do parque computacional do TJCE, bem como da missão institucional do Tribunal, produzir documentação que determine a MISSÃO DA ETIR junto ao Tribunal:
1.6.3.1 Esta declaração deverá conter concisa e inequívoca descrição dos objetivos e a função da ETIR do TJCE.
1.6.3.2 Observa-se que a ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede;
1.6.4 A empresa deverá pautar suas ações na CRIAÇÃO da ETIR do TJCE com base em modelos de organização CENTRALIZADOS, observando-se:
1.6.4.1 A Equipe deverá ser composta, necessariamente, por pessoal com dedicação exclusiva às atividades de tratamento e resposta aos incidentes em redes computacionais.
1.6.4.2 Deverá ser realizado o estudo prévio das atividades/funções de TI em operação no Tribunal, do número de sistemas e plataformas suportadas, do número de serviços a serem oferecidos pela ETIR e do conhecimento técnico necessário do pessoal a ser alocado à equipe de tratamento de incidentes em questão. A estrutura organizacional da ETIR criada deverá observar/atender TODAS AS DEMANDAS LEVANTADAS pelo resultado do estudo prévio.
1.6.5 A AUTONOMIA COMPARTILHADA será o modelo de autonomia a ser observada na constituição da ETIR e esta autonomia deverá obedecer às seguintes características:
1.6.5.1 A ETIR deverá trabalhar em acordo com os outros setores da organização a fim de participar do processo de tomada de decisão;
1.6.5.2 A equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os outros membros da organização;
1.6.6 Deverá ser apresentado documento de CONSTITUIÇÃO DA ETIR onde deverão ser indicados TODOS os membros do processo decisório do Tribunal envolvidos com TODA a tomada de decisão relacionada a incidentes identificados em âmbito do Tribunal.
1.6.6.1 Apresentam-se, abaixo, as especialidades (membros) que poderão compor a ETIR, entre outros julgados pertinentes ao incidente a ser tratado:
1.6.6.1.1 Administradores de sistema ou de segurança;
1.6.6.1.2 Administradores de banco de dados;
1.6.6.1.3 Administradores de rede;
1.6.6.1.4 Analistas de suporte;
1.6.6.1.5 Representantes legais de áreas específicas da organização;
1.6.6.1.6 Controle interno.
1.6.7 A empresa contratada deverá apresentar ao TJCE procedimentos a serem aplicados a TODOS OS MEMBROS DA ETIR QUE DEIXAREM A EQUIPE EM QUESTÃO. Abrangendo, no mínimo:
1.6.7.1 Mudança de senhas (pessoais e de sistemas);
1.6.7.2 Devolução de todos os dispositivos/ferramentas em posse do membro em questão;
1.6.7.3 Revogação de chaves;
1.6.7.4 Entrevista de saída com a finalidade de relembrar ao colaborador das responsabilidades assumidas e ciência de sigilo profissional;
1.6.7.5 Informações sobre novo contato do colaborador (e-mail, telefone).
1.6.8 A empresa contratada deverá documentar, descrever e estruturar 02 (dois) tipos de serviços proativos e reativos da ETIR, com detalhamento de tarefas e ações específicas;
1.6.9 A empresa Contratada deverá produzir e apresentar ao TJCE uma política de classificação de incidentes computacionais. Esta política deverá conter uma taxonomia comum que possibilite identificação e classificação correta dos vários tipos de incidentes de TI.
1.6.10 A empresa Contratada deverá propor modelo de formulário específico para reporte de incidentes computacionais.
1.6.11 A empresa deverá indicar ao TJCE a necessidade ou não da aplicação de turnos diferenciados de trabalhos para a ETIR, recomendando práticas de sucesso adotadas em outros órgãos federais e/ou iniciativa privada.
1.6.12 A empresa deverá apresentar ao TJCE proposta de ferramentas para limpeza completa de dados em processo de descarte, bem como orientar o Tribunal sobre a forma e modo de eliminação de informações geradas pelos trabalhos realizados pela ETIR.
1.6.13 A empresa Contratada deverá padronizar procedimento de comunicação da ETIR do TJCE em relação à ocorrência de incidentes de segurança em redes de computadores.
1.6.14 A empresa Contratada deverá padronizar rotinas junto a ETIR do TJCE que possibilite aos membros

desta equipe:
1.6.14.1 Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;
1.6.14.2 Observar os procedimentos para preservação das evidências exigindo consulta às orientações sobre cadeia de custódia, conforme ato normativo específico a ser expedido;
1.6.14.3 Priorizar a continuidade dos serviços da ETIR do TJCE e da missão institucional da organização, observando os procedimentos previstos no item acima.
1.6.15 A empresa deverá apresentar ao TJCE uma proposta de treinamento para TODOS OS MEMBROS DA ETIR, devendo atender, no mínimo, conhecimentos relacionados a:
1.6.15.1 Procedimentos operacionais de ETIRs;
1.6.15.2 Políticas de segurança do Tribunal;
1.6.15.3 Identificação e entendimento de técnicas de intrusão;
1.6.15.4 Procedimento de comunicação com as partes envolvidas;
1.6.15.5 Análise de incidentes;
1.6.15.6 Gravação e manutenção de incidentes;
1.6.15.7 Distribuição de tarefas/ações pertinentes;
1.6.15.8 Produção de relatórios de tratamento de incidentes com informações detalhadas, no mínimo, sobre: descrição do incidente de segurança, indicação do método utilizado para coleta de evidências, ações de contenção realizadas, evidências apuradas, recomendações de controles, ações corretivas e preventivas para evitar a reincidência do incidente de segurança e observações pertinentes ao tratamento do incidente em questão.

1.6.16 PRODUTOS ESPERADOS:

1.6.16.1 Modelo de Gestão de Resposta a Incidentes;
1.6.16.2 Proposta de Implantação;
1.6.16.3 Documento com Missão da ETIR;
1.6.16.4 Documento de constituição da ETIR;
1.6.16.5 Documento com detalhamento de tipos de serviços, tarefas e ações da ETIR;
1.6.16.6 Política de classificação de incidentes computacionais;
1.6.16.7 Modelo de formulário para reporte de incidentes computacionais;
1.6.16.8 Proposta de utilização de ferramentas para limpeza completa de dados;
1.6.16.9 Procedimento de comunicação da ETIR do TJCE em caso de indícios de ilícitos criminais;
1.6.16.10 Proposta de treinamento;
1.6.16.11 Treinamento para os membros do ETIR;

1.6.17 ATIVIDADES DE APOIO:

1.6.17.1 PLANO DE TRABALHO com o detalhamento do escopo da metodologia e cronograma de execução;
1.6.17.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;
1.6.17.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

1.6.18 PRAZO DE ENTREGA:

1.6.18.1 O serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

1.7 DESCRIÇÃO DETALHADA PARA CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DO MODELO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

1.7.1 Criação ou revisão da forma de estruturação e atuação do Comitê Gestor de Segurança da Informação do TJCE em conformidade com o regimento interno e as portarias vigentes no Órgão, assim como dos Normativos: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.
1.7.2 Deverão ser revisadas ou criadas, neste serviço, as definições de infraestrutura de Segurança da Informação para:
1.7.2.1 Processos componentes;
1.7.2.2 Funções dos processos componentes;
1.7.2.3 Fluxos de informações entre os processos componentes bem como com os demais processos corporativos;
1.7.2.4 Responsáveis pelos processos componentes;
1.7.2.5 Estrutura organizacional necessária ao perfeito funcionamento da infraestrutura;
1.7.2.6 Estratégia de implementação da infraestrutura de Segurança da Informação.
1.7.3 Deverá ser efetuada, ainda, a inclusão dos processos de infraestrutura de segurança da informação na estrutura organizacional do TJCE, a ser representada graficamente por meio do organograma da instituição.
1.7.4 Deverá ser observado que algumas das funções definidas não terão, necessariamente, unidade

operacional exclusiva sendo, portanto, desempenhadas por unidades já existentes;
1.7.5 A infraestrutura de Segurança da Informação a ser revisada deverá estar em conformidade com os tópicos relacionados ao assunto das normas ABNT NBR ISO/IEC 27002:2005 e ABNT NBR ISO/IEC 27001:2006.
1.7.6 O Modelo de Gestão de Segurança da Informação deverá contemplar toda a infraestrutura operacional e organizacional existente no TJCE.

1.7.7 PRODUTOS ESPERADOS:

1.7.7.1 Relatório com análise da estruturação e atuação do Comitê;
1.7.7.2 Relatório de Propostas de Melhoria;
1.7.7.3 Definições de infraestrutura de Segurança da Informação;
1.7.7.4 Modelo de gestão documentado, contendo: Descrição dos processos definidos; Funções definidas; Fluxo de informações entre os processos; Responsáveis pelos processos; Relatório de Modelo de Gestão de Segurança da Informação e Comunicações; Estratégia de implantação com a superposição dos processos definidos sobre as áreas responsáveis já existentes.

1.7.8 ATIVIDADES DE APOIO:

1.7.8.1 PLANO DE TRABALHO com o detalhamento do escopo da revisão e cronograma de execução;
1.7.8.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;
1.7.8.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

1.7.9 PRAZO DE ENTREGA:

1.7.9.1 O serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

1.8 DESCRIÇÃO DETALHADA PARA CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

1.8.1 Estabelecer diretrizes, critérios e procedimentos para análise, revisão, complementação, elaboração, atualização, institucionalização e divulgação da Política de Segurança da Informação – PSI do TJCE, retificando, ratificando ou incluindo normas, e da ABNT:
1.8.1.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.
1.8.1.2 Sistemas de gestão de segurança da informação - Requisitos - ABNT NBR ISO/IEC 27001:2006;
1.8.1.3 ABNT NBR ISO/IEC 27002:2005 - Código de Prática;
1.8.1.4 Gestão de riscos de segurança da informação - ABNT NBR ISO/IEC 27005:2008;
1.8.1.5 Gestão de continuidade de negócios - Parte 1: Código de prática ABNT NBR 15999-1:2007 e Parte 2: Requisitos - ABNT NBR 15999-2:2008.
1.8.2 Em legislação brasileira deverá ser observado, necessariamente, a seguinte legislação pertinente: Lei nº 9.983, de 14 de julho de 2000 (Código Penal).
1.8.3 Caso haja mudança dos normativos relacionados acima, as mudanças deverão ser, necessariamente, observadas e aplicadas durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas demandas normativas apresentadas;
1.8.4 Caso os normativos acima sejam, em sua totalidade ou em parte, substituídos, os novos normativos deverão ser, necessariamente, observados e aplicados;
1.8.5 Durante a execução dos serviços, deverá ser observada pela Contratada tantas mudanças quanto forem necessárias para adequar o Tribunal aos novos normativos em vigência;
1.8.6 Deverão ser considerados os resultados da análise de riscos, quanto aos aspectos relativos à falta de padronização e normatização das práticas de tratamento da informação corporativa;
1.8.7 Política de Segurança da Informação deverá ser revisada em conjunto com Grupo de Trabalho constituído por representantes dos diferentes setores do TJCE;
1.8.8 A Política de Segurança da Informação deverá ser composta por 3 (três) níveis:
1.8.8.1 Diretrizes Gerais – compreendendo as diretrizes e políticas de segurança, definidas de acordo com a estrutura organizacional, administrativa e funcional do TJCE, devendo conter, no mínimo, os temas abaixo, considerando as Normas específicas vigentes no ordenamento jurídico:
1.8.8.1.1 Tratamento da Informação;
1.8.8.1.2 Tratamento e Resposta de Incidentes de Rede;
1.8.8.1.3 Gestão de Risco;
1.8.8.1.4 Gestão de Continuidade;
1.8.8.1.5 Auditoria e Conformidade;
1.8.8.1.6 Controles de Acesso;
1.8.8.1.7 Uso de e-mail; e
1.8.8.1.8 Acesso a Internet.
1.8.8.2 Tático - compreende as regras de normatização das permissões e proibições no âmbito da

segurança corporativa da informação e comunicações;
1.8.8.3 Operacional – compreende as definições dos procedimentos de execução das ações de segurança e os padrões a serem adotados.
1.8.9 A empresa Contratada deverá rever e atualizar, necessariamente os normativos de segurança da informação, atualmente em vigor no tribunal:
1.8.10 Deverão ser elaborados, também, modelos de documentos auxiliares à implementação da Política de Segurança e Comunicações, como Termos de Compromisso, Termo de Ciência, dentre outros que se fizerem necessários;
1.8.11 Todos os documentos gerados deverão conter, no mínimo, as seções:
1.8.11.1 Objetivo;
1.8.11.2 Público alvo;
1.8.11.3 Descrição;
1.8.11.4 Definições;
1.8.11.5 Data de publicação;
1.8.11.6 Data de validade;
1.8.11.7 Data da última atualização;
1.8.11.8 Condições obrigatórias de atualização do documento;
1.8.11.9 Responsável pela atualização;
1.8.11.10 Dicionário de referência contendo os termos técnicos.
1.8.12 Para a divulgação da Política de Segurança da Informação deverão ser elaborado e fornecido pela contratada material informativo com os princípios gerais da Política de Segurança da Informação na forma de guia de consulta rápida;
1.8.13 A empresa contratada deverá elaborar e submeter à apreciação do TJCE um novo conjunto de normativos não contemplados, especificamente, pela atual política de segurança da informação do TJCE, conforme definido a seguir:
1.8.13.1 Norma de conformidade legal – Estabelece procedimento de checagem (checklist) da aderência legal dos contratos e procedimentos administrativos internos, em atendimento a legislação civil ou criminal, estatutos, regulamentações, normativos ou obrigações contratuais e requisitos de segurança da informação;
1.8.13.2 Norma de segregação de funções – Estabelece critérios para evitar controle total de um processo por parte de um único usuário do Tribunal, impedindo, assim, acúmulo de autoridade bem como uso acidental ou deliberado dos ativos corporativos em prejuízo do Tribunal e terceiros;
1.8.13.3 Norma de segurança para equipe técnica de TI do TJCE – Estabelece regras gerais para a administração/operacionalização de recursos de tecnologia da informação do Tribunal;
1.8.13.4 Norma para instalação e configuração segura de dispositivos de roteamento computacional – Estabelece regras de instalação e configuração segura, específicas para dispositivos de roteamento computacional, com revisão de procedimentos atualmente aplicados pelo Tribunal;
1.8.13.5 Norma para instalação e configuração segura de dispositivos de segurança da informação do TJCE - Estabelece regras de instalação e configuração segura a serem implementadas nos dispositivos de segurança da informação do TJCE, com revisão de procedimentos atualmente aplicados pelo Tribunal;
1.8.13.6 Norma para instalação e configuração segura de sistemas operacionais – Estabelece regras seguras que deverão ser observadas quanto à instalação e configuração de sistemas operacionais corporativos, com revisão de procedimentos atualmente aplicados pelo Tribunal;
1.8.13.7 Norma para instalação e configuração de aplicações – Estabelece regras seguras que deverão ser observadas quanto à instalação e configuração de aplicações, com revisão de procedimentos atualmente aplicados pelo Tribunal;
1.8.13.8 Norma de Segurança para SLA (Servise Level Agreement) Acordo de Nível de Serviço – Estabelece regras seguras que deverão ser observadas e utilizadas nos contratos baseados em acordo de nível de serviço;
1.8.13.9 Norma de aspectos da Gestão da Continuidade de Negócio – Estabelece regras seguras que deverão ser observadas e utilizadas na gestão da continuidade do negócio;
1.8.13.10 Norma com aspectos da Gestão de Riscos – Estabelece regras seguras que deverão ser observadas e utilizadas na gestão de riscos;
1.8.13.11 Norma de Computação Móvel e Trabalho Remoto – Estabelece regras seguras que deverão ser observadas e utilizadas para a computação móvel e trabalho remoto;
1.8.13.12 Norma de Uso de Redes Sociais – Estabelece regras seguras que deverão ser observadas e utilizadas no uso de redes sociais, regulação, monitoramento e código de conduta;
1.8.13.13 Norma de Classificação e Tratamento de Incidentes Computacionais – Estabelece regras seguras que deverão ser observadas e utilizadas no tratamento de incidentes, contendo no mínimo:
1.8.13.13.1 O que constitui um incidente de segurança da informação;
1.8.13.13.2 Como este incidente deve ser tratado;
1.8.13.13.3 Quais os ativos críticos que devem ser protegidos.
1.8.13.13.4 Termos a serem abordados na norma:
1.8.13.13.4.1 Atividades de tratamento de incidente; Artefatos; Ataques; Eventos; Incidentes; Intrusão; Reporte de incidente; Probe/Scan; Vulnerabilidade e Tratamento da vulnerabilidade.

1.8.13.14 Norma de implementação, operacionalização, manutenção e acesso às redes sem fio do TJCE – Estabelece procedimento de implementação, operacionalização, manutenção e acesso às redes sem fio do TJCE. Esta norma deverá conter:
1.8.13.14.1 As melhores práticas de segurança da informação relativas às redes sem fio comercialmente oferecidas no mundo;
1.8.13.14.2 Orientações para a realização periódica de testes de invasão e análise de riscos e vulnerabilidades em redes sem fio;
1.8.13.14.3 Segregação de tarefas na administração da solução de redes sem fio do TJCE;
1.8.13.14.4 Política de educação dos usuários com relação à segurança no manuseio da solução em questão;
1.8.13.14.5 Regras de instalação, configuração, gerenciamento, administração, localização e aprovação de Pontos de Acesso nas dependências do Tribunal;
1.8.13.14.6 Modo de operação de cartões de rede que acessam as redes sem fio do Tribunal;
1.8.13.14.7 Concessão e revogação de privilégios de acesso para usuários comuns e usuários privilegiados (técnicos);
1.8.13.14.8 Orientações com relação à atualização desta norma, a partir da mudança do parque computacional do TJCE que suporta esta solução sem fio (manter a norma sempre coerente com a evolução tecnológica das redes sem fio do Tribunal);
1.8.13.14.9 Indicação de que todos os técnicos envolvidos com o constante suporte desta solução deverão passar por treinamento específico, a partir da alteração/mudança/atualização dos ativos de TI relacionados às redes sem fio do Tribunal;
1.8.13.14.10 Orientações com relação à requisição de níveis específicos de autenticação para acesso a aplicações críticas do Tribunal;
1.8.13.14.11 A exigência de que todos os dispositivos de rede sem fio operem somente em modo de infraestrutura (infrastructure mode);
1.8.13.14.12 Orientações de como proceder, caso o usuário necessite utilizar os dispositivos de rede sem fio do TJCE (notebooks) fora das dependências do Tribunal (acesso a redes sem fio públicas).
1.8.13.15 Norma sobre uso de dispositivos móveis dentro do TJCE – Estabelece procedimento de implementação, operacionalização e manutenção de regras e diretrizes no uso de dispositivos móveis nos aspectos relativos a Segurança da Informação e Comunicação em âmbito do Tribunal. Esta norma deverá criar os seguintes atores responsáveis pelo manuseio dos dispositivos móveis:
1.8.13.15.1 Agentes públicos com dispositivos móveis corporativos;
1.8.13.15.2 Agentes públicos com dispositivos móveis particulares;
1.8.13.15.3 Agente Responsável;
1.8.13.15.4 Dispositivos móveis;
1.8.13.15.5 Usuários visitantes com dispositivos móveis;
1.8.13.15.6 Dispositivos móveis removíveis de armazenamento;

1.8.14 PRODUTOS ESPERADOS:

1.8.14.1 Relatório com Análise das Normas vigentes;
1.8.14.2 Relatório de Propostas de Melhoria das Normas vigentes;
1.8.14.3 Documento de Política de Segurança da Informação, com o novo conjunto de normativos;
1.8.14.4 Documento para formalização e aprovação por parte da autoridade máxima responsável;
1.8.14.5 Dicionário dos termos técnicos utilizados nos documentos;
1.8.14.6 Sumário executivo para apresentação à alta Administração;
1.8.14.7 Guia de consulta rápida com os princípios gerais da Política de Segurança da Informação e para a divulgação da Política de Segurança da Informação;

1.8.15 ATIVIDADES DE APOIO:

1.8.15.1 PLANO DE TRABALHO com o detalhamento do escopo da revisão e cronograma de execução;
1.8.15.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;
1.8.15.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

1.8.16 PRAZO DE ENTREGA:

1.8.16.1 O serviço deverá ser executado em até 90 (noventa) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

1.9 DESCRIÇÃO DETALHADA PARA ELABORAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL

1.9.1 Implantar processos de Gestão de Continuidade de Negócios buscando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do TJCE, além de permitir que sejam recuperados ativos da informação a um nível aceitável por intermédio de ações de prevenção, resposta e recuperação.
1.9.2 Deverão ser considerados os resultados da análise de riscos, quanto aos aspectos relativos ao

levantamento de risco físico e valoração dos ativos e sistemas de informação.
1.9.3 O escopo do projeto será definido com base na análise de impacto onde deverão ser considerados apenas os ativos que fazem parte da missão critico-institucional do Tribunal, levantados e identificados previamente pela empresa Contratada e acordados com o TJCE.
1.9.4 Deverá ser realizada coleta de dados junto aos responsáveis da Secretaria de Tecnologia da Informação - SETIN para a definição das operações críticas realizadas pela área, definir e elaborar os planos de recuperação.
1.9.4.1 A SETIN poderá solicitar que seja realizada coleta de dados junto às áreas gestoras, responsáveis pela alimentação dos sistemas e bancos de dados;
1.9.5 Deverá ser gerado um documento descrevendo o plano de recuperação de desastres em ambiente computacional do TJCE (PRDAC-TJCE) para o escopo definido na análise de riscos, considerando os normativos aplicáveis.
1.9.5.1 O programa deverá prover o TJCE com ações e ferramentas que possibilitem a recuperação de sistemas e redes computacionais ao seu estado normal de operação no MENOR TEMPO POSSÍVEL (tempo a ser definido com base no resultado do levantamento realizado pela contratada em relação aos processos e tecnologias críticas que mantêm os negócios essenciais do TJCE com clara concordância do Tribunal).
1.9.6 Normativos aplicáveis quando da elaboração, implantação e manutenção do PRDAC-TJCE:
1.9.6.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.
1.9.6.2 Normativos internacionais - deverá se observado, NO QUE FOR PERTINENTE, a seguinte base normativa:
1.9.6.2.1 NIST SP 800-34;
1.9.6.2.2 NIST SP 800-34 REV1
1.9.6.2.3 COBIT v4.1, em especial os processos AI2, DS1, DS2, DS4, DS8, DS11, DS13, PO2 e PO9;
1.9.6.2.4 ITIL v3, em especial os processos SD4.5, CSI5.6.3, SD4.4.5.2 e SO5.2;
1.9.6.2.5 ISO/IEC 24762;
1.9.6.2.6 BS 25777;
1.9.6.2.7 BS 25999;
1.9.6.3 Normativos ABNT - deverá ser observado, NO QUE FOR PERTINENTE, os seguintes normativos da ABNT:
1.9.6.3.1 ABNT NBR ISO/IEC 15999#1:2007;
1.9.6.3.2 ABNT NBR ISO/IEC 27005:2008;
1.9.6.3.3 ABNT NBR ISO/IEC 27002:2005.
1.9.6.3.4 ABNT NBR ISO 22301:2013.
1.9.7 A empresa Contratada deverá identificar e sugerir mudanças na infraestrutura das redes computacionais do TJCE para atender a continuidade das atividades de TI do Tribunal dentro dos novos padrões de recuperação tecnológica propostos.
1.9.8 O plano de recuperação de desastres em ambiente computacional do TJCE a ser implementado precisará abordar:
1.9.8.1 Requisitos estratégicos de continuidade computacional relativos aos processos e às atividades operacionais;
1.9.8.2 Ações para mitigação de riscos, reação durante um evento e recuperação depois de um evento;
1.9.8.3 Priorização de processos críticos de negócio suportados pela TI.
1.9.9 A produção do plano de recuperação de desastres em ambiente computacional do TJCE deverá considerar:
1.9.9.1 A conformidade com os requisitos de segurança da informação e comunicações necessárias à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, o que inclui pessoas, processos, infraestrutura e recursos de tecnologia da informação e comunicações do Tribunal;
1.9.9.2 Os requisitos de uma atualização anual do Programa;
1.9.10 A empresa contratada deverá:
1.9.10.1 Obedecer, no mínimo, as seguintes fases para a produção do PRDAC:
1.9.10.1.1 PREVENÇÃO/REDUÇÃO/MITIGAÇÃO;
1.9.10.1.2 REAÇÃO;
1.9.10.1.3 RECUPERAÇÃO;
1.9.10.2 Apresentar, no mínimo, os seguintes planos, componentes do PRDAC e seus sub-planos claramente identificados dentro deste programa:
1.9.10.2.1 PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;
1.9.10.2.2 PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS;
1.9.10.2.3 PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA);
1.9.10.2.4 PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;
1.9.10.2.5 PLANO DE TESTES E EXERCÍCIOS;

1.9.10.2.6 PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE;
1.9.10.2.7 PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL;
1.9.10.2.8 PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS.
1.9.11 Na fase de PREVENÇÃO/REDUÇÃO/MITIGAÇÃO a empresa contratada deverá:
1.9.11.1 Apresentar o PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE, onde deverão ser abordadas as necessidades de recuperação de desastres computacionais do Tribunal, a organização e administração do PRDAC -TJCE;
1.9.11.2 Avaliar os riscos computacionais associados aos processos críticos e atividades operacionais do TJCE e apresentar o PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS;
1.9.11.3 Apresentar o PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA), onde serão identificadas as operações críticas do Tribunal apoiadas pela TI, bem como os recursos necessários para sustentar estas operações;
1.9.11.4 Apresentar o PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE, onde deverá ser demonstrada a metodologia de desenvolvimento do PRDAC –TJCE, bem como sua organização, forma de implantação e documentação;
1.9.11.5 Apresentar o PLANO DE TESTES E EXERCÍCIOS, onde deverão constar os tipos de testes e exercícios a serem aplicados no ambiente computacional do Tribunal de acordo com a suas peculiaridades e características;
1.9.11.6 Apresentar o PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE, onde deverão ser abordadas as metodologias de auditoria, revisão e manutenção do PRDAC-TJCE;
1.9.11.7 Estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho da entidade, bem como as técnicas para quantificar e qualificar esses impactos. Deverá ser estimado, também, a criticidade dos processos computacionais do Tribunal, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.
1.9.12 PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE
1.9.12.1 A empresa contratada deverá definir com o TJCE:
1.9.12.1.1 O objetivo do PRDAC;
1.9.12.1.2 A montagem/treinamento de equipes específicas para apoio do PRDAC.
1.9.12.2 Deverá conter, entre outros artefatos considerados importantes pela empresa contratada, os seguintes produtos:
1.9.12.2.1 Proposta de PRDAC para a TI;
1.9.12.2.2 Estrutura do PRDAC em detalhes que possam identificar TODAS AS AÇÕES E ATIVIDADES PERTINENTES À CORRETA RECUPERAÇÃO DE DESASTRES COMPUTACIONAIS DO TJCE;
1.9.12.2.3 Definição de terminologias e pontos essenciais aplicados ao PRDAC;
1.9.12.2.4 Método de gerenciamento de mudanças no PRDAC;
1.9.12.2.5 Papel, no mínimo, das seguintes equipes:
1.9.12.2.5.1 Planejamento:
1.9.12.2.5.1.1 Direção da SETIN;
1.9.12.2.5.1.2 Equipe de desenvolvimento e manutenção do PRDAC.
1.9.12.2.6 Resposta:
1.9.12.2.6.1 Equipe de resposta à emergência computacional;
1.9.12.2.6.2 Equipe de avaliação de danos;
1.9.12.2.6.3 Equipe de comunicação.
1.9.12.2.7 Recuperação:
1.9.12.2.7.1 Equipe de recuperação operacional e tecnológica;
1.9.12.2.7.2 Equipe associada de suporte.
1.9.12.3 As equipes acima poderão ser agrupadas caso não haja prejuízo das atividades a serem desenvolvidas e caso a direção da SETIN assim o determine.
1.9.13 PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS:
1.9.13.1 Deverão ser atendidos, no mínimo, os seguintes elementos-chave da gestão de continuidade de negócios do TJCE, pertinentes também a TI, segundo a norma ABNT NBR ISO/IEC 27002:2005:
1.9.13.1.1 Entendimento dos riscos a que a organização esta exposta;
1.9.13.1.2 Identificação de todos os ativos de TI envolvidos em processos críticos de negócio;
1.9.13.1.3 Entendimento do impacto que incidentes computacionais com envolvimento da segurança da informação terão sobre os negócios;
1.9.13.1.4 Probabilidade e impacto da interrupção de TODOS OS PROCESSOS COMPUTACIONAIS CRÍTICOS DO TRIBUNAL, tanto em escala de dano quanto em relação ao período de recuperação;
1.9.13.2 Deverão ser demonstradas a identificação, quantificação e priorização dos critérios baseados nos riscos, com a identificação e inclusão de TODOS OS RECURSOS CRÍTICOS COMPUTACIONAIS, IMPACTO DE INTERRUPÇÃO E PRIORIDADE DE RECUPERAÇÃO DESTES RECURSOS DO TJCE;
1.9.13.3 A empresa contratada deverá levar em consideração, no mínimo, os riscos advindos de:
1.9.13.3.1 Riscos naturais (inundações, incêndios, etc.);

1.9.13.3.2 Riscos humanos (greves, paralisações, empregados mal preparados, etc.);
1.9.13.3.3 Riscos técnicos (ambiente computacional, datacenter, comunicação de dados, rede telefônica, energia, etc.);
1.9.13.4 A empresa também deverá:
1.9.13.4.1 Classificar, pontuar os riscos e apresentar matrizes de riscos;
1.9.13.4.2 Agrupar os riscos interdependentes;
1.9.13.4.3 Reconhecer, documentar e priorizar riscos à organização;
1.9.13.4.4 Identificar e mapear os impactos qualitativos e quantitativos de um evento de risco;
1.9.13.4.5 Identificar e avaliar os tipos de controles em operação. Incluir custo de manutenção destes controles;
1.9.13.4.6 Sugerir melhoras nos controles existentes por meio de documentação, capacitação, reforço, manutenção e testes. Apresentar custo/benefício dos controles.
1.9.13.4.7 Recomendar controles adicionais;
1.9.13.4.8 Auditar funções e responsabilidades e apresentar recomendações de mudanças pertinentes;
1.9.13.5 O PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS deverá conter ainda, entre outros artefatos considerados importantes pela empresa contratada, os seguintes produtos:
1.9.13.5.1 Eventos e exposições de alta frequência e impacto;
1.9.13.5.2 Lista de controles e proteção;
1.9.13.5.3 Priorização dos riscos e investimentos;
1.9.13.5.4 Coleta externa e interna de dados para avaliação de riscos.
1.9.14 PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA):
1.9.14.1 Deverá ser realizada uma Análise de Impacto nos Negócios (Business Impact Analysis – BIA) do TJCE, com objetivo de:
1.9.14.1.1 Avaliar a criticidade dos processos tecnológicos de sistemas de informação;
1.9.14.1.2 Estimar a importância dos ativos de sustentação tecnológica da organização;
1.9.14.1.3 Definir os tempos máximos de parada e recuperação (RTO – Recovery Time Objective) e de perda de dados (RPO – Recovery Point Objective);
1.9.14.1.4 Levantar, mapear e propor solução para todo inter-relacionamento entre os fornecedores de TI do TJCE e os sistemas críticos do Tribunal, com relação ao adequado tempo de recuperação dos ativos computacionais críticos do Tribunal;
1.9.14.1.5 Levantar e mapear os conhecimentos internos associados à recuperação destes sistemas bem como sequências lógicas de ações para o correto reestabelecimento das atividades críticas do Tribunal;
1.9.14.1.6 Definir os processos e ativos que serão contemplados nos planos, bem como sua ordem de priorização.
1.9.14.2 Deverá, após identificação dos riscos computacionais, categorizar e priorizar as operações computacionais críticas do TJCE e seus inter-relacionamentos e sugerir orçamentos/recursos necessários para mantê-las em atividade.
1.9.14.3 Deverão ser observados e atendidos os seguintes itens:
1.9.14.3.1 Fornecer:
1.9.14.3.2 Alternativas de estratégias de recuperação de desastres;
1.9.14.3.3 Informações sobre possíveis perdas.
1.9.14.3.4 Estabelecer:
1.9.14.3.4.1 Objetivos de recuperação no tempo (RTO).
1.9.14.3.5 Determinar:
1.9.14.3.5.1 Prazos de recuperação e exigências mínimas de recursos.
1.9.14.3.6 Avaliar:
1.9.14.3.6.1 Os possíveis impactos da interrupção ao longo do tempo.
1.9.14.3.7 Identificar os seguintes fatores de impacto:
1.9.14.3.7.1 Operacionais;
1.9.14.3.7.2 Financeiros;
1.9.14.3.8 Apresentar:
1.9.14.3.8.1 Relatório executivo com informações relevantes levantadas na fase do BIA.
1.9.14.3.9 Realizar as seguintes fases com contextualização pertinente e apresentação de resultados:
1.9.14.3.9.1 Planejamento do projeto de BIA;
1.9.14.3.9.2 Coleta e análise de dados;
1.9.14.3.9.3 Documentação dos achados.
1.9.14.3.10 Definir, junto com o TJCE, as áreas foco da BIA;
1.9.14.3.11 Identificar e apresentar custos do impacto das interrupções dos processos computacionais críticos do TJCE nos seguintes aspectos:
1.9.14.3.11.1 Financeiro;
1.9.14.3.11.2 Cidadão;
1.9.14.3.11.3 Legal/regulamentação;
1.9.14.3.11.4 Ambiental;
1.9.14.3.11.5 Operacional;

1.9.14.3.11.6 Público interno;
1.9.14.3.11.7 Contratual.
1.9.14.3.12 Períodos de recuperação:
1.9.14.3.12.1 Determinar o RTO para as funções computacionais críticas identificadas;
1.9.14.3.12.2 Determinar a ordem de recuperação (criticidade) das atividades computacionais;
1.9.14.3.12.3 Determinar o RPO;
1.9.14.3.12.4 Determinar a necessidades de recursos para recuperação e continuidade das funções críticas e sistemas de suporte;
1.9.14.3.12.5 Determinar a época de substituição de recursos;
1.9.14.3.12.6 Apresentar cronograma de restauração de recursos.
1.9.15 PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE
1.9.15.1 A empresa contratada deverá demonstrar a metodologia de desenvolvimento do PRDAC-TJCE e apresentar a documentação, implementação e organização do plano em questão.
1.9.15.2 A empresa contratada também deverá:
1.9.15.2.1 Observar os seguintes elementos do PRDAC:
1.9.15.2.1.1 Pessoas;
1.9.15.2.1.2 Locais;
1.9.15.2.1.3 Informação;
1.9.15.2.1.4 Recursos;
1.9.15.2.1.5 Processos.
1.9.15.2.2 Definir no PRDAC:
1.9.15.2.2.1 Linhas de tempo;
1.9.15.2.2.2 Objetivos;
1.9.15.2.2.3 Produtos;
1.9.15.2.2.4 Documentação especifica;
1.9.15.2.2.5 Premissas;
1.9.15.2.2.6 Cenários;
1.9.15.2.2.7 Procedimento de distribuição e controle;
1.9.15.2.2.8 Tipos de segurança aplicadas aos documentos;
1.9.15.2.2.9 Períodos para revisões do PRDAC.
1.9.15.2.3 Na confecção do plano, abordar:
1.9.15.2.3.1 Locais;
1.9.15.2.3.2 Processos de negócio;
1.9.15.2.3.3 Catalogação, por níveis, dos possíveis impactos advindos da interrupção dos processos e serviços críticos do TJCE;
1.9.15.2.3.4 Estratégias recomendadas para a devida recuperação de desastres em ambiente computacional do TJCE;
1.9.15.2.3.5 Projeção de validade e atualização deste plano pelo prazo de 05 (cinco) anos.
1.9.15.2.4 Observar os seguintes componentes do PRDAC:
1.9.15.2.4.1 Visão geral;
1.9.15.2.4.2 Gerenciamento de incidentes;
1.9.15.2.4.3 Grupos e tarefas;
1.9.15.2.4.4 Processo críticos;
1.9.15.2.4.5 Contatos críticos;
1.9.15.2.4.6 Tecnologias envolvidas (Identificação dos ativos computacionais que suportam estes processos críticos);
1.9.15.2.4.7 Registros vitais e armazenamento externo;
1.9.15.2.4.8 Equipamentos e suprimentos;
1.9.15.2.4.9 Manutenção do plano;
1.9.15.2.4.10 Anexos.
1.9.15.3 O plano deverá ter CARÁTER GERENCIAL, com linguagem clara e objetiva, para exposição à DIRETORIA DE TECNOLOGIA do Tribunal, avaliação e validação.
1.9.15.4 A empresa contratada deverá apresentar PLANEJAMENTO para manutenção do PRDAC-TJCE.
1.9.15.5 Deverão ser apresentadas TODAS AS HIPÓTESES ONDE O PRDAC-TJCE PRECISARÁ SER ATUALIZADO, levando em conta a criticidade das operações internas e observando a metodologia de gerenciamento de mudanças já implantada corporativamente.
1.9.16 PLANO DE RECUPERAÇÃO DE OPERAÇÕES
1.9.16.1 Deverá ser baseado nos levantamentos/mapeamentos realizados na infraestrutura operacional do TJCE que suportam os processos computacionais críticos do Tribunal;
1.9.16.2 A empresa contratada deverá observar e apresentar roteiro / manuais / procedimentos que habilitem as pessoas a, em caso de situações de contingência corporativa, seguir determinadas linhas de ação para conter os danos provocados por paradas nas soluções computacionais críticas do TJCE. Estes roteiros/manuais/procedimentos deverão ser objetivos, claros e possibilitar, efetivamente, o

contingenciamento das situações apresentadas. Deverá, também, identificar as ações a que cada equipe mapeada no processo de recuperação estará responsável.
1.9.16.3 O plano deverá prever, entre outros insumos:
1.9.16.4 Alternativas para evitar paradas dos processos computacionais críticos do TJCE, devendo ser considerado e analisado, de acordo com os níveis de criticidade das soluções de negócio do TJCE suportadas pela TI, a melhor alternativa, levando-se em considerações soluções de mercado como:
1.9.16.4.1 Plano COLD SITE;
1.9.16.4.2 Plano WARM SITE;
1.9.16.4.3 Plano HOT SITE;
1.9.16.4.4 Contratos de reciprocidade;
1.9.16.4.5 Plano SITE ESPELHO;
1.9.16.4.6 Os tipos de armazenamentos fora do TJCE, como armazenamento online de dados e logs críticos, espelhamentos de base de dados;
1.9.16.4.7 As frequências destes armazenamentos;
1.9.16.4.8 Os tipos de backups usados: incremental, completo, diferencial;
1.9.16.5 O armazenamento, fora das dependências do Tribunal, de seu PRDAC – TJCE, com a devida segurança/controle de acesso. Esta segurança deverá ser compatível e/ou superior à segurança aplicada em ambiente interno e observar os processos DS4.9 do COBIT, SO 5.2.3 do ITIL v3 e item 10.5.1 da ABNT NBR ISO/IEC 27002:2005.
1.9.16.6 Estabelecer metodologias para acionamento de equipes de recuperação computacional do TJCE, onde deverá constar TODAS AS TAREFAS AFETAS ÀS EQUIPES, os recursos necessários (tecnologia, pessoal, informações, etc), os detalhes de contatos internos e externos, quem, como e quando acionar, entre outros;
1.9.16.7 Propor prazos para que as equipes de recuperação sejam acionadas;
1.9.16.8 Apresentar custos estimados para atendimento das alternativas mencionadas;
1.9.16.9 Apresentar pré-requisitos operacionais / técnicos / corporativos e de infraestrutura computacional para manter as soluções críticas do TJCE em constante operação;
1.9.16.10 Propor, a partir da análise do PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS, as situações, condições e ocorrências que determinarão o acionamento das equipes de recuperação mencionadas.
1.9.17 PLANO DE TESTES E EXERCÍCIOS
1.9.17.1 A empresa contratada deverá:
1.9.17.1.1 Demonstrar os tipos de testes e exercícios pertinentes ao âmbito do Tribunal, incluindo:
1.9.17.1.1.1 Simulação de PARADA TOTAL dos sistemas críticos do TJCE;
1.9.17.1.1.2 Simulação de PARADA PARCIAL dos sistemas críticos do TJCE;
1.9.17.1.1.3 Simulação de checagem dos procedimentos pertinentes implementados junto à equipe de restauração/recuperação;
1.9.17.1.1.4 Indicação de como e quando cada elemento do plano será testado;
1.9.17.1.1.5 Simulação de diferentes cenários e diferentes formas de interrupção;
1.9.17.1.1.6 Apresentação de ações de recuperação em ambientes/locais alternativos;
1.9.17.1.1.7 As prioridades, frequência e tipos de testes e exercícios aplicáveis ao Tribunal.
1.9.17.2 Os testes e exercícios deverão ser realizados, também, de forma geral (testando se o TJCE, seu pessoal, equipamentos, recursos e processos podem enfrentar interrupções).
1.9.17.2.1 Definir testes em:
1.9.17.2.1.1 Equipamentos;
1.9.17.2.1.2 Tecnologias;
1.9.17.2.2 Selecionar método de testes/exercícios que:
1.9.17.2.2.1 Possam testar o plano em sua máxima extensão possível;
1.9.17.2.2.2 Custos não sejam proibitivos para o TJCE;
1.9.17.2.2.3 Interrupções de trabalho sejam mínimas;
1.9.17.2.2.4 Resultados possibilitem alto grau de confiabilidade na capacidade de recuperação;
1.9.17.2.2.5 Resultados demonstrem que as ações aplicadas foram efetivamente aprendidas pelo TJCE;
1.9.17.3 Realizar testes de interdependência entre diferentes tecnologias computacionais;
1.9.17.4 Estabelecer regras de confidencialidade pertinentes.
1.9.17.5 Observa-se que parte dos testes deste plano foram coletados e deverão obedecer a norma ABNT NBR ISO/IEC 27002:2005 com a devida aplicação junto a TI.
1.9.17.6 Deverá ser executado 1 (um) teste de mesa para validação dos planos elaborados.
1.9.17.7 Deverão ser definidos claramente os objetivos do(s) teste(s), sendo preparados checklists de acompanhamento e validação.
1.9.17.8 Deverá ser elaborado relatório contendo os resultados obtidos no(s) teste(s).
1.9.17.9 Ao final do(s) teste(s), o plano deverá ser atualizado de acordo com os resultados obtidos.
1.9.18 PLANOS DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC -TJCE
1.9.18.1 A empresa contratada deverá apresentar:
1.9.18.1.1 Metodologia de revisão/atualização do PRDAC-TJCE bem como respectiva metodologia de

auditoria;
1.9.18.1.2 Proposta e aplicação de manutenção do PRDAC-TJCE;
1.9.18.1.3 Fatores de mudança do Programa;
1.9.18.1.4 Procedimentos para controle da documentação do PRDAC-TJCE.
1.9.18.2 Deverão ser inseridos nos PLANOS DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE as seguintes atividades, dentre outras consideradas importantes pela empresa contratada:
1.9.18.2.1 No plano de MANUTENÇÃO:
1.9.18.2.1.1 Definição de responsabilidades;
1.9.18.2.1.2 Manutenção programada;
1.9.18.2.1.3 Manutenção não programada;
1.9.18.2.1.4 Inclusão de todos os ativos tecnológicos críticos do TJCE.
1.9.18.2.2 No plano de REVISÃO:
1.9.18.2.2.1 Aplicação de metas e métodos pertinentes;
1.9.18.2.2.2 Identificação de fatores de mudanças;
1.9.18.2.2.3 Revisão completamente documentada;
1.9.18.2.3 No plano de AUDITORIA a empresa deverá fornecer ao TJCE, após análise do PRDAC-TJCE, clara evidência da gestão eficiente e eficaz de TODO O PROCESSO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TRIBUNAL.
1.9.18.2.4 Os procedimentos de auditoria aplicados deverão obedecer, dentro da devida pertinência, aos requisitos elencados nos normativos federais, internacionais e da ABNT abordados neste programa, propondo, a partir do resultado de cada auditoria, melhorias e alterações pertinentes ao PRDAC-TJCE.
1.9.18.3 As auditorias acima referidas deverão ser realizadas nas instalações do TJCE e de forma SEMESTRAL enquanto perdurar a vigência contratual entre o Tribunal e a empresa contratada.
1.9.19 Na fase de REAÇÃO a empresa contratada deverá:
1.9.19.1 Apresentar o PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL, com a finalidade de:
1.9.19.1.1 Propor procedimentos de comunicação pertinentes;
1.9.19.1.2 Propor a estabilização dos locais afetados;
1.9.19.1.3 Propor a minimização de danos ocorridos;
1.9.19.1.4 Identificar:
1.9.19.1.4.1 Tipos de emergências pertinentes ao Tribunal;
1.9.19.1.4.2 Atuais procedimentos implementados pelo TJCE bem como recomendar novas ações de resposta a emergência;
1.9.19.1.4.3 Equipes e tarefas;
1.9.19.2 Estabelecer, junto com o TJCE, notificação de autoridades apropriadas em horário comercial e fora deste horário;
1.9.19.3 Desenvolver:
1.9.19.3.1 Notificação de emergência identificando:
1.9.19.3.1.1 Propósitos;
1.9.19.3.1.2 Objetivos;
1.9.19.3.1.3 Sequência de notificação;
1.9.19.3.2 Alarmes.
1.9.20 Na fase de RECUPERAÇÃO a empresa contratada deverá apresentar o PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS.
1.9.20.1 O plano terá por finalidade:
1.9.20.1.1 Apresentar diretrizes de uma comunicação eficaz, coleta e avaliação de informações relevantes, público-alvo da crise e porta-voz nomeado para representação do Tribunal em situações de crise;
1.9.20.1.2 Identificar ações necessárias para contenção dos danos advindos do desastre ocorrido;
1.9.20.1.3 Apresentar orientações sobre recuperação e avaliação de danos.
1.9.20.2 A empresa contratada deverá propor PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS que possibilite a manutenção da disponibilidade da informação no nível e escala de tempo requeridos pelo TJCE, após a ocorrência de interrupções ou falhas dos processos computacionais críticos do Tribunal, conforme observado pelo item 14.1.3 da norma ABNT NBR ISO/IEC 27002:2005.
1.9.20.3 A empresa deverá levantar e identificar, junto com o TJCE, as seguintes informações que comporão o plano em questão:
1.9.20.3.1 Objetivo e escopo;
1.9.20.3.2 Papéis e responsabilidades;
1.9.20.3.3 Autoridade responsável;
1.9.20.3.4 Detalhes de contato;
1.9.20.3.5 Lista de tarefas;
1.9.20.3.6 Fases do plano de recuperação;
1.9.20.3.7 Recursos necessários;
1.9.20.3.8 Perda aceitável de informações e serviços;
1.9.20.3.9 Implementação de procedimentos que possibilitem a recuperação e restauração das operações computacionais e da disponibilidade da informação nos prazos necessários (prazos a serem apresentados

como resultado da análise de impacto computacional no negócio do TJCE - BIA). Estes procedimentos de recuperação deverão:
1.9.20.3.9.1 Descrever ações detalhadas para a transferência das atividades computacionais críticas do Tribunal para localidade alternativa temporária e reativação destas atividades no prazo determinado;
1.9.20.3.9.2 Descrever ações a serem adotadas quando do restabelecimento das operações;
1.9.20.3.10 Avaliação de dependências computacionais externas ao negócio e contratos existentes;
1.9.20.3.11 Procedimentos que permitam a finalização de restaurações e recuperações pendentes;
1.9.20.3.12 Documentação de processos e procedimentos de recuperação;
1.9.20.3.13 Treinamento adequado dos responsáveis pelo acompanhamento e ações relativas aos processos e procedimentos de recuperação;
1.9.20.3.14 Procedimentos operacionais temporários durante a conclusão da recuperação e restauração pertinentes;
1.9.20.3.15 Programação de manutenção que especifique quando e como este plano deverá ser testado e o modo de se proceder a sua manutenção;
1.9.20.4 Observa-se que os itens acima, a constituírem o PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS DO TJCE, refletem as instruções emanadas pelas normas ABNT NBR ISO/IEC 27002:2005, que deverão ser obedecidas pela empresa contratada.
1.9.20.5 Observa-se, ainda, que o plano deverá:
1.9.20.5.1 Apresentar períodos de tempo (dias/horas/minutos) para recuperação de atividades/sistemas/processos computacionais críticos do TJCE (RTO). Apresentar, ainda, método de classificação de itens, categorias de negócios críticos e relacioná-los aos períodos acima;
1.9.20.5.2 Apresentar planejamento que determine o ponto no tempo onde as atividades/sistemas/processos computacionais críticos do TJCE serão recuperadas após interrupções (RPO). Este planejamento deverá estar alinhado à metodologia de armazenamento e backup apresentada pelo PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;
1.9.20.5.3 Apresentar estimativas de tempo de recuperação para:
1.9.20.5.3.1 Datacenter corporativo;
1.9.20.5.3.2 Redes e comunicação de dados corporativos;
1.9.20.5.3.3 Help-Desk corporativo.
1.9.20.6 As equipes formadas para gerenciamento do processo de recuperação do ambiente computacional deverão ser plenamente capacitadas para responder às possíveis situações de crises levantadas neste Programa. Deverá ainda ser apresentado o mapeamento de TODAS AS TAREFAS AFETAS A ESTAS EQUIPES, DE FORMA ESPECÍFICA. Estas tarefas deverão possibilitar aos responsáveis o tratamento da crise do começo ao final, inclusive após a normalização das atividades/serviços críticos afetados.
1.9.20.7 O PLANO ainda deverá conter o REGISTRO DE INFORMAÇÃO DO PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAL, abaixo mencionado.
1.9.21 REGISTRO DE INFORMAÇÃO DO PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAL
1.9.21.1 A empresa contratada deverá apresentar planejamento para implementação de sistema que possibilite ao TJCE recuperar TODAS AS INFORMAÇÕES INERENTES A DESASTRES, PARADAS DE SISTEMAS e RECUPERAÇÃO DE SUAS OPERAÇÕES CRÍTICAS.
1.9.22 O PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS deverá compreender somente os dados e equipamentos da Sala Cofre, sob supervisão da área de Tecnologia da Informação.

1.9.23 PRODUTOS ESPERADOS:

1.9.23.1 Na 1ª execução:
1.9.23.1.1 Plano de Recuperação de Desastres em Ambiente Computacional (PRDACTJCE);
1.9.23.1.2 RELATÓRIO INICIAL para o TJCE, após levantamento realizado nas dependências da SETIN, de todas as soluções computacionais em vigência no Tribunal relativas à recuperação de seus ativos tecnológicos, com demonstrativo da situação atual do Tribunal e a situação futura (a partir do levantamento e apresentação do PRDAC-TJCE);
1.9.23.1.3 PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;
1.9.23.1.4 PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS;
1.9.23.1.5 PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA);
1.9.23.1.6 PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;
1.9.23.1.7 PLANO DE RECUPERAÇÃO DE OPERAÇÕES;
1.9.23.1.8 PLANO DE TESTES E EXERCÍCIOS;
1.9.23.1.9 PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE;
1.9.23.1.10 PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL;
1.9.23.1.11 PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS.
1.9.23.1.12 Treinamento das equipes de recuperação de desastres;
1.9.23.1.13 Relatórios de testes realizados;

1.9.23.2 Nas demais execuções durante a vigência do contrato a empresa contratada deverá revisar o PRDAC-TJCE, incluídos todos os planos que fazem parte deste programa, nas seguintes hipóteses:
1.9.23.2.1 Mudança normativo-legal federal relativo à continuidade de negócios no que tange a TI;
1.9.23.2.2 Mudança em normativos internacionais afetos à continuidade de negócios no que tange a TI;
1.9.23.2.3 Mudança e acréscimos de normativos ABNT inerentes ao PRDAC -TJCE;
1.9.23.2.4 Criação de novos normativos nacionais e/ou internacionais que venham a agregar dados e informações que possibilitem a melhora do PRDAC-TJCE;
1.9.23.2.5 Sempre que for solicitado pelo TJCE com base em mudanças estruturais/organizacionais/lógicas/físicas de seu ambiente computacional, que determinem alterações necessárias no PRDAC-TJCE para manter válido todos os planos e ações inerentes à continuidade de negócios do Tribunal providas pela TI.

1.9.24 ATIVIDADES DE APOIO:

1.9.24.1 PLANO DE TRABALHO com o detalhamento do escopo da elaboração e cronograma de execução, de maneira a possibilitar que o TJCE verifique o integral cumprimento do item "PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE", bem como deste Termo de Referência;
1.9.24.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;
1.9.24.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

1.9.25 PRAZO DE ENTREGA:

1.9.25.1 Na 1ª execução: o serviço deverá ser executado em até 90 (noventa) dias corridos contados a partir da emissão de Ordem de Serviço – OS;
1.9.25.2 Nas demais execuções na vigência do contrato: o serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

1.10 DESCRIÇÃO DETALHADA PARA ELABORAÇÃO DO PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO

1.10.1 Desenvolvimento de um plano estratégico de segurança da informação para a organização, alinhado com o Plano Estratégico Institucional (PEI) e o Plano Estratégico de Tecnologia da Informação (PETI) do Tribunal, com intuito de direcionar seus esforços de manutenção, inovação e melhoria da Segurança da Informação dentro de uma visão de gestão institucional, informacional e de riscos com a diminuição dos impactos decorrentes de falhas de segurança da informação.
1.10.2 Descrição detalhada das ações de segurança a serem implementadas, contendo seus objetivos, descrições, detalhamento de recursos mínimos necessários, prazo de execução e pré-requisitos obrigatórios;
1.10.3 Cronograma de Trabalho, com a representação gráfica das ações de segurança descritas no plano, distribuídas no tempo, contendo as datas de início e fim recomendadas para as atividades, sua duração e os recursos mínimos necessários para a sua execução.
1.10.4 O PDSI deverá ter o seguinte escopo:
1.10.4.1 Deverá abranger todas as possíveis e necessárias ações de segurança a serem executadas durante o prazo de 04 (quatro) anos;
1.10.4.2 Deverá possuir, não se restringindo aos mesmos, os controles constantes das normas ABNT NBR ISO/IEC 27002:2005 e ABNT NBR ISO/IEC 27001:2006 aplicáveis à realidade do TJCE, em conformidade com a fase de análise de riscos e testes de invasão;
1.10.4.3 Deverá observar, dentro da devida pertinência, o resultado dos levantamentos/testes/análises realizados.
1.10.5 Identificação das necessidades de segurança de novos serviços de proteção, de novos ativos e controles que precisarão ser implementados para elevar o grau de serviço prestado pelo TJCE, com base na análise de riscos e teste de invasão realizadas;
1.10.6 Emissão de relatório técnico com as necessidades que a arquitetura de segurança de TI do TJCE precisará satisfazer contemplando:
1.10.6.1 A confrontação das necessidades com as melhores práticas adotadas pelo mercado;
1.10.6.2 Os objetivos gerais a serem atendidos;
1.10.6.3 A lista de serviços a serem implementados;
1.10.6.4 Relação de ativos de segurança que necessitam ser implementados e ou aperfeiçoados;
1.10.7 Definição das arquiteturas de referência rede / serviços de TI capazes de satisfazer no curto, médio e longo prazo as necessidades identificadas, alinhadas com as tendências tecnológicas globais e em aderência às estratégias do Tribunal para Segurança da Informação;

1.10.8 PRODUTOS ESPERADOS:

1.10.8.1 Na 1ª execução:
1.10.8.1.1 Relatório técnico com as necessidades que a nova arquitetura de Segurança de TI do TJCE precisará satisfazer contemplando:

1.10.8.1.2 A confrontação das necessidades com as melhores práticas adotadas pelo mercado;
1.10.8.1.3 O estabelecimento dos objetivos gerais a serem atendidos pela nova arquitetura de tecnologia da informação do TJCE;
1.10.8.1.4 A lista de serviços de informação a serem prestados por esta nova arquitetura;
1.10.8.1.5 A relação de ativos de segurança que necessitam ser implementados e ou aperfeiçoados.
1.10.8.1.6 Documento com objetivos de evolução da rede corporativa do TJCE, delineando a topologia e arquitetura da rede, os aspectos relacionados com backbone principal, comunicação com organizações externas e as disciplinas de gerência necessárias à gestão desta estrutura;
1.10.8.1.7 Documento com ajustes necessários no núcleo básico da arquitetura de segurança do ambiente de informática decorrente da nova arquitetura de referência, com descrição das estratégias de contingência e recuperação (plano de contingência e recuperação de desastres);
1.10.8.1.8 Relatório do Plano Diretor de Segurança da Informação;
1.10.8.1.9 Cronograma de Trabalho anexo ao relatório, representando graficamente as ações de segurança descritas no Plano Diretor de Segurança da Informação e sua distribuição temporal.
1.10.8.2 Nas demais execuções durante a vigência do contrato, a empresa contratada deverá revisar o PDSI incluídos todos os documentos e cronogramas que fazem parte deste programa, nas seguintes hipóteses:
1.10.8.2.1 Mudança em normativo legal relativo à continuidade de negócios no que tange a TI;
1.10.8.2.2 Mudança em normativos internacionais afetos à continuidade de negócios no que tange a TI;
1.10.8.2.3 Mudança e acréscimos de normativos ABNT inerentes ao PDSI;
1.10.8.2.4 Criação de novos normativos nacionais e/ou internacionais que venham a agregar dados e informações que possibilitem a melhora do PDSI;
1.10.8.2.5 Mudanças no PDTI e no PEI que afetem a Segurança da Informação;
1.10.8.2.6 Sempre que for solicitado pelo TJCE com base em mudanças estruturais/organizacionais/lógicas/físicas de seu ambiente computacional, que determinem alterações necessárias no PDSI para manter válido todos os planos e ações inerentes à continuidade de negócios do Tribunal providas pela TI.

1.10.9 ATIVIDADES DE APOIO:

1.10.9.1 PLANO DE TRABALHO com o detalhamento do escopo do planejamento e cronograma de execução;
1.10.9.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;
1.10.9.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

1.10.10 PRAZO DE ENTREGA:

1.10.10.1 O serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;
1.10.10.2 Nas demais execuções na vigência do contrato: o serviço deverá ser executado em até 45 (quarenta e cinco) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

1.11 DESCRIÇÃO DETALHADA PARA DIVULGAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

1.11.1 Esta etapa tem como objetivo a divulgação por meio de palestras, treinamento e cursos para os servidores e prestadores de serviço do TJCE, em todos os níveis hierárquicos, dos conceitos de Segurança da Informação e das Políticas de Segurança elaboradas para o TJCE.
1.11.2 A capacitação realizada pela CONTRATADA enfocará públicos diferentes, levando-se em consideração os 04 (quatro) seguintes tipos de usuários do TJCE: COLABORADORES (servidores e prestadores de serviço em geral), CORPO TÉCNICO DE TI, COMITÊ DE SEGURANÇA DA INFORMAÇÃO E ALTA ADMINISTRAÇÃO. As informações ofertadas a cada público, por ocasião das atividades de treinamentos/palestras/workshops, deverá passar por PRÉVIA AVALIAÇÃO DO TJCE e enfocar linguagem pertinente ao público-alvo das atividades.
1.11.3 Deverá ser montado um Plano de Divulgação e Treinamento, conforme os públicos acima indicados, sobre os conceitos gerais de Segurança da Informação e de ações que serão realizadas por esta etapa.
1.11.3.1 A divulgação deverá levar em consideração o emprego de recursos visuais para colocação nas áreas internas do TJCE, como folders, cartazes, papel de parede desktop, material na Intranet;
1.11.3.2 O plano deverá contemplar a montagem da Semana da Segurança da Informação e a estratégia de conteúdo a ser passado para conhecimento dos servidores e prestadores de serviço do TJCE;
1.11.3.3 Também, o plano deverá considerar um Seminário de Segurança da Informação para os Colaboradores do Departamento de Informática, visando capacitar tais colaboradores nas práticas de segurança da informação do TJCE;
1.11.3.4 Deverá ser incluído no plano os demais treinamentos que serão empregados ao Corpo Técnico, ao Comitê de Segurança da Informação e à alta Administração;
1.11.4 Os Instrutores das palestras e dos treinamentos deverão ser profissionais certificados e capacitados OFICIALMENTE por instituições reconhecidas pelo MEC e/ou por instituições reconhecidas pelo mercado

nacional e/ou internacional no quesito Segurança da Informação e com conhecimento dos serviços do TJCE;
1.11.5 A Contratante resguardar-se-á do direito de acompanhar e avaliar a capacitação, com instrumento próprio, e caso a Contratada não atinja os requisitos mínimos da Contratante, a Contratada deverá reestruturar a capacitação para atingir estes objetivos, sem nenhum custo adicional à Contratante;
1.11.6 Deverá ser realizada a Semana da Segurança da Informação com palestras para o público de servidores e prestadores de serviço em geral do TJCE em Auditório:
1.11.6.1 Cada palestra deverá ter duração mínima de 1hr (uma hora), sendo no período da manhã e/ou no período da tarde, visando facilitar a presença de todos;
1.11.6.2 Prever, em seu planejamento, um total de 10 (dez) palestras para o período da Semana da Segurança da Informação;
1.11.6.3 O conteúdo da palestra deverá contemplar no mínimo:

Item	Palestra
1	Política de segurança da informação do TJCE, com base em conhecimento técnico da CONTRATADA bem como em normas de segurança da informação do TJCE JÁ REVISADAS PELA CONTRATADA. Conteúdo programático: Gestão de segurança da Informação; Classificação segura da informação; Áreas de segurança e prevenção de acessos não autorizados; Proteção contra software malicioso; Correio eletrônico do TJCE; Utilização da Internet; Tratamento de incidentes de segurança da informação; Troca de informações e softwares do TJCE entre os agentes internos e externos do Tribunal; Responsabilidades dos usuários; Acesso seguro aos sistemas operacionais.
2	Manuseio seguro de informações, com base em conhecimento técnico da CONTRATADA bem como em conteúdo programático abaixo. Conteúdo programático mínimo: Ameaças; Backup (cópia de segurança); Ciclo de Segurança; Medidas de Segurança; Riscos; Vulnerabilidades; Códigos maliciosos; Requisitos legais; Incidentes de segurança; Ambiente de trabalho; Antivírus; Controle de acesso; Direitos de privacidade; Direitos de propriedade intelectual; Estação de trabalho: Mesa limpa e tela limpa; Senha seguras; Identificação e autenticação; Golpes virtuais e fraude eletrônica; Segurança em computadores pessoais; Uso de crachá; Vídeos de segurança da informação. A empresa contratada poderá inserir, além dos temas acima observados, outros temas pertinentes e atuais à época das palestras para complementar/completar este tópico.

1.11.6.4 As turmas das palestras não deverão ser limitadas na quantidade de ouvintes, respeitando-se apenas a capacidade máxima suportada pelas instalações físicas do local de realização;
1.11.6.5 A Empresa deverá preparar e fornecer a versão eletrônica do material nos formatos *CAD e PDF* para divulgação interna no TJCE, como folders, cartazes, papel de parede desktop, conteúdo de Intranet. Caberá ao TJCE a impressão e distribuição de qualquer material no formato físico.
1.11.6.6 A Empresa deverá preparar e fornecer material didático informativo a ser distribuído aos participantes das palestras;
1.11.6.7 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o desenvolvimento das palestras, assim como também controlar e registrar as presenças.
1.11.6.8 A empresa deverá produzir e fornecer Certificado de participação das palestras para cada um dos participantes da Semana da Segurança da Informação;
1.11.7 Ao Corpo Técnico de TI, colaboradores do Departamento de Informática em geral, deverá ser realizado um Seminário de Segurança da Informação contemplando um conjunto de palestras de conteúdo específico e diferenciado para capacitação desse público:
1.11.7.1 O Seminário deverá ocorrer em, pelo menos, 03 (três) dias com palestras na manhã e/ou à tarde, em Auditório, envolvendo os seguintes tópicos:
1.11.7.1.1 Política de Segurança da Informação e Comunicações (PSIC) do TJCE;
1.11.7.1.2 Gestão de riscos em Segurança da Informação;
1.11.7.1.3 Tratamento e resposta a incidentes de Segurança da Informação;
1.11.7.1.4 Guia de desenvolvimento seguro de aplicações;
1.11.7.1.5 Modelo de gestão de Segurança da Informação;
1.11.7.1.6 Plano de recuperação de desastres em ambiente computacional;
1.11.7.1.7 Plano Diretor de Segurança da Informação;
1.11.7.1.8 Normativos Federais/Estaduais;
1.11.7.1.8.1 Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário;
1.11.7.1.8.2 Decreto no 3.505, de 13 de junho de 2000;
1.11.7.1.9 Normativos ABNT;
1.11.7.1.9.1 ABNT NBR ISO Guia 73:2005; ABNT NBR ISO/IEC 15408, Nível 2 e 3; ABNT NBR ISO/IEC 27005:2008; ABNT NBR ISO/IEC 27001:2006; ABNT NBR ISO/IEC 27002:2005; ABNT NBR 15999:2007, Parte 2: Requisitos - ABNT NBR 15999-2:2008 e ABNT NBR ISO 22301:2013;
1.11.7.1.10 Lei de Acesso à Informação, Lei nº 12.527, de 18 de novembro de 2011;
1.11.7.2 As turmas das palestras deverão ser formatadas para atender a um público de no mínimo 50

(cinquenta) participantes;
1.11.7.3 Nos intervalos entre as palestras deverá ser realizado coffee-break;
1.11.7.4 A Empresa deverá preparar e fornecer material para divulgação interna no TJCE, como folders, cartazes, papel de parede desktop, conteúdo de Intranet;
1.11.7.5 A Empresa deverá preparar e fornecer material didático com conteúdo do Seminário aos participantes;
1.11.7.6 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o desenvolvimento das palestras, assim como também controlar, registrar as presenças e apresentar ao TJCE o resultado do comparecimento dos colaboradores da SETIN para avaliação do Tribunal;
1.11.7.7 A empresa deverá produzir e fornecer Certificado de participação das palestras para cada um dos Técnicos participantes do Seminário;
1.11.7.8 A Empresa deverá produzir e fornecer questionários aos participantes dos eventos com a finalidade de se verificar a didática e qualidade das informações repassadas aos alunos. Estes formulários serão, após devido recolhimento e parametrização pela Contratada, entregues ao TJCE, onde este (TJCE) irá verificar a qualidade do serviço realizado. Caso, comprovadamente (com base nas respostas dos referidos questionários), a empresa não consiga repassar os conhecimentos propostos, esta deverá realizar, por suas custas, novo treinamento. Para aceitação e recebimento do treinamento pelo Tribunal, a Contratada deverá demonstrar índice de satisfação da turma treinada na casa de 70%, obtida por meio do computo total (resultado) das perguntas realizadas;
1.11.8 Ao Corpo Técnico de TI deverão ser realizados treinamentos específicos sobre normativos da ABNT assim como boas práticas em segurança da informação.
1.11.8.1 Os treinamentos estão relacionados na tabela a seguir e o seu conteúdo programático.

Item	Treinamento	Quantidade Técnicos	Carga Horária Mínima
1	Gestão de continuidade de negócios, com base em conhecimento técnico da CONTRATADA bem como nas normas ABNT NBR 15999-1:2007, ABNT NBR 15999-2:2008 e ABNT NBR ISO 22301:2013	10	16
2	Sistemas de gestão de segurança da informação, com base em conhecimento técnico da CONTRATADA bem como nas normas ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005.	10	16
3	Gestão de riscos em TI, com base em conhecimento técnico da CONTRATADA bem como na norma ABNT NBR ISO/IEC 27005:2008 e ABNT NBR ISO/IEC Guia 73:2005	10	16
4	Diretrizes para gestão da segurança da informação, com base em conhecimento técnico da CONTRATADA bem como nas normas ABNT NBR ISO/IEC 27002:2005, ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27011:2009.	10	16

1.11.8.2 Os horários para início e fim dos treinamentos serão conforme disponibilidade do Corpo Técnico do DEINF, em períodos matutinos, vespertinos ou noturnos - 4hrs/dia;
1.11.8.3 Nos intervalos dos cursos deverá ser realizado coffee-break;
1.11.8.4 Empresa deverá preparar e fornecer material didático com conteúdo dos cursos aos participantes;
1.11.8.5 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o desenvolvimento dos cursos, assim como também controlar e registrar as presenças;
1.11.8.6 A Empresa deverá produzir e fornecer questionários aos participantes dos eventos com a finalidade de se verificar a didática e qualidade das informações repassadas aos alunos. Estes formulários serão, após devido recolhimento e parametrização pela Contratada, entregues ao TJCE, onde este verificará a qualidade do serviço realizado. Caso, comprovadamente (com base nas respostas dos referidos questionários), a empresa não consiga repassar os conhecimentos propostos, esta deverá realizar, por suas custas, novo treinamento. Para aceitação e recebimento do treinamento pelo Tribunal, a Contratada deverá demonstrar índice de satisfação da turma treinada na casa de 70%, obtida por meio do computo total (resultado) das perguntas realizadas;
1.11.8.7 A Empresa deverá produzir e fornecer Certificado de participação dos cursos para cada um dos Técnicos participantes.
1.11.9 Para os integrantes do Comitê de Segurança da Informação do TJCE, deverão ser realizados treinamentos específicos sobre normativos da ABNT assim como de práticas de segurança da informação.
1.11.9.1 Os treinamentos estão relacionados na tabela a seguir e o conteúdo programático está descrito abaixo.

Item	Treinamento	Carga Horária Máxima
1	Sistemas de gestão de segurança da informação, com base em conhecimento técnico da CONTRATADA bem como nas normas ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005.	08

1.11.9.2 Os horários para início e fim dos treinamentos serão conforme disponibilidade dos responsáveis do TJCE, em períodos matutinos, vespertinos ou noturnos – 4hrs/dia;
1.11.9.3 Nos intervalos dos cursos deverá ser realizado coffee-break;
1.11.9.4 A Empresa deverá preparar e fornecer material didático com conteúdo dos cursos aos participantes;
1.11.9.5 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o desenvolvimento dos cursos, assim como também controlar e registrar as presenças;
1.11.9.6 A Empresa deverá produzir e fornecer questionários aos participantes do evento com a finalidade de se verificar a didática e qualidade das informações repassadas aos alunos. Estes formulários serão, após devido recolhimento e parametrização pela Contratada, entregues ao TJCE, onde este verificará a qualidade do serviço realizado. Caso, comprovadamente (com base nas respostas dos referidos questionários), a empresa não consiga repassar os conhecimentos propostos, esta deverá realizar, por suas custas, novo treinamento. Para aceitação e recebimento do treinamento pelo Tribunal, a Contratada deverá demonstrar índice de satisfação da turma treinada na casa de 70%, obtida por meio do computo total (resultado) das perguntas realizadas;
1.11.9.7 A Empresa deverá produzir e fornecer Certificado de participação dos cursos para cada um dos Técnicos participantes.
1.11.10 Para a alta Administração e demais Autoridades indicadas, deverá ser realizado Workshop sobre Política de Segurança desenvolvida para o Tribunal assim como de boas práticas de segurança da informação.

Item	Treinamento	Carga Horária Máxima
1	Workshop sobre Política de Segurança desenvolvida para o Tribunal assim como de boas práticas de segurança da informação.	04

1.11.10.1 Os horários para início e fim do Workshop será conforme disponibilidade dos responsáveis do TJCE, em períodos matutinos, vespertinos ou noturnos, em períodos de expediente alternados ou contínuos;
1.11.10.2 O Instrutor do Workshop deverá ser profissional capacitado OFICIALMENTE por instituições reconhecidas pelo MEC e/ou por instituições reconhecidas pelo mercado nacional e/ou internacional no quesito Segurança da Informação e com a seguinte qualificação:
1.11.10.2.1 Prova do Registro na Ordem dos Advogados do Brasil – OAB;
1.11.10.2.2 Experiência acadêmica na área de Direito Eletrônico comprovada através de Certificados fornecidos pela instituição de ensino promotora do curso no qual foram ministradas as aulas;
1.11.10.2.3 Deverá possuir publicações na área de direito eletrônico. A comprovação de publicações deverá ser efetuada mediante a apresentação de exemplar integral (original ou cópia de boa qualidade) em que conste claramente o nome do profissional e o ISBN. Não serão aceitas publicações em mídia eletrônica;
1.11.10.2.4 Apresentação de atestado de capacidade técnica, fornecida por Pessoa Jurídica de Direito público, em nome do profissional, comprovando que prestou serviço de característica técnicas semelhantes ao objeto licitado fazendo uso de cópia de propriedade da proponente da norma ABNT NBR ISO IEC 17799:2005;
1.11.10.3 A Empresa deverá preparar e fornecer material didático com conteúdo dos cursos aos participantes;
1.11.10.4 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o desenvolvimento dos cursos, assim como também controlar e registrar as presenças;
1.11.10.5 Empresa deverá produzir e fornecer questionários aos participantes do evento com a finalidade de se verificar a didática e qualidade das informações repassadas aos alunos. Estes formulários serão, após devido recolhimento e parametrização pela Contratada, entregues ao TJCE, onde este verificará a qualidade do serviço realizado. Caso, comprovadamente (com base nas respostas dos referidos questionários), a empresa não consiga repassar os conhecimentos propostos, esta deverá realizar, por suas custas, novo treinamento. Para aceitação e recebimento do treinamento pelo Tribunal, a Contratada deverá demonstrar índice de satisfação da turma treinada na casa de 70%, obtida por meio do computo total (resultado) das perguntas realizadas;
1.11.10.6 A Empresa deverá produzir e fornecer Certificado de participação dos cursos para cada um dos Responsáveis do TJCE participantes.
1.11.11 Descrição do conteúdo programático dos treinamentos técnicos:
1.11.11.1 Gestão de continuidade de negócios:
1.11.11.1.1 Interpretação da Norma ABNT 15999:2007, Parte 2: Requisitos - ABNT NBR 15999-2:2008 e ABNT NBR ISO 22301:2013, contemplando no mínimo: visão geral da gestão de continuidade de negócios (GCN); A política de gestão de continuidade de negócios; Gestão do programa de GCN; Entendendo a organização; Determinando a estratégia de continuidade de negócios; Desenvolvendo e implementando uma resposta de GCN; Testando, mantendo e analisando criticamente os preparativos de GCN; Incluindo a GCN na cultura da organização; Planejamento do SGCN; Implementação e operação do SGCN; Monitoração e análise crítica do SGCN;- Manutenção e melhoria do SGCN;
1.11.11.2 Sistemas de gestão de segurança da informação:

1.11.11.2.1 Interpretação da Norma ABNT NBR ISO/IEC 27001:2006, contemplando no mínimo: Visão Geral das normas NBR ISO/IEC 27001 e NBR ISO/IEC 17799; Conceitos: informação, segurança da informação, ativos, confidencialidade, integridade, disponibilidade, vulnerabilidades, ameaças, impactos, probabilidade; Conceitos: riscos de segurança, processos de avaliação e tratamento do risco, sistema de gestão, sistema de gestão de segurança da informação; Interpretação das cláusulas: 0, 1, 2, 3 da NBR ISO/IEC 27001:2006; Interpretação das cláusulas: 4 /4.1, 4.2/ 4.2.1, 4.2.2, da NBR ISO/IEC 27001:2006; Interpretação das cláusulas: 4.2.3, 4.2.4, 4.3/ 4.3.1, 4.3.2, 4.3.3 da NBR ISO/IEC 27001:2006; Interpretação das cláusulas: 5, 6, 7 e 8 da NBR ISO/IEC 27001:2006; Visão Geral do Anexo A - objetivos de controle; Anexo A - Controles detalhados do A5 ao A9; Anexo A - Controles detalhados do A10 ao A12;
1.11.11.2.2 Interpretação da Norma ABNT NBR ISO/IEC 27002:2005, contemplando no mínimo: Visão geral das normas NBR ISO/IEC 27002 e NBR ISO/IEC 27001, apresentação do processo de exame do EXIN; Informação, objetivos do negócio e requisitos de qualidade - Formas, sistemas, valor da informação, disponibilidade, integridade e confidencialidade, análise da informação, gestão da informação; Conceitos de riscos e ameaças para segurança da informação - Tipos de ameaças, danos e riscos, medidas para redução de risco, guia para implementação de medidas de segurança; Ativos da informação e incidentes de segurança - O que são estes ativos e como gerenciá-los, sua classificação, papéis; Medidas físicas - Segurança física, anéis de proteção, alarmes, proteção contra incêndio; Medidas técnicas - Gerenciamento do acesso lógico, requisitos de segurança para sistemas de informação, criptografia, segurança de arquivos do sistema, vazamento de informação; Medidas organizacionais - Política de segurança, pessoal, gestão de continuidade do negócio, gestão das comunicações e processos de operação; Legislação e regulamentações - Observação de regulamentações, adequação, propriedade intelectual, proteção de documentos do negócio, de dados e confidencialidade de dados pessoais, prevenção contra abuso das instalações, cumprimento de política e padrões de segurança, medidas de monitoramento, auditorias, proteção de deficiências;
1.11.11.3 Gestão de riscos de segurança da informação:
1.11.11.3.1 Interpretação da Norma ABNT NBR ISO/IEC 27005:2008, contemplando no mínimo: Visão geral do processo de Gestão de Riscos de Segurança da Informação; Termos e definições; Conceitos relacionados com Gestão de Riscos de Segurança da Informação; Apresentação da organização da Norma; Análise/Avaliação de riscos de segurança da informação; Tratamento do risco de segurança da informação; Comunicação do risco de segurança da informação; Monitoramento e análise crítica de riscos de segurança da informação; Ferramentas para Gestão de Riscos;
1.11.11.4 Diretrizes para gestão da segurança da informação para organizações de telecomunicações:
1.11.11.4.1 Interpretação da Norma ABNT NBR 27011:2009, contemplando no mínimo: Termos e Definições Relacionados com Segurança da Informação; Segurança de Telecomunicações e Legislação Especifica; Política de Segurança da Informação; Organizando a Segurança da Informação; Gestão de Ativos; Segurança em Recursos Humanos; Segurança Física e do Ambiente; Gerenciamento das Operações e Comunicações; Controle de Acesso; Aquisição, Desenvolvimento, e Manutenção de Sistemas de Informação; Gestão de Incidentes de Segurança da Informação; Gestão de Continuidade de Negócios; Conformidade; Conjunto de Controles Extendidos para Telecomunicações; Diretrizes Adicionais de Implementação;
1.11.12 A reprodução de todo o material de divulgação e de todo o material didático necessário à execução dos cursos e das palestras será de responsabilidade da Contratada;
1.11.13 As dependências físicas (Auditório, Salas) realização para os cursos e palestras serão de responsabilidade do TJCE.
1.11.14 Os cursos e palestras deverão ser teóricos, sem a necessidade de utilização de equipamentos de informática pelos Participantes.

1.11.15 PRODUTOS ESPERADOS:

1.11.16 Plano de Divulgação e Treinamento;
1.11.17 As palestras da Semana da Segurança da Informação para os servidores e prestadores de serviço em geral do TJCE, acompanhado de todo o material de divulgação e didático;
1.11.18 As palestras do Seminário de Segurança da Informação para o Corpo Técnico de TI da SETIN, acompanhado de todo o material de divulgação, didático e certificados;
1.11.19 Os treinamentos do Corpo Técnico de TI, acompanhado de todo o material de divulgação, didático e certificados;
1.11.20 Os treinamentos para os integrantes do Comitê de Segurança da Informação do TJCE, acompanhado de todo o material de divulgação, didático e certificados;
1.11.21 O Workshop da alta Administração do TJCE e demais Autoridades indicadas, acompanhado de todo o material de divulgação, didático e certificados;

1.11.22 ATIVIDADES DE APOIO:

1.11.22.1 PLANO DE TRABALHO com o detalhamento do escopo da divulgação e cronograma de execução;
1.11.22.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;
1.11.22.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do

TJCE;

1.11.23 PRAZO DE ENTREGA:

1.11.23.1 O serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS para o "Plano de Divulgação e Treinamento";
1.11.23.2 O prazo de entrega de cada capacitação e ou treinamento será definido na Ordem de Serviço – OS competente de acordo com disponibilidade das Equipes do TJCE;

2. DA PRESTAÇÃO DOS SERVIÇOS

2.1 Do Local

2.1.1 TJCE: na Av. General Afonso Albuquerque Lima, S/N. - Cambeba CEP: 60822-325, Fortaleza-CE, na Secretaria de Tecnológica da Informação – SETIN

2.2 Dos Prazos

2.2.1 O fornecimento deverá ser executado a partir de notificação para fornecimento a ser emitida pelo TJCE posterior à assinatura do contrato;
2.2.2 Em até 15 (quinze) dias corridos a partir da data de emissão da notificação para fornecimento pelo TJCE, a empresa Contratada deverá efetuar inicialização de projeto;
2.2.3 Efetuada a inicialização do projeto, com o competente aceite de abertura do projeto, todos os serviços contemplados pelo Objeto deverão estar disponíveis para demanda do TJCE via emissão de Ordem de Serviços – OS;
2.2.4 O prazo para execução de cada serviço contemplado no Objeto é de acordo com a definição de "prazo de entrega" de cada subitem de serviço constante da "Descrição detalhada dos serviços";

2.3 Forma de Fornecimento

2.3.1 Todo o fornecimento deverá estar de acordo com os critérios estabelecidos nos itens deste Termo de Referência;
2.3.2 A Contratada deverá implementar rigorosa gerência de projeto, com observância às regras a seguir além de adotar a Metodologia de Gerenciamento de Projetos – MGP da SETIN;
2.3.3 Para a inicialização do projeto, a empresa Contratada deverá executar:
2.3.3.1 Atividades que serão realizadas nesta fase:
2.3.3.2 Abertura do projeto: deverá ser elaborado e apresentado Termo de Abertura do Projeto;
2.3.3.3 Apresentação do escopo do serviço: deverá ser elaborado e apresentado Declaração de Escopo do Projeto;
2.3.3.4 Pré-planejamento do projeto: deverá ser elaborado e apresentado Plano de Gerenciamento do Projeto;
2.3.3.5 A Contratada deverá apresentar Cronograma de Execução, constando atividades, subatividades e marcos, contemplando todas as ações previstas para a execução dos serviços, datas de entrega de documentação, datas das reuniões de ponto de controle, dentre qualquer outro evento que se julgar relevante e necessário;
2.3.3.6 Em até 07 (sete) dias consecutivos após emissão da ordem de fornecimento, a Contratada deverá agendar reunião ("kick-off meeting") junto aos responsáveis técnicos da Contratante, objetivando dar início ao acompanhamento da execução do Contrato;
2.3.3.7 Na reunião de "kick-off", a Contratada deverá apresentar sua equipe de trabalho, composta, no mínimo, por 01 (um) Gerente de Projeto e Equipe de Técnicos Especialistas;
2.3.3.8 Para apoio ao Gerente de Projeto, deverão ser alocados todos os técnicos necessários para a execução dos serviços;
2.3.3.9 Caberá ao Gerente de Projeto coordenar e orientar todo o processo de planejamento e execução dos serviços do Contrato, respeitando os prazos estabelecidos, atestando a qualidade dos produtos entregues e serviços executados;
2.3.3.10 Deverá ser elaborada e apresentada Lista de Contatos do Projeto;
2.3.3.11 Definição das regras para execução do serviço;
2.3.3.12 Definição das responsabilidades de cada um dos envolvidos;
2.3.4 A contar da 1ª reunião do projeto, deverão ser executadas reuniões periódicas de controle do projeto ("Status do Projeto") entre as equipes técnicas envolvidas, onde o Gerente de Projeto posicionará os responsáveis do Contratante sobre o andamento do projeto e apresentando os documentos pertinentes;
2.3.5 As reuniões de status poderão ser realizadas semanalmente, quinzenalmente ou conforme a demanda, a critério da Contratante;
2.3.6 O Gerente será responsável pela elaboração e entrega de relatórios de progresso e ou situação do projeto ("Relatório de Acompanhamento"), onde deverão ser descritas as atividades pertinentes ao período, além de destacar as pendências e solicitações de mudança do projeto, dentre outros tópicos;
2.3.7 Os relatórios de progresso e ou situação do projeto deverão ser fornecidos por período, semanalmente, quinzenalmente ou conforme a demanda, a critério da Contratante;

2.3.8 Todas as reuniões do projeto deverão ser registradas em “Ata”, a qual será de inteira responsabilidade do Gerente;
2.3.9 As atas deverão ser entregues em no máximo 48 (quarenta e oito) horas após a realização da reunião para verificação e revisão por parte do TJCE, para posterior emissão de aceite por ambas as partes;
2.3.10 Após a apresentação e aprovação dos documentos relacionados ao plano de projeto, a equipe do projeto dará início às demais Fases do cronograma;
2.3.11 Produtos da fase para entrega ao TJCE:
2.3.11.1 Documentação inicial do projeto, incluindo termo de abertura, declaração de escopo, plano de gerenciamento, cronograma de trabalho, matriz de responsabilidade e lista de contatos dos participantes;
2.3.11.2 Documentos de acompanhamento do projeto, incluindo relatórios de situação e atas de reunião;
2.3.11.3 Termo de Aceitação;
2.3.12 O TJCE oficializará a demanda dos serviços por meio da emissão de uma “Ordem de Serviço – OS”, conforme:
2.3.12.1 A execução será sempre precedida da emissão pelo TJCE da competente “Ordem de Serviço – OS”, contendo no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço e produtos esperados;
2.3.13 A “Ordem de Serviço – OS” será emitida, assinada e autorizada pelo Fiscal do Contrato;
2.3.14 Toda “Ordem de Serviço – OS” deverá ser assinada pelo Gerente do Projeto / Preposto, representante da Contratada perante o TJCE, declarando a concordância da Contratada em executar as atividades descritas na “Ordem de Serviço – OS”, de acordo com as especificações estabelecidas pelo TJCE;
2.3.15 Os serviços deverão estar sempre de acordo com as especificações constantes nas “Ordens de Serviços – OS”;
2.3.16 O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução – quando a “Ordem de Serviço – OS” é emitida pelo TJCE, durante a execução – com o acompanhamento e supervisão de responsáveis do TJCE, e ao término da execução – com o fornecimento de “Relatório de Serviços” pela Contratada e atesto dos mesmos por responsáveis do TJCE;
2.3.17 Todos os serviços prestados pela Contratada deverão ser necessariamente documentados (passo-a-passo), registrados e entregues ao TJCE pela mesma, em cópias impressas e gravadas em meio magnético, complementarmente ao “Relatório de Serviços”;
2.3.18 A partir da emissão da “Ordem de Serviço – OS”, a Contratada terá até 07 (sete) dias corridos para iniciar a sua execução, ressalvados os casos em que comprovadamente seja necessário um agendamento dos trabalhos;

2.4 Do Recebimento

2.4.1 O objeto será dado como recebido de acordo com os artigos 73 a 76 da Lei 8.666/93, conforme abaixo informado:
2.4.1.1 Provisoriamente, em até 5 (cinco) dias, a partir da entrega do serviço ou fornecimento do produto, para efeito de posterior verificação de sua conformidade;
2.4.1.2 Definitivamente, em até 10 (dez) dias úteis, a partir do recebimento provisório e após minuciosa verificação e avaliação dos serviços executados;
2.4.2 Para aceite do recebimento e posterior encaminhamento ao pagamento, deverão ser apresentados os seguintes documentos:
2.4.2.1 Ordem de Serviços emitida e assinada, Relatório de Serviços e demais Documentos Técnicos pertinentes e comprobatórios de execução do serviço;
2.4.3 Independentemente da aceitação no recebimento, a Contratada deverá garantir a qualidade do serviço executado pelo prazo estabelecido nas especificações e nas condições constantes deste Termo de Referência, obrigando-se a corrigir aquele que apresentar inconsistência no prazo estabelecido pelo TJCE.
2.4.4 O pagamento será efetuado com apresentação da(s) respectiva(s) Nota(s) Fiscal(is) / Fatura(s), uma vez que tenham sido cumpridos, no que couber, todos os critérios estabelecidos neste Termo de Referência, acompanhado dos documentos de aceite de cada tipo de serviço e conforme eventos a seguir relacionados:
2.4.4.1 Dos serviços: na conclusão ou encerramento de cada ciclo de atendimento ou da OS;
2.4.5 Os Fiscais do Contrato verificarão a conformidade dos serviços e/ou da entrega e da documentação requerida e, no caso de estarem conformes, atestará a Nota Fiscal e encaminhará para pagamento. No caso de não estarem conformes, as devolverá, com as ressalvas devidas, no prazo de até 10 (dez) dias da apresentação, para a Contratada providenciar a sua conformidade e novo encaminhamento para o TJCE.
2.4.6 No caso dos serviços e/ou entregas em não conformidade, a contagem dos prazos aqui estabelecidos será reiniciada a contar da data do saneamento das ressalvas pela Contratada, devidamente certificadas pelo Fiscal do Contrato.
2.4.7 O TJCE rejeitará, no todo ou em parte, os serviços e fornecimentos executados em desacordo com o disposto neste Termo de Referência. Se, após o recebimento provisório, constatar-se que os serviços e fornecimentos foram executados em desacordo com o especificado, com defeito ou incompleto, os responsáveis do TJCE notificarão, por escrito, à Contratada, interrompendo-se os prazos de recebimento e ficando suspenso o pagamento até que seja sanada a situação.

2.4.8 Em caso de produto entregue em desconformidade com o especificado, será determinado um prazo, pelo TJCE, para que a Contratada faça a correção, sendo emitido pelo TJCE "Termo de Recusa do Serviço". Este prazo iniciar-se-á a partir da data da emissão do mencionado termo de recusa. A Contratada ficará obrigada a substituir, às suas expensas, o item do objeto que for recusado.
2.4.9 Os valores da(s) NF(s) / Fatura(s) deverão ser os mesmos consignados na Nota de Empenho, sem o que não será liberado o respectivo pagamento. Em caso de divergência, será estabelecido prazo para a Contratada fazer a substituição desta(s) NF(s) / Fatura(s).
2.4.10 São critérios de mensuração dos serviços prestados para controle dos fornecimentos e dos pagamentos:

Item	Métrica	Indicador	Valor
Serviços técnicos	Unidade	Serviço Especificado na OS	100% executado
Transferência de conhecimento	Participantes	Conhecimento atualizado	100% prestado

3. ELEMENTOS PARA GESTÃO DO CONTRATO

3.1 Papeis e Responsabilidade

ID	Papel	Entidade	Responsabilidade
1	Fiscal Técnico	SETIN – Diretor(a) da Divisão de Segurança da Informação	Confecção e assinatura do Termo de Recebimento Provisório, quando da entrega do objeto resultante de cada Ordem de Serviço ou de Fornecimento de Bens; Avaliação da qualidade dos serviços realizados ou dos bens entregues e justificativas, de acordo com os Critérios de Aceitação definidos em contrato; Identificação de não conformidade com os termos contratuais; Verificação da manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica. Verificação de manutenção das condições elencadas no Plano de Sustentação (Documento elaborado no planejamento da contratação, que visa garantir a continuidade do negócio durante e após a entrega da Solução de Tecnologia da Informação, bem como após o encerramento do contrato); Comunicar por escrito ao gestor do contrato qualquer falta cometida pela empresa contratada, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão levar a aplicação de sanção ou à rescisão contratual; Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato; Realizar pessoalmente a medição dos serviços contratados; Recusar serviço ou fornecimento irregular ou em desacordo com condições previstas em edital, na proposta da contratada e no contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados; Averiguar se é o contratado quem executa o contrato e certificar-se de que não existe cessão ou subcontratação fora das hipóteses legais; Verificar o cumprimento das normas trabalhistas por parte do contratado, a exemplo da jornada de trabalho, limitações de horas extras, descanso semanal, bem como da obediência às normas de segurança do trabalho, a fim de evitar acidentes com agentes administrativos, terceiros e empregados do contrato; Atestar a efetiva realização do objeto contratado para fins de pagamento das faturas correspondentes; Acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle da qualidade dos materiais, serviços e equipamentos a serem aplicados nos serviços.
2	Fiscal Requisitante do Contrato	SETIN – Chefia do Suporte Técnico	Avaliação da qualidade dos serviços realizados ou dos bens entregues e justificativas, de acordo com os Critérios de Aceitação definidos em contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Identificação de não conformidade com os termos contratuais, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato;

			Verificação da manutenção da necessidade, economicidade e oportunidade da contratação; Verificação de manutenção das condições elencadas no Plano de Sustentação (Documento elaborado no planejamento da contratação, que visa garantir a continuidade do negócio durante e após a entrega da Solução de Tecnologia da Informação, bem como após o encerramento do contrato), em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle da qualidade dos materiais, serviços e equipamentos a serem aplicados nos serviços, em conjunto com o Fiscal Técnico; Verificar o cumprimento das normas trabalhistas por parte do contratado, a exemplo da jornada de trabalho, limitações de horas extras, descanso semanal, bem como da obediência às normas de segurança do trabalho, a fim de evitar acidentes com agentes administrativos, terceiros e empregados do contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Comunicar por escrito ao gestor do contrato qualquer falta cometida pela empresa contratada, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão levar a aplicação de sanção ou à rescisão contratual, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato.
3	Fiscal Administrativo	SETIN – Diretor(a) da Divisão de Apoio da Secretaria de Tecnologia da Informação	Certificar-se do correto cálculo e recolhimento das obrigações trabalhistas, previdenciárias, e tributárias decorrentes do contrato; Proceder à obrigatória liquidação da despesa, mediante fatura de serviço devidamente atestada pelo fiscal técnico, para fins de apuração da origem e do objeto do que se deve pagar, da importância exata a ser paga e a quem se deve pagar para extinguir a obrigação, com base no contrato, na nota de empenho e nos comprovantes de entrega do material ou da efetiva prestação do serviço, em conformidade com o disposto nos arts. 62 e 63 da Lei nº 4.320, de 18 de março de 1964; Efetuar o controle da vigência, realizando comunicado ao fiscal técnico em tempo hábil, uma vez que este deverá controlar os prazos de execução, necessidades de prorrogações ou nova contratação, ficando o fiscal administrativo o controle da época de reajustamento dos preços contratados, tomando as providências cabíveis em tempo hábil junto à Divisão Central de Contratos e Convênios do TJCE, quando necessário; Verificar se a empresa contratada cumpriu com a garantia prevista no contrato.
4	Gestor do Contrato	SETIN – Secretário(a) de Tecnologia da Informação	Manter registro próprio, atualizado, das ocorrências relacionadas à execução do contrato; Acompanhar o cumprimento do cronograma de execução e dos prazos previstos; Determinar à contratada a regularização das falhas ou defeitos observados, assinalando prazo para correção; Relatar, por escrito, ao titular do órgão responsável, a inobservância de cláusulas contratuais ou quaisquer ocorrências que possam trazer dificuldades, atrasos, defeitos e prejuízos à execução da avença, em especial os que ensejarem a aplicação de penalidades; Comunicar ao titular do órgão responsável, apresentando as devidas justificativas, a eventual necessidade de acréscimos ou supressões de serviços, materiais ou equipamentos, identificadas no curso das atividades de fiscalização; Solicitar à contratada a substituição de empregado ou preposto da contratada e aprovar, previamente, mediante termo juntado ao processo, a substituição de iniciativa da contratada, quando assim exigir o contrato; Receber, definitivamente, por meio de ateste na nota fiscal/fatura ou

			documento equivalente, devidamente discriminado, obras, serviços e materiais; Acompanhar o prazo de vigência do contrato e manifestar-se, quando provocado pela Administração, sobre os aspectos de oportunidade, conveniência, razoabilidade e economicidade administrativa de realizar-se alteração, prorrogação ou rescisão do contrato, anexando, quando for o caso, documentação comprobatória;

4. DEVERES E RESPONSABILIDADES DA CONTRATANTE

4.1 Proporcionar todas as facilidades para a Contratada executar o fornecimento do objeto do presente Termo de Referência, permitindo o acesso dos profissionais da Contratada às suas dependências. Esses profissionais ficarão sujeitos a todas as normas internas do TJCE, principalmente as de segurança, inclusive àquelas referentes à identificação, trajes, trânsito e permanência em suas dependências;
4.2 Promover o acompanhamento e a fiscalização da execução do objeto do presente Termo de Referência, sob o aspecto quantitativo e qualitativo, anotando em registro próprio as falhas detectadas;
4.3 Comunicar prontamente à Contratada qualquer anormalidade na execução do objeto, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no presente Termo de Referência;
4.4 Fornecer à Contratada todo tipo de informação interna essencial à realização dos fornecimentos e dos serviços;
4.5 Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando esta estiver em conformidade com os padrões de informação e qualidade exigidos;
4.6 Homologar os serviços prestados, quando estes estiverem de acordo com o especificado no Termo de Referência;
4.7 Efetuar o pagamento à Contratada;

5. DEVERES E RESPONSABILIDADES DA CONTRATADA

5.1 Atender a todas as condições descritas no presente Termo de Referência e respectivo Contrato;
5.2 Manter as condições de habilitação e qualificação exigidas durante toda a vigência do Contrato;
5.3 Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, contribuições previdenciárias, impostos e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que estes não têm nenhum vínculo empregatício com o TJCE;
5.4 Responsabilizar-se pelo fornecimento do objeto deste Termo de Referência, respondendo civil e criminalmente por todos os danos, perdas e prejuízos que, por dolo ou culpa sua, de seus empregados, prepostos, ou terceiros no exercício de suas atividades, vier a, direta ou indiretamente, causar ou provocar à TJCE;
5.5 Obter todas as autorizações, aprovações e franquias necessárias à execução dos fornecimentos e dos serviços, pagando os emolumentos prescritos por lei e observando as leis, regulamentos e posturas aplicáveis. É obrigatório o cumprimento de quaisquer formalidades e o pagamento, à sua custa, das multas porventura impostas pelas autoridades, mesmo daquelas que, por força dos dispositivos legais, sejam atribuídas à Administração Pública;
5.6 Não ceder ou transferir, total ou parcialmente, parte alguma do contrato. A fusão, cisão ou incorporação só será admitida com o consentimento prévio e por escrito do TJCE;
5.7 Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades objeto do Contrato, sem prévia autorização do TJCE;
5.8 Dar ciência, imediatamente e por escrito, de qualquer anormalidade que verificar na execução do objeto bem como prestar esclarecimentos que forem solicitados pelo TJCE;
5.9 Manter sigilo absoluto sobre informações, dados e documentos provenientes da execução do Contrato e também às demais informações internas do TJCE a que a Contratada tiver conhecimento;
5.10 Não deixar de executar qualquer atividade necessária ao perfeito fornecimento do objeto, sob qualquer alegação, mesmo sob pretexto de não ter sido executada anteriormente qualquer tipo de procedimento;
5.11 Somente desativar hardware, software e qualquer outro recurso computacional relacionado à execução do objeto mediante prévia autorização do TJCE;
5.12 Prestar qualquer tipo de informação solicitada pelo TJCE sobre os fornecimentos e sobre os serviços contratados bem como fornecer qualquer documentação julgada necessária ao perfeito entendimento do objeto deste Termo de Referência;
5.13 Elaborar e apresentar documentação técnica dos fornecimentos e serviços executados nas datas aprazadas, visando sua homologação pelo TJCE;
5.14 Alocar profissionais devidamente capacitados e habilitados para os serviços contratados;
5.15 Providenciar a substituição imediata dos profissionais alocados ao serviço que, eventualmente, não

atendam aos requisitos deste Termo de Referência ou por solicitação do TJCE devidamente justificada;
5.16 Implementar rigorosa gerência de contrato com observância a todas as disposições constantes deste Termo de Referência;
5.17 Em até 10 (dez) dias após a assinatura do contrato, a CONTRATADA disporá de profissionais com capacidade técnica suficiente e necessária ao desempenho dos serviços Objeto do Contrato, exigindo-se:
5.17.1 Todos os profissionais deverão possuir experiência mínima comprovada de 03 (três) anos na área de Segurança da Informação e terem participado de projetos similares;
5.17.2 A equipe de profissionais envolvida para exercer as funções, deve possuir as seguintes certificações ou equivalentes:
5.17.2.1 01 (uma) Certificação Auditor Líder ISO 27001;
5.17.2.2 01 (uma) Certificação Auditor Líder ISO 22301;
5.17.2.3 01 (uma) Certificação GCIA - GIAC Certified Intrusion Analyst;
5.17.2.4 01 (uma) Certificação CBCP – Certified Business Continuity Professional;
5.17.2.5 01 (uma) Certificação CISSP (Certified Information Systems Security Professional);
5.17.2.6 01 (uma) Certificação CGEIT - Certified Governance Enterprise IT (ISACA),
5.17.2.7 01 (uma) Certificação CISA - Certified Information Systems Auditor;
5.17.2.8 01 (uma) Certificação CISM - Certified Information Security Manager;
5.17.2.9 01 (uma) Certificação CRISC - Certified em Risk Control;
5.17.2.10 01 (uma) Certificação ITIL Expert – Information Technology Infrastructure Library;
5.17.2.11 01 (uma) Certificação PMI-PMP Project Management Professional ou 01 (uma) Certificação PMI-ACP Profissional Certificado em Métodos Ágeis, práticas e ferramentas e técnicas através de metodologias ágeis.
5.17.3 A comprovação de que os profissionais compõem o quadro permanente da licitante se fará mediante a apresentação de cópia da Carteira de Trabalho (CTPS) ou do contrato social da licitante, no caso de sócio, ou contrato de prestação de serviços pelo prazo de vigência do contrato.
5.17.4 A comprovação de que os profissionais são detentores de experiência se dará com o fornecimento de Atestado(s) de Capacidade Técnica (fornecido(s) por pessoa jurídica de direito público ou privado, em documento timbrado) e a comprovação de que os profissionais são detentores de conhecimento com apresentação de documentos comprobatórios de diplomas e das certificações exigidas.

6. FORMA DE ACOMPANHAMENTO DO CONTRATO

6.1 O acompanhamento e a fiscalização da execução do Contrato serão realizados por servidores do TJCE e designados como Fiscais do Contrato, os quais obedecerão às disposições de normas e resoluções internas do Tribunal, assim como o artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010.
6.2 Conforme alínea “a” do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, caberá à fiscalização providenciar elaboração do Plano de Inserção da contratada.
6.3 Conforme alínea “b” do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, deverá ser realizada reunião inicial com participação dos Fiscais do Contrato, do Representante Legal da Contratada (apresentando o Preposto da mesma) e demais intervenientes identificados.
6.4 Conforme item 2 da alínea “b” do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, entrega, por parte da Contratada, a pauta da reunião mencionada acima contemplará a entrega do Termo de Compromisso e do Termo de Ciência.
6.5 É importante informar que este Termo de Referência é fruto da sequência de trabalhos da etapa de Planejamento da Contratação conforme a INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, a qual dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional.
6.6 Conforme a instrução normativa acima, os documentos de planejamento (Análise de Viabilidade, Plano de Sustentação, Análise de Riscos e Estratégia de Contratação) foram devidamente elaborados e se encontram aprovados.

7. METODOLOGIA DE AVALIAÇÃO DA QUALIDADE

7.1 Todo o trabalho realizado pela CONTRATADA estará sujeito à avaliação técnica, sendo homologado quando estiver de acordo com o padrão de qualidade exigido pelos Órgãos e de acordo com os prazos definidos.
7.2 A documentação técnica gerada deverá seguir o padrão definido pelo TJCE ou pelo CONTRATANTE, sendo devidamente verificada por responsável técnico e atestada pelo Fiscal do Contrato;

8. LEVANTAMENTO DE QUANTITATIVOS

Bem/Serviço	Estimativa	Forma de Estimativa

FORNECIMENTO E IMPLANTAÇÃO DE FERRAMENTAS PARA AUTOMATIZAR A GESTÃO DA SEGURANÇA DA INFORMAÇÃO		
Software de gestão de segurança da informação	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Serviços de suporte, manutenção e atualização de software	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO		
Metodologia de gestão de risco documentada	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Piloto para validação da metodologia de gestão de riscos	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TRABALHO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIOS DE ACOMPANHAMENTO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
APRESENTAÇÃO INICIAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
SERVIÇO DE ANÁLISE DE RISCOS E VULNERABILIDADES EM SEGURANÇA DA INFORMAÇÃO		
Relatório Análise do Faltante (Gap Analisys)	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório de Inventário de Ativos de Informação	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório Gerencial de Riscos	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório de Ocorrência de Riscos Identificados e Recomendações	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório de Mitigação de Riscos	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Plano de Tratamento de Riscos	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Plano de Tratamento de Riscos Anual	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório Trimestral de Riscos dos Ativos	04	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório Consolidado de Riscos	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TRABALHO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIOS DE ACOMPANHAMENTO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
APRESENTAÇÃO INICIAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
SERVIÇO DE TESTES DE INVASÃO INTERNOS E EXTERNOS		
PLANO DE TESTE DE INVASÃO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIO DE DESCOBERTA DE TESTE DE INVASÃO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIO DE RETORNO SOBRE INVESTIMENTO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIO DA SEGURANÇA FÍSICA	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIO DA SEGURANÇA TÉCNICO ADMINISTRATIVA	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TESTE DE INVASÃO anual	01	Estimativa da quantidade dos produtos a serem

		entregues durante o contrato
RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO mensal	12	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO trimestral	04	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO semestral	02	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TRABALHO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIOS DE ACOMPANHAMENTO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
APRESENTAÇÃO INICIAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO		
Modelo de Gestão de Resposta a Incidentes	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Proposta de Implantação	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Documento com Missão da ETIR	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Documento de constituição da ETIR	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Documento com detalhamento de tipos de serviços, tarefas e ações da ETIR	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Política de classificação de incidentes computacionais	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Modelo de formulário para reporte de incidentes computacionais	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Proposta de utilização de ferramentas para limpeza completa de dados	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Procedimento de comunicação da ETIR do TJCE em caso de indícios de ilícitos criminais	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Proposta de treinamento	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Treinamento para os membros do ETIR	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TRABALHO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIOS DE ACOMPANHAMENTO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
APRESENTAÇÃO INICIAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DO MODELO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO		
Relatório com análise da estruturação e atuação do Comitê	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório de Propostas de Melhoria	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Definições de infraestrutura de Segurança da Informação	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Modelo de gestão documentado	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TRABALHO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIOS DE ACOMPANHAMENTO	01	Estimativa da quantidade dos produtos a serem

		entregues durante o contrato
APRESENTAÇÃO INICIAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		
Relatório com Análise das Normas vigentes	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório de Propostas de Melhoria das Normas vigentes	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Documento de Política de Segurança da Informação, com o novo conjunto de normativos	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Documento para formalização e aprovação por parte da autoridade máxima responsável	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Dicionário dos termos técnicos utilizados nos documentos	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Sumário executivo para apresentação à alta Administração	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Guia de consulta rápida	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TRABALHO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIOS DE ACOMPANHAMENTO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
APRESENTAÇÃO INICIAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
SERVIÇO DE ELABORAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL		
Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE)	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIO INICIAL para o TJCE	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA)	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE RECUPERAÇÃO DE OPERAÇÕES	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TESTES E EXERCÍCIOS	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Treinamento das equipes de recuperação de desastres	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatórios de testes realizados	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato

Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE) - anual	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TRABALHO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIOS DE ACOMPANHAMENTO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
APRESENTAÇÃO INICIAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
SERVIÇO DE ELABORAÇÃO DO PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO		
Relatório técnico com as necessidades que a nova arquitetura de Segurança de TI do TJCE precisará satisfazer	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Documento com objetivos de evolução da rede corporativa do TJCE	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Documento com ajustes necessários no núcleo básico da arquitetura de segurança	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório do Plano Diretor de Segurança da Informação	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Cronograma de Trabalho anexo ao relatório	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Relatório do Plano Diretor de Segurança da Informação – anual.	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TRABALHO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIOS DE ACOMPANHAMENTO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
APRESENTAÇÃO INICIAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
SERVIÇO DE DIVULGAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO		
Plano de Divulgação e Treinamento	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Palestras da Semana da Segurança da Informação	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Palestras do Seminário de Segurança da Informação	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Treinamentos do Corpo Técnico de TI da SETIN - Gestão de continuidade de negócios	10	Estimativa da quantidade de participantes a serem treinados durante o contrato
Treinamentos do Corpo Técnico de TI da SETIN – Sistemas de gestão de segurança da informação	10	Estimativa da quantidade de participantes a serem treinados durante o contrato
Treinamentos do Corpo Técnico de TI da SETIN - Gestão de riscos em TI	10	Estimativa da quantidade de participantes a serem treinados durante o contrato
Treinamentos do Corpo Técnico de TI da SETIN – Diretrizes para gestão da segurança da informação para organizações de telecomunicações	10	Estimativa da quantidade de participantes a serem treinados durante o contrato
Treinamentos dos integrantes do Comitê de Segurança da Informação - Sistemas de gestão de segurança da informação	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
Workshop para a alta Administração do TJCE	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
PLANO DE TRABALHO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
RELATÓRIOS DE ACOMPANHAMENTO	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato
APRESENTAÇÃO INICIAL	01	Estimativa da quantidade dos produtos a serem entregues durante o contrato

9. CONDIÇÕES PARA PAGAMENTO

9.1 O fornecimento do software poderá ser faturado após a solicitação de pagamento por parte da CONTRATADA e entrega/aceite dos documentos comprobatórios (entregáveis) dos mesmos. A aceitação será formalizada, pela CONTRATANTE, através da emissão do Termo de Recebimento Definitivo (TRD) ou documento similar;
9.2 Os serviços poderão ser faturados após a solicitação de pagamento por parte da CONTRATADA e entrega/aceite dos documentos comprobatórios (entregáveis) dos mesmos. A aceitação será formalizada, pela CONTRATANTE, através da emissão do Termo de Recebimento Definitivo (TRD) ou documento similar;
9.3 As notas fiscais deverão ser emitidas em nome do Fundo de Especial de Reaparelhamento e Modernização do Judiciário – FERMOJU, CNPJ nº. 41.655.846/0001-47;
9.4 O pagamento referente ao fornecimento e aos serviços serão realizados através de depósito bancário nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias corridos contados do recebimento do documento fiscal previamente assinado pelas unidades responsáveis pelo contrato;
9.5 O Tribunal de Justiça reserva-se o direito de recusar o pagamento, no ato da ATESTAÇÃO, caso o objeto não esteja em conformidade com as condições deste instrumento;
9.6 Nenhum pagamento será efetuado à CONTRATADA na pendência de qualquer uma das situações abaixo especificadas, sem que isso gere direito a alteração de preços ou compensação financeira: Apresentação da Certidão Negativa de Débito da Previdência Social – CND; Apresentação de Certidão Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida Ativa da União; Apresentação de Certidão Negativa de Débitos junto aos Governos Estadual e Municipal; Apresentação de Certificado de Regularidade do FGTS – CRF; Certidão Negativa de Débitos Trabalhistas.
9.7 Nenhum pagamento será efetuado à CONTRATADA antes de paga à multa que por ventura lhe tenha sido aplicada;
9.8 Caso existam penalidades a serem aplicadas a CONTRATADA será notificada, conforme especificado no item **MECANISMOS FORMAIS DE COMUNICAÇÃO**, sendo o prazo do atesto da respectiva ORDEM DE SERVIÇO interrompido até a entrega das justificativas pela CONTRATADA;

10. GARANTIA CONTRATUAL

10.1 Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive pagamento de multas eventualmente aplicadas, a licitante prestará garantia no percentual de 5% (cinco por cento) do valor total do contrato, podendo a CONTRATADA optar por qualquer das modalidades previstas no art. 56 da Lei 8.666/93, a saber:
10.1.1 Caução em dinheiro ou títulos da dívida pública, cuja exigibilidade não seja contestada pelo TJCE;
10.1.2 Quando se tratar de caução em dinheiro, deverá ser recolhido na Secretaria de Finanças do TJCE;
10.1.3 Seguro garantia;
10.1.4 Fiança bancária.
10.2 Em se tratando de fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil;
10.3 Se o valor da garantia for utilizado em pagamento de qualquer obrigação, a Contratada deverá re-integralizar o seu valor, no prazo não superior a 10 (dez) dias corridos, contados da data em que for notificada;
10.4 A não apresentação da garantia até a assinatura contratual significará recusa à assinatura do contrato, ensejando aplicação das sanções previstas;
10.5 No caso de rescisão do contrato, a garantia se presta a cobrir prejuízos comprovados;

11. PROPRIEDADE, SIGILO, RESTRIÇÕES

11.1 A contratada cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do art. 111, da Lei Federal N.º 8.666/93, combinado com o art. 4.º, da Lei Federal N.º 9.609/98, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência dos serviços contratados, entendendo-se por resultados quaisquer estudos, relatórios, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presenta contratação, em papel ou em mídia eletrônica;
11.2 Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a CONTRATADA, zelar por si, por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados;
11.3 A obrigação assumida de Confidencialidade permanecerá válida durante o período de vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA, previstas no CONTRATO e na legislação pertinente;

11.4 Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados, a qualquer título, da equipe executante do Objeto deste Termo de Referência, a assinatura do ANEXO 09 - TERMO DE COMPROMISSO, bem como a assinatura do ANEXO 08 – TERMO DE CIÊNCIA onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.

12. MECANISMOS FORMAIS DE COMUNICAÇÃO

Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade
Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Através de telefone, e-mail, presencial, relatórios, documentos de texto, planilhas, slides, e-mail, sítios da internet, PDF (*Portable Document Format*): documento em formato portável.	Quando necessário
Comunicações oficiais	Contratada/ Contratante	Contratante/ Contratada	Ofício por correspondência	Quando necessário

13. ESTIMATIVA DOS PREÇOS UNITÁRIOS

ITEM	UND	QTD	DESCRIÇÃO	VALOR UNIT. (R$)	VALOR TOTAL (R$)
FORNECIMENTO E IMPLANTAÇÃO DE FERRAMENTAS PARA AUTOMATIZAR A GESTÃO DA SEGURANÇA DA INFORMAÇÃO					
1	UND	01	Software de gestão de segurança da informação	R$ 352.131,74	R$ 352.131,74
2	UND	01	Serviços de suporte, manutenção e atualização de software	R$ 81.957,87	R$ 81.957,87
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO					
3	UND	01	Metodologia de gestão de risco documentada	R$ 14.440,21	R$ 14.440,21
4	UND	01	Piloto para validação da metodologia de gestão de riscos	R$ 36.935,81	R$ 36.935,81
5	UND	01	PLANO DE TRABALHO	R$ 9.163,15	R$ 9.163,15
6	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 33.637,65	R$ 33.637,65
7	UND	01	APRESENTAÇÃO INICIAL	R$ 8.998,24	R$ 8.998,24
SERVIÇO DE ANÁLISE DE RISCOS E VULNERABILIDADES EM SEGURANÇA DA INFORMAÇÃO					
8	UND	01	Relatório Análise do Faltante (Gap Analisys)	R$ 75.789,58	R$ 75.789,58
9	UND	01	Relatório de Inventário de Ativos de Informação	R$ 38.142,15	R$ 38.142,15
10	UND	01	Relatório Gerencial de Riscos	R$ 39.131,60	R$ 39.131,60
11	UND	01	Relatório de Ocorrência de Riscos Identificados e Recomendações	R$ 39.131,60	R$ 39.131,60
12	UND	01	Relatório de Mitigação de Riscos	R$ 38.142,15	R$ 38.142,15
13	UND	01	Plano de Tratamento de Riscos	R$ 39.131,60	R$ 39.131,60
14	UND	01	Plano de Tratamento de Riscos Anual	R$ 73.315,96	R$ 73.315,96
15	UND	04	Relatório Trimestral de Riscos dos Ativos	R$ 18.328,99	R$ 73.315,96
16	UND	01	Relatório Consolidado de Riscos	R$ 73.315,96	R$ 73.315,96
17	UND	01	PLANO DE TRABALHO	R$ 69.358,17	R$ 69.358,17
18	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 70.842,34	R$ 70.842,34
19	UND	01	APRESENTAÇÃO INICIAL	R$ 69.358,17	R$ 69.358,17
SERVIÇO DE TESTES DE INVASÃO INTERNOS E EXTERNOS					
20	UND	01	PLANO DE TESTE DE INVASÃO	R$ 63.410,72	R$ 63.410,72
21	UND	01	RELATÓRIO DE DESCOBERTA DE TESTE DE INVASÃO	R$ 69.842,14	R$ 69.842,14
22	UND	01	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO	R$ 69.842,14	R$ 69.842,14
23	UND	01	RELATÓRIO DE RETORNO SOBRE INVESTIMENTO	R$ 67.863,24	R$ 67.863,24

24	UND	01	RELATÓRIO DA SEGURANÇA FÍSICA	R$ 70.336,86	R$ 70.336,86
25	UND	01	RELATÓRIO DA SEGURANÇA TÉCNICO ADMINISTRATIVA	R$ 69.842,14	R$ 69.842,14
26	UND	01	PLANO DE TESTE DE INVASÃO anual	R$ 63.410,72	R$ 63.410,72
27	UND	12	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO mensal	R$ 15.709,28	R$ 188.511,36
28	UND	04	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO trimestral	R$ 16.368,92	R$ 65.475,68
29	UND	02	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO semestral	R$ 17.358,36	R$ 34.716,72
30	UND	01	PLANO DE TRABALHO	R$ 63.410,72	R$ 63.410,72
31	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 65.389,62	R$ 65.389,62
32	UND	01	APRESENTAÇÃO INICIAL	R$ 63.410,72	R$ 63.410,72
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO					
33	UND	01	Modelo de Gestão de Resposta a Incidentes	R$ 13.615,67	R$ 13.615,67
34	UND	01	Proposta de Implantação	R$ 5.653,48	R$ 5.653,48
35	UND	01	Documento com Missão da ETIR	R$ 5.653,48	R$ 5.653,48
36	UND	01	Documento de constituição da ETIR	R$ 6.972,74	R$ 6.972,74
37	UND	01	Documento com detalhamento de tipos de serviços, tarefas e ações da ETIR	R$ 8.292,01	R$ 8.292,01
38	UND	01	Política de classificação de incidentes computacionais	R$ 9.899,92	R$ 9.899,92
39	UND	01	Modelo de formulário para reporte de incidentes computacionais	R$ 8.049,96	R$ 8.049,96
40	UND	01	Proposta de utilização de ferramentas para limpeza completa de dados	R$ 5.653,48	R$ 5.653,48
41	UND	01	Procedimento de comunicação da ETIR do TJCE em caso de indícios de ilícitos criminais	R$ 7.632,37	R$ 7.632,37
42	UND	01	Proposta de treinamento	R$ 4.664,03	R$ 4.664,03
43	UND	01	Treinamento para os membros do ETIR	R$ 13.615,67	R$ 13.615,67
44	UND	01	PLANO DE TRABALHO	R$ 8.998,24	R$ 8.998,24
45	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 11.966,59	R$ 11.966,59
46	UND	01	APRESENTAÇÃO INICIAL	R$ 8.998,24	R$ 8.998,24
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DO MODELO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO					
47	UND	01	Relatório com análise da estruturação e atuação do Comitê	R$ 14.303,98	R$ 14.303,98
48	UND	01	Relatório de Propostas de Melhoria	R$ 14.303,98	R$ 14.303,98
49	UND	01	Definições de infraestrutura de Segurança da Informação	R$ 30.586,85	R$ 30.586,85
50	UND	01	Modelo de gestão documentado	R$ 40.933,04	R$ 40.933,04
51	UND	01	PLANO DE TRABALHO	R$ 11.335,63	R$ 11.335,63
52	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 13.644,35	R$ 13.644,35
53	UND	01	APRESENTAÇÃO INICIAL	R$ 11.335,63	R$ 11.335,63
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO					
54	UND	01	Relatório com Análise das Normas vigentes	R$ 20.885,96	R$ 20.885,96
55	UND	01	Relatório de Propostas de Melhoria das Normas vigentes	R$ 20.391,24	R$ 20.391,24
56	UND	01	Documento de Política de Segurança da Informação, com o novo conjunto de normativos	R$ 30.780,44	R$ 30.780,44
57	UND	01	Documento para formalização e aprovação por parte da autoridade máxima responsável	R$ 23.359,58	R$ 23.359,58
58	UND	01	Dicionário dos termos técnicos utilizados nos documentos	R$ 20.885,96	R$ 20.885,96

59	UND	01	Sumário executivo para apresentação à alta Administração	R$ 20.885,96	R$ 20.885,96
60	UND	01	Guia de consulta rápida	R$ 20.885,96	R$ 20.885,96
61	UND	01	PLANO DE TRABALHO	R$ 16.928,17	R$ 16.928,17
62	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 16.928,17	R$ 16.928,17
63	UND	01	APRESENTAÇÃO INICIAL	R$ 16.928,17	R$ 16.928,17
SERVIÇO DE ELABORAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL					
64	UND	01	Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE)	R$ 44.877,93	R$ 44.877,93
65	UND	01	RELATÓRIO INICIAL para o TJCE	R$ 40.425,41	R$ 40.425,41
66	UND	01	PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	R$ 80.356,10	R$ 80.356,10
67	UND	01	PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS	R$ 41.414,86	R$ 41.414,86
68	UND	01	PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA)	R$ 44.877,93	R$ 44.877,93
69	UND	01	PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	R$ 44.877,93	R$ 44.877,93
70	UND	01	PLANO DE RECUPERAÇÃO DE OPERAÇÕES	R$ 47.351,55	R$ 47.351,55
71	UND	01	PLANO DE TESTES E EXERCÍCIOS	R$ 44.877,93	R$ 44.877,93
72	UND	01	PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE	R$ 42.404,31	R$ 42.404,31
73	UND	01	PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL	R$ 44.877,93	R$ 44.877,93
74	UND	01	PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS	R$ 44.877,93	R$ 44.877,93
75	TUR	01	Treinamento das equipes de recuperação de desastres	R$ 40.425,41	R$ 40.425,41
76	UND	01	Relatórios de testes realizados	R$ 40.425,41	R$ 40.425,41
77	UND	01	Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE) - anual	R$ 44.877,93	R$ 44.877,93
78	UND	01	PLANO DE TRABALHO	R$ 80.356,10	R$ 80.356,10
79	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 80.356,10	R$ 80.356,10
80	UND	01	APRESENTAÇÃO INICIAL	R$ 80.356,10	R$ 80.356,10
SERVIÇO DE ELABORAÇÃO DO PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO					
81	UND	01	Relatório técnico com as necessidades que a nova arquitetura de Segurança de TI do TJCE precisará satisfazer	R$ 30.310,81	R$ 30.310,81
82	UND	01	Documento com objetivos de evolução da rede corporativa do TJCE	R$ 8.814,51	R$ 8.814,51
83	UND	01	Documento com ajustes necessários no núcleo básico da arquitetura de segurança	R$ 31.300,26	R$ 31.300,26
84	UND	01	Relatório do Plano Diretor de Segurança da Informação	R$ 45.152,53	R$ 45.152,53
85	UND	01	Cronograma de Trabalho anexo ao relatório	R$ 8.814,51	R$ 8.814,51
86	UND	01	Relatório do Plano Diretor de Segurança da Informação – anual.	R$ 35.258,05	R$ 35.258,05
87	UND	01	PLANO DE TRABALHO	R$ 14.660,68	R$ 14.660,68
88	UND	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 15.979,95	R$ 15.979,95
89	UND	01	APRESENTAÇÃO INICIAL	R$ 14.660,68	R$ 14.660,68
SERVIÇO DE DIVULGAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO					
90	UND	01	Plano de Divulgação e Treinamento	R$ 9.104,36	R$ 9.104,36

91	PRO	01	Palestras da Semana da Segurança da Informação	R$ 10.802,37	R$ 10.802,37
92	PRO	01	Palestras do Seminário de Segurança da Informação	R$ 11.132,19	R$ 11.132,19
93	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN - Gestão de continuidade de negócios	R$ 2.242,39	R$ 22.423,90
94	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN – Sistemas de gestão de segurança da informação	R$ 2.242,39	R$ 22.423,90
95	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN - Gestão de riscos em TI	R$ 2.242,39	R$ 22.423,90
96	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN – Diretrizes para gestão da segurança da informação para organizações de telecomunicações	R$ 2.242,39	R$ 22.423,90
97	UND	01	Treinamentos dos integrantes do Comitê de Segurança da Informação - Sistemas de gestão de segurança da informação	R$ 22.423,91	R$ 22.423,91
98	UND	01	Workshop para a alta Administração do TJCE	R$ 11.436,01	R$ 11.436,01
99	UND	01	PLANO DE TRABALHO	R$ 17.107,42	R$ 17.107,42
100	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 17.107,42	R$ 17.107,42
101	UND	01	APRESENTAÇÃO INICIAL	R$ 17.107,42	R$ 17.107,42
				TOTAL	**R$ 3.955.557,18**

Obs: Valores obtidos através da média de 03 propostas da pesquisa mercadológica. Valores arrendondados em função das divisões.

14. ADEQUAÇÃO ORÇAMENTÁRIA

Fonte	**Ação**	**PPA - 2012/2015**
Fundo Especial de Reaparelhamento e Modernização do Poder Judiciário do Estado do Ceará (FERMOJU)	**Manutenção e funcionamento de TI**	**Iniciativa 00001 - Ampliação e Modernização da infraestrutura do Tribunal de Justiça do Estado do Ceará**
Software de gestão de segurança da informação		**Serviço**
Serviço de suporte, manutenção e atualização de software		**Serviço**
Serviço de elaboração das metodologias de gestão de riscos em segurança da informação		**Serviço**
Serviço de análise de riscos e vulnerabilidades em segurança da informação		**Serviço**
Serviço de testes de invasão internos e externos		**Serviço**
Serviço de elaboração das metodologias de tratamento e resposta a incidentes de segurança da informação		**Serviço**
Serviço de criação, revisão e atualização do modelo de gestão de segurança da informação		**Serviço**
Serviço de criação, revisão e atualização da política de segurança da informação		**Serviço**
Serviço de elaboração do plano de recuperação de desastres em ambiente computacional		**Serviço**
Serviço de elaboração do plano diretor de segurança da informação		**Serviço**
Serviço de divulgação e treinamento em segurança da informação		**Serviço**
Código do Projeto		**PJSETIN2012028 PJSETIN2012030**
Código Financeiro		**1112012028 1112012030**
Regionalização da Despesa		**Fortaleza/CE**
Exercício 2013/2014		**R$ 3.955.557,18**

15. SANÇÕES ADMINISTRATIVAS

15.1 Atendendo ao Art. 15, inciso III, alínea "h" da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010 e conforme os Arts. 86, 87 e 88 da Lei No 8.666 de 1993, seguem, abaixo, definições claras e detalhadas das sanções administrativas a serem aplicadas a esta contratação com vinculação por Termo de Contrato.
15.2 Pela inexecução total ou parcial do objeto definido neste Termo de Referência, o TJCE poderá, garantida a prévia defesa, aplicar à Contratada, as sanções a seguir, de acordo com o grau do prejuízo causado pelo descumprimento das respectivas obrigações:
15.2.1 Advertência escrita quando se tratar de infração leve, a juízo da fiscalização, no caso de descumprimento das obrigações e responsabilidades assumidas no contrato ou ainda no caso de outras ocorrências que possam acarretar prejuízos ao TJCE desde que não caiba a aplicação de sanção mais grave;
15.2.2 0,3% (três décimos por cento) por dia sobre o valor dos serviços entregues com atraso, até o percentual de 9% (nove por cento) e mais 1% (um por cento) caso ultrapasse os 30 dias de atraso. Decorridos mais de 30 (trinta) dias de atraso o TJCE poderá decidir pela rescisão, em razão da inexecução total.
15.2.3 1% (um por cento) por dia sobre o valor da garantia contratual, pela não apresentação/atualização, até o percentual de 10% (dez por cento) no prazo estabelecido neste instrumento, da garantia de execução contratual.
15.2.4 0,5% (meio por cento) por evento sobre o valor global atualizado do contrato, pela não manutenção das condições de habilitação e qualificação exigidas no instrumento convocatório.
15.2.5 10 % (dez por cento) sobre o valor do contrato, nas hipóteses de rescisão contratual por inexecução total do contrato.
15.2.6 Suspensão temporária de participar em licitação e impedimento de contratar com a Administração, pelo prazo não superior a 5 (cinco) anos;
15.2.7 Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos que determinaram sua punição ou até que seja promovida a sua reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

16. DA VIGÊNCIA CONTRATUAL

16.1 O contrato deverá ter vigência iniciando-se na data de sua assinatura e com duração de 24 (vinte e quatro) meses, permitindo efetuar o acompanhamento da execução do Plano Diretor de Segurança da Informação – PDSI no ciclo de sua operação de 04 (quatro) anos.

17. DA VISTORIA TÉCNICA AO AMBIENTE DA CONTRATANTE

17.1 A critério da licitante, caso seja necessário levantar, in-loco, subsídios para formulação de suas propostas, esta poderá realizar vistoria técnica nas instalações do Tribunal, em dias úteis durante o horário de 09:00 às 17:00 horas. Caso a licitante não realize a vistoria técnica deverá emitir declaração de dispensa informando que tem pleno conhecimento da natureza e do escopo dos serviços.
17.2 O agendamento da vistoria deverá ser previamente efetuado nos telefones de contatos do TJCE, mencionando as informações de contato da Empresa (razão social, endereço e telefone) e de seu representante (nome completo e telefone) o qual efetuará a vistoria.
17.2.1 TJCE: na Av. General Afonso Albuquerque Lima, S/N. - Cambeba CEP: 60822-325, Fortaleza-CE, por meio dos telefones: (85) 3207-7756 / 6850, na Secretaria de tecnologia da Informação.
17.3 A vistoria deverá ser agendada e realizada em no máximo 02 (dois) dias úteis antes da abertura das propostas.
17.4 Durante a vistoria, será dado acesso às dependências do Tribunal.
17.5 Quando da vistoria, a Licitante deverá se inteirar de todos os aspectos referentes à execução do fornecimento, não se admitindo, posteriormente, qualquer alegação de desconhecimento desses aspectos.
17.6 Para todos os efeitos, considerar-se-á que a Empresa tem pleno conhecimento da natureza e do escopo dos serviços, não se admitindo, posteriormente, qualquer alegação de desconhecimento desses elementos de contratação.
17.7 Efetuada a vistoria será lavrado, por representante da equipe técnica do TJCE designado para tanto, o respectivo Atestado de Vistoria, conforme modelo, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação.

18. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

18.1 Da Proposta de Preço

18.1.1 A proposta deverá conter obrigatoriamente os seguintes elementos:
18.1.1.1 Preço unitário por item, em moeda corrente nacional, cotados com apenas duas casas decimais,

expressos em algarismos e por extenso, sendo que, em caso de divergência entre os preços expressos em algarismos e por extenso, serão levados em consideração os últimos;
18.1.1.2 Não deve conter cotações alternativas, emendas, rasuras ou entrelinhas;
18.1.1.3 Deve fazer menção ao número do pregão e do processo licitatório;
18.1.1.4 Deve ser datada e assinada na última folha e rubricadas nas demais, pelo representante legal da empresa;
18.1.1.5 Deve conter na última folha o número do CNPJ da empresa;
18.1.1.6 Deve informar o prazo de validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, contados da data de entrega da mesma;
18.1.1.7 Indicação do nome do banco, número da agência, número da conta-corrente, para fins de recebimento dos pagamentos;
18.1.2 A proposta de preços deverá vir acompanhada, ainda, de:
18.1.2.1 Atestado de Capacidade Técnica e Declaração que disporá dos profissionais com capacidade técnica conforme ITEM 5.17 após a assinatura do contrato.

18.2 Da Qualificação Técnica

18.2.1 A licitante será habilitada a participar do certame com a apresentação de Atestado de Vistoria a ser fornecido pelo TJCE ou declaração de dispensa e Atestado(s) de Capacidade Técnica, a ser(em) fornecido(s) por pessoa jurídica de direito público ou privado, em documento timbrado, e que comprove(m) a aptidão da licitante para desempenho de atividade pertinente e compatível com o objeto da licitação, contendo:
18.2.1.1 Serviços de natureza e vulto compatíveis com o objeto ora licitado e que façam explícita referência pelo menos às parcelas de maior relevância técnica e valor significativo, que permitam estabelecer, por comparação, proximidade de características funcionais técnicas, dimensionais, quantitativas e qualitativas com o objeto da presente licitação, mencionando explicitamente os seguintes serviços:
18.2.1.1.1 Planejamento de Segurança da Informação;
18.2.1.1.2 Elaboração / revisão de Política de Segurança da Informação;
18.2.1.1.3 Gestão de Segurança da Informação, com base nas normas ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005;
18.2.1.1.4 Análise de riscos e vulnerabilidades em Segurança da Informação, com base nas normas ABNT NBR ISO Guia 73:2005 e ABNT NBR ISO/IEC 27005:2008;
18.2.1.1.5 Gestão de continuidade de negócios, com base nas normas ABNT NBR 15999- 1 e ABNT NBR 15999-2;
18.2.1.1.6 Elaboração das metodologias de tratamento e resposta a incidentes de Segurança da Informação;
18.2.1.1.7 Capacitação e treinamento em Segurança da Informação;
18.2.2 Serão aceitos o somatório de atestados para comprovação;
18.2.3 A Administração se resguarda no direito de diligência junto à pessoa jurídica do Atestado/Declaração de Capacidade Técnica, visando obter informação sobre o serviço prestado e cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatórios do conteúdo declarado.

18.3 Modalidade de Licitação

18.3.1 A modalidade de licitação sugerida deve ser o Pregão Eletrônico, considerando se tratar de bem e serviço comuns, nos termos da lei Federal n° 10.520/2002.

18.4 Tipo de Licitação

18.4.1 A licitação será do tipo menor preço global do lote. Os valores máximos aceitáveis, tanto unitários quanto global, estão descritos no item **ESTIMATIVA DE PREÇO.**

ANEXO 02

ORÇAMENTO DETALHADO

LOTE 01

ITEM	UND	QTD	DESCRIÇÃO	VALOR UNIT. (R$)	VALOR TOTAL MENSAL (R$)	VALOR TOTAL ANUAL (R$)
SERVIÇO DE ADMINISTRAÇÃO, GERENCIAMENTO E MONITORAMENTO DOS ATIVOS DE SEGURANÇA						
1	UND	03	Gerenciamento de appliance Firewall/VPN no site principal do tipo CISCO ASA 5550	R$ 4.221,62	R$ 12.664,86	R$ 151.978,32
2	UND	26	Gerenciamento de appliance firewall/VPN nos sites remotos do tipo CISCO ASA 5505	R$ 84,07	R$ 2.185,82	R$ 26.229,84
3	UND	190	Gerenciamento de appliance firewall/VPN nos sites remotos do tipo a ser adquirido pelo TJCE	R$ 84,07	R$ 15.973,30	R$ 191.679,60
4	UND	02	Gerenciamento de appliance IPS no site principal do tipo CISCO IPS-4260	R$ 3.458,14	R$ 6.916,28	R$ 82.995,36
5	UND	01	Gerenciamento de appliance SIEM no site principal do tipo CISCO Mars	R$ 8.078,89	R$ 8.078,89	R$ 96.946,68
SERVIÇO DE TRATAMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA						
6	SOL	01	Tratamento de Respostas a incidente - Firewall/VPN do tipo CISCO ASA 5550/5505	R$ 13.180,48	R$ 13.180,48	R$ 158.165,76
7	SOL	01	Tratamento de Respostas a incidente - IPS no site principal do tipo CISCO IPS-4260	R$ 2.688,51	R$ 2.688,51	R$ 32.262,12
8	SOL	01	Tratamento de Respostas a incidente - SIEM do tipo CISCO Mars	R$ 3.856,18	R$ 3.856,18	R$ 46.274,16
9	SOL	01	Tratamento de Respostas a incidente - Mail Security do tipo CISCO Ironport C160	R$ 4.888,83	R$ 4.888,83	R$ 58.665,96
10	SOL	01	Tratamento de Respostas a incidente - Web Security tipo McAfee Web Gateway	R$ 11.557,30	R$ 11.557,30	R$ 138.687,60
11	SOL	01	Tratamento de Respostas a incidente - EndPoint Security do tipo Kaspersky Security Center	R$ 13.327,83	R$ 13.327,83	R$ 159.933,96
					TOTAL	**R$ 1.143.819,36**

LOTE 02

ITEM	UND	QTD	DESCRIÇÃO	VALOR UNIT. (R$)	VALOR TOTAL (R$)
FORNECIMENTO E IMPLANTAÇÃO DE FERRAMENTAS PARA AUTOMATIZAR A GESTÃO DA SEGURANÇA DA INFORMAÇÃO					
1	UND	01	Software de gestão de segurança da informação	R$ 352.131,74	R$ 352.131,74
2	UND	01	Serviços de suporte, manutenção e atualização de software	R$ 81.957,87	R$ 81.957,87
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO					

3	UND	01	Metodologia de gestão de risco documentada	R$ 14.440,21	R$ 14.440,21
4	UND	01	Piloto para validação da metodologia de gestão de riscos	R$ 36.935,81	R$ 36.935,81
5	UND	01	PLANO DE TRABALHO	R$ 9.163,15	R$ 9.163,15
6	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 33.637,65	R$ 33.637,65
7	UND	01	APRESENTAÇÃO INICIAL	R$ 8.998,24	R$ 8.998,24
SERVIÇO DE ANÁLISE DE RISCOS E VULNERABILIDADES EM SEGURANÇA DA INFORMAÇÃO					
8	UND	01	Relatório Análise do Faltante (Gap Analisys)	R$ 75.789,58	R$ 75.789,58
9	UND	01	Relatório de Inventário de Ativos de Informação	R$ 38.142,15	R$ 38.142,15
10	UND	01	Relatório Gerencial de Riscos	R$ 39.131,60	R$ 39.131,60
11	UND	01	Relatório de Ocorrência de Riscos Identificados e Recomendações	R$ 39.131,60	R$ 39.131,60
12	UND	01	Relatório de Mitigação de Riscos	R$ 38.142,15	R$ 38.142,15
13	UND	01	Plano de Tratamento de Riscos	R$ 39.131,60	R$ 39.131,60
14	UND	01	Plano de Tratamento de Riscos Anual	R$ 73.315,96	R$ 73.315,96
15	UND	04	Relatório Trimestral de Riscos dos Ativos	R$ 18.328,99	R$ 73.315,96
16	UND	01	Relatório Consolidado de Riscos	R$ 73.315,96	R$ 73.315,96
17	UND	01	PLANO DE TRABALHO	R$ 69.358,17	R$ 69.358,17
18	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 70.842,34	R$ 70.842,34
19	UND	01	APRESENTAÇÃO INICIAL	R$ 69.358,17	R$ 69.358,17
SERVIÇO DE TESTES DE INVASÃO INTERNOS E EXTERNOS					
20	UND	01	PLANO DE TESTE DE INVASÃO	R$ 63.410,72	R$ 63.410,72
21	UND	01	RELATÓRIO DE DESCOBERTA DE TESTE DE INVASÃO	R$ 69.842,14	R$ 69.842,14
22	UND	01	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO	R$ 69.842,14	R$ 69.842,14
23	UND	01	RELATÓRIO DE RETORNO SOBRE INVESTIMENTO	R$ 67.863,24	R$ 67.863,24
24	UND	01	RELATÓRIO DA SEGURANÇA FÍSICA	R$ 70.336,86	R$ 70.336,86
25	UND	01	RELATÓRIO DA SEGURANÇA TÉCNICO ADMINISTRATIVA	R$ 69.842,14	R$ 69.842,14
26	UND	01	PLANO DE TESTE DE INVASÃO anual	R$ 63.410,72	R$ 63.410,72
27	UND	12	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO mensal	R$ 15.709,28	R$ 188.511,36
28	UND	04	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO trimestral	R$ 16.368,92	R$ 65.475,68
29	UND	02	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO semestral	R$ 17.358,36	R$ 34.716,72
30	UND	01	PLANO DE TRABALHO	R$ 63.410,72	R$ 63.410,72
31	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 65.389,62	R$ 65.389,62
32	UND	01	APRESENTAÇÃO INICIAL	R$ 63.410,72	R$ 63.410,72
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO					
33	UND	01	Modelo de Gestão de Resposta a Incidentes	R$ 13.615,67	R$ 13.615,67
34	UND	01	Proposta de Implantação	R$ 5.653,48	R$ 5.653,48
35	UND	01	Documento com Missão da ETIR	R$ 5.653,48	R$ 5.653,48
36	UND	01	Documento de constituição da ETIR	R$ 6.972,74	R$ 6.972,74
37	UND	01	Documento com detalhamento de tipos de serviços, tarefas e ações da ETIR	R$ 8.292,01	R$ 8.292,01
38	UND	01	Política de classificação de incidentes computacionais	R$ 9.899,92	R$ 9.899,92
39	UND	01	Modelo de formulário para reporte de incidentes computacionais	R$ 8.049,96	R$ 8.049,96
40	UND	01	Proposta de utilização de ferramentas para limpeza completa de dados	R$ 5.653,48	R$ 5.653,48
41	UND	01	Procedimento de comunicação da ETIR do TJCE em caso de indícios de ilícitos criminais	R$ 7.632,37	R$ 7.632,37
42	UND	01	Proposta de treinamento	R$ 4.664,03	R$ 4.664,03
43	UND	01	Treinamento para os membros do ETIR	R$ 13.615,67	R$ 13.615,67
44	UND	01	PLANO DE TRABALHO	R$ 8.998,24	R$ 8.998,24
45	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 11.966,59	R$ 11.966,59
46	UND	01	APRESENTAÇÃO INICIAL	R$ 8.998,24	R$ 8.998,24
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DO MODELO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO					
47	UND	01	Relatório com análise da estruturação e atuação do Comitê	R$ 14.303,98	R$ 14.303,98
48	UND	01	Relatório de Propostas de Melhoria	R$ 14.303,98	R$ 14.303,98

49	UND	01	Definições de infraestrutura de Segurança da Informação	R$ 30.586,85	R$ 30.586,85
50	UND	01	Modelo de gestão documentado	R$ 40.933,04	R$ 40.933,04
51	UND	01	PLANO DE TRABALHO	R$ 11.335,63	R$ 11.335,63
52	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 13.644,35	R$ 13.644,35
53	UND	01	APRESENTAÇÃO INICIAL	R$ 11.335,63	R$ 11.335,63
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO					
54	UND	01	Relatório com Análise das Normas vigentes	R$ 20.885,96	R$ 20.885,96
55	UND	01	Relatório de Propostas de Melhoria das Normas vigentes	R$ 20.391,24	R$ 20.391,24
56	UND	01	Documento de Política de Segurança da Informação, com o novo conjunto de normativos	R$ 30.780,44	R$ 30.780,44
57	UND	01	Documento para formalização e aprovação por parte da autoridade máxima responsável	R$ 23.359,58	R$ 23.359,58
58	UND	01	Dicionário dos termos técnicos utilizados nos documentos	R$ 20.885,96	R$ 20.885,96
59	UND	01	Sumário executivo para apresentação à alta Administração	R$ 20.885,96	R$ 20.885,96
60	UND	01	Guia de consulta rápida	R$ 20.885,96	R$ 20.885,96
61	UND	01	PLANO DE TRABALHO	R$ 16.928,17	R$ 16.928,17
62	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 16.928,17	R$ 16.928,17
63	UND	01	APRESENTAÇÃO INICIAL	R$ 16.928,17	R$ 16.928,17
SERVIÇO DE ELABORAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL					
64	UND	01	Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE)	R$ 44.877,93	R$ 44.877,93
65	UND	01	RELATÓRIO INICIAL para o TJCE	R$ 40.425,41	R$ 40.425,41
66	UND	01	PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	R$ 80.356,10	R$ 80.356,10
67	UND	01	PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS	R$ 41.414,86	R$ 41.414,86
68	UND	01	PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA)	R$ 44.877,93	R$ 44.877,93
69	UND	01	PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	R$ 44.877,93	R$ 44.877,93
70	UND	01	PLANO DE RECUPERAÇÃO DE OPERAÇÕES	R$ 47.351,55	R$ 47.351,55
71	UND	01	PLANO DE TESTES E EXERCÍCIOS	R$ 44.877,93	R$ 44.877,93
72	UND	01	PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE	R$ 42.404,31	R$ 42.404,31
73	UND	01	PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL	R$ 44.877,93	R$ 44.877,93
74	UND	01	PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS	R$ 44.877,93	R$ 44.877,93
75	TUR	01	Treinamento das equipes de recuperação de desastres	R$ 40.425,41	R$ 40.425,41
76	UND	01	Relatórios de testes realizados	R$ 40.425,41	R$ 40.425,41
77	UND	01	Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE) - anual	R$ 44.877,93	R$ 44.877,93
78	UND	01	PLANO DE TRABALHO	R$ 80.356,10	R$ 80.356,10
79	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 80.356,10	R$ 80.356,10
80	UND	01	APRESENTAÇÃO INICIAL	R$ 80.356,10	R$ 80.356,10
SERVIÇO DE ELABORAÇÃO DO PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO					
81	UND	01	Relatório técnico com as necessidades que a nova arquitetura de Segurança de TI do TJCE precisará satisfazer	R$ 30.310,81	R$ 30.310,81
82	UND	01	Documento com objetivos de evolução da rede corporativa do TJCE	R$ 8.814,51	R$ 8.814,51
83	UND	01	Documento com ajustes necessários no núcleo básico da arquitetura de segurança	R$ 31.300,26	R$ 31.300,26
84	UND	01	Relatório do Plano Diretor de Segurança da Informação	R$ 45.152,53	R$ 45.152,53

85	UND	01	Cronograma de Trabalho anexo ao relatório	R$ 8.814,51	R$ 8.814,51
86	UND	01	Relatório do Plano Diretor de Segurança da Informação – anual.	R$ 35.258,05	R$ 35.258,05
87	UND	01	PLANO DE TRABALHO	R$ 14.660,68	R$ 14.660,68
88	UND	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 15.979,95	R$ 15.979,95
89	UND	01	APRESENTAÇÃO INICIAL	R$ 14.660,68	R$ 14.660,68
SERVIÇO DE DIVULGAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO					
90	UND	01	Plano de Divulgação e Treinamento	R$ 9.104,36	R$ 9.104,36
91	PRO	01	Palestras da Semana da Segurança da Informação	R$ 10.802,37	R$ 10.802,37
92	PRO	01	Palestras do Seminário de Segurança da Informação	R$ 11.132,19	R$ 11.132,19
93	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN - Gestão de continuidade de negócios	R$ 2.242,39	R$ 22.423,90
94	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN – Sistemas de gestão de segurança da informação	R$ 2.242,39	R$ 22.423,90
95	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN - Gestão de riscos em TI	R$ 2.242,39	R$ 22.423,90
96	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN – Diretrizes para gestão da segurança da informação para organizações de telecomunicações	R$ 2.242,39	R$ 22.423,90
97	UND	01	Treinamentos dos integrantes do Comitê de Segurança da Informação - Sistemas de gestão de segurança da informação	R$ 22.423,91	R$ 22.423,91
98	UND	01	Workshop para a alta Administração do TJCE	R$ 11.436,01	R$ 11.436,01
99	UND	01	PLANO DE TRABALHO	R$ 17.107,42	R$ 17.107,42
100	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$ 17.107,42	R$ 17.107,42
101	UND	01	APRESENTAÇÃO INICIAL	R$ 17.107,42	R$ 17.107,42
				TOTAL	**R$ 3.955.557,18**

OBS 1: Os valores constantes na coluna "valor unitário", "valor total mensal" e "valor total" representam informação ao licitante quanto aos limites máximos por item, estimado pelo Tribunal, segundo pesquisa de mercado.

OBS 2: Na proposta do licitante deverão ser mantidas as informações constantes nas colunas "Item", "Und", "Qtd" e "Descrição", devendo preencher as colunas: "valor unitário", "valor total mensal" e "valor total", com a sua proposta de preços, observando os limites máximos unitários e totais informados.

ANEXO 03

MODELO DE APRESENTAÇÃO DA PROPOSTA

À
Comissão Permanente de Licitações do Tribunal de Justiça do Estado do Ceará

Ref.: Pregão Eletrônico nº _____
A proposta comercial encontra-se em conformidade com as informações previstas no edital e seus anexos.

1. Identificação do licitante:
- Razão Social:
- CPF/CNPJ e Inscrição Estadual:
- Endereço completo:
- Representante Legal (nome, nacionalidade, estado civil, profissão, RG, CPF, domicílio):
- Telefone, celular, fax, e-mail:
- Banco Brasileiro de Descontos S/A – BRADESCO, agência e nº da conta corrente:

2. Condições Gerais da Proposta:
- A presente proposta é válida por _____(_____) dias, contados da data de sua emissão.

3. Formação do Preço:

LOTE 01

ITEM	UND	QTD	DESCRIÇÃO	VALOR UNIT. (R$)	VALOR TOTAL MENSAL (R$)	VALOR TOTAL ANUAL (R$)
SERVIÇO DE ADMINISTRAÇÃO, GERENCIAMENTO E MONITORAMENTO DOS ATIVOS DE SEGURANÇA						
1	UND	03	Gerenciamento de appliance Firewall/VPN no site principal do tipo CISCO ASA 5550	R$	R$	R$
2	UND	26	Gerenciamento de appliance firewall/VPN nos sites remotos do tipo CISCO ASA 5505	R$	R$	R$
3	UND	190	Gerenciamento de appliance firewall/VPN nos sites remotos do tipo a ser adquirido pelo TJCE	R$	R$	R$
4	UND	02	Gerenciamento de appliance IPS no site principal do tipo CISCO IPS-4260	R$	R$	R$
5	UND	01	Gerenciamento de appliance SIEM no site principal do tipo CISCO Mars	R$	R$	R$
SERVIÇO DE TRATAMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA						
6	SOL	01	Tratamento de Respostas a incidente - Firewall/VPN do tipo CISCO ASA 5550/5505	R$	R$	R$
7	SOL	01	Tratamento de Respostas a incidente - IPS no site principal do tipo CISCO IPS-4260	R$	R$	R$
8	SOL	01	Tratamento de Respostas a incidente - SIEM do tipo CISCO Mars	R$	R$	R$
9	SOL	01	Tratamento de Respostas a incidente - Mail Security do tipo CISCO Ironport C160	R$	R$	R$
10	SOL	01	Tratamento de Respostas a incidente - Web Security tipo McAfee Web Gateway	R$	R$	R$
11	SOL	01	Tratamento de Respostas a incidente - EndPoint Security do tipo Kaspersky	R$	R$	R$

			Security Center			
					TOTAL	**R$**

LOTE 02

ITEM	UND	QTD	DESCRIÇÃO	VALOR UNIT. (R$)	VALOR TOTAL (R$)
FORNECIMENTO E IMPLANTAÇÃO DE FERRAMENTAS PARA AUTOMATIZAR A GESTÃO DA SEGURANÇA DA INFORMAÇÃO					
1	UND	01	Software de gestão de segurança da informação	R$	R$
2	UND	01	Serviços de suporte, manutenção e atualização de software	R$	R$
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO					
3	UND	01	Metodologia de gestão de risco documentada	R$	R$
4	UND	01	Piloto para validação da metodologia de gestão de riscos	R$	R$
5	UND	01	PLANO DE TRABALHO	R$	R$
6	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$	R$
7	UND	01	APRESENTAÇÃO INICIAL	R$	R$
SERVIÇO DE ANÁLISE DE RISCOS E VULNERABILIDADES EM SEGURANÇA DA INFORMAÇÃO					
8	UND	01	Relatório Análise do Faltante (Gap Analisys)	R$	R$
9	UND	01	Relatório de Inventário de Ativos de Informação	R$	R$
10	UND	01	Relatório Gerencial de Riscos	R$	R$
11	UND	01	Relatório de Ocorrência de Riscos Identificados e Recomendações	R$	R$
12	UND	01	Relatório de Mitigação de Riscos	R$	R$
13	UND	01	Plano de Tratamento de Riscos	R$	R$
14	UND	01	Plano de Tratamento de Riscos Anual	R$	R$
15	UND	04	Relatório Trimestral de Riscos dos Ativos	R$	R$
16	UND	01	Relatório Consolidado de Riscos	R$	R$
17	UND	01	PLANO DE TRABALHO	R$	R$
18	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$	R$
19	UND	01	APRESENTAÇÃO INICIAL	R$	R$
SERVIÇO DE TESTES DE INVASÃO INTERNOS E EXTERNOS					
20	UND	01	PLANO DE TESTE DE INVASÃO	R$	R$
21	UND	01	RELATÓRIO DE DESCOBERTA DE TESTE DE INVASÃO	R$	R$
22	UND	01	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO	R$	R$
23	UND	01	RELATÓRIO DE RETORNO SOBRE INVESTIMENTO	R$	R$
24	UND	01	RELATÓRIO DA SEGURANÇA FÍSICA	R$	R$
25	UND	01	RELATÓRIO DA SEGURANÇA TÉCNICO ADMINISTRATIVA	R$	R$
26	UND	01	PLANO DE TESTE DE INVASÃO anual	R$	R$
27	UND	12	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO mensal	R$	R$
28	UND	04	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO trimestral	R$	R$
29	UND	02	RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO semestral	R$	R$
30	UND	01	PLANO DE TRABALHO	R$	R$
31	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$	R$
32	UND	01	APRESENTAÇÃO INICIAL	R$	R$
SERVIÇO DE ELABORAÇÃO DAS METODOLOGIAS DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO					
33	UND	01	Modelo de Gestão de Resposta a Incidentes	R$	R$
34	UND	01	Proposta de Implantação	R$	R$
35	UND	01	Documento com Missão da ETIR	R$	R$
36	UND	01	Documento de constituição da ETIR	R$	R$

37	UND	01	Documento com detalhamento de tipos de serviços, tarefas e ações da ETIR	R$	R$
38	UND	01	Política de classificação de incidentes computacionais	R$	R$
39	UND	01	Modelo de formulário para reporte de incidentes computacionais	R$	R$
40	UND	01	Proposta de utilização de ferramentas para limpeza completa de dados	R$	R$
41	UND	01	Procedimento de comunicação da ETIR do TJCE em caso de indícios de ilícitos criminais	R$	R$
42	UND	01	Proposta de treinamento	R$	R$
43	UND	01	Treinamento para os membros do ETIR	R$	R$
44	UND	01	PLANO DE TRABALHO	R$	R$
45	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$	R$
46	UND	01	APRESENTAÇÃO INICIAL	R$	R$
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DO MODELO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO					
47	UND	01	Relatório com análise da estruturação e atuação do Comitê	R$	R$
48	UND	01	Relatório de Propostas de Melhoria	R$	R$
49	UND	01	Definições de infraestrutura de Segurança da Informação	R$	R$
50	UND	01	Modelo de gestão documentado	R$	R$
51	UND	01	PLANO DE TRABALHO	R$	R$
52	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$	R$
53	UND	01	APRESENTAÇÃO INICIAL	R$	R$
SERVIÇO DE CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO					
54	UND	01	Relatório com Análise das Normas vigentes	R$	R$
55	UND	01	Relatório de Propostas de Melhoria das Normas vigentes	R$	R$
56	UND	01	Documento de Política de Segurança da Informação, com o novo conjunto de normativos	R$	R$
57	UND	01	Documento para formalização e aprovação por parte da autoridade máxima responsável	R$	R$
58	UND	01	Dicionário dos termos técnicos utilizados nos documentos	R$	R$
59	UND	01	Sumário executivo para apresentação à alta Administração	R$	R$
60	UND	01	Guia de consulta rápida	R$	R$
61	UND	01	PLANO DE TRABALHO	R$	R$
62	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$	R$
63	UND	01	APRESENTAÇÃO INICIAL	R$	R$
SERVIÇO DE ELABORAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL					
64	UND	01	Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE)	R$	R$
65	UND	01	RELATÓRIO INICIAL para o TJCE	R$	R$
66	UND	01	PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	R$	R$
67	UND	01	PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS	R$	R$
68	UND	01	PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA)	R$	R$
69	UND	01	PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE	R$	R$
70	UND	01	PLANO DE RECUPERAÇÃO DE OPERAÇÕES	R$	R$
71	UND	01	PLANO DE TESTES E EXERCÍCIOS	R$	R$
72	UND	01	PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE	R$	R$

73	UND	01	PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL	R$	R$
74	UND	01	PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS	R$	R$
75	TUR	01	Treinamento das equipes de recuperação de desastres	R$	R$
76	UND	01	Relatórios de testes realizados	R$	R$
77	UND	01	Plano de Recuperação de Desastres em Ambiente Computacional (PRDAC-TJCE) - anual	R$	R$
78	UND	01	PLANO DE TRABALHO	R$	R$
79	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$	R$
80	UND	01	APRESENTAÇÃO INICIAL	R$	R$
SERVIÇO DE ELABORAÇÃO DO PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO					
81	UND	01	Relatório técnico com as necessidades que a nova arquitetura de Segurança de TI do TJCE precisará satisfazer	R$	R$
82	UND	01	Documento com objetivos de evolução da rede corporativa do TJCE	R$	R$
83	UND	01	Documento com ajustes necessários no núcleo básico da arquitetura de segurança	R$	R$
84	UND	01	Relatório do Plano Diretor de Segurança da Informação	R$	R$
85	UND	01	Cronograma de Trabalho anexo ao relatório	R$	R$
86	UND	01	Relatório do Plano Diretor de Segurança da Informação – anual.	R$	R$
87	UND	01	PLANO DE TRABALHO	R$	R$
88	UND	01	RELATÓRIOS DE ACOMPANHAMENTO	R$	R$
89	UND	01	APRESENTAÇÃO INICIAL	R$	R$
SERVIÇO DE DIVULGAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO					
90	UND	01	Plano de Divulgação e Treinamento	R$	R$
91	PRO	01	Palestras da Semana da Segurança da Informação	R$	R$
92	PRO	01	Palestras do Seminário de Segurança da Informação	R$	R$
93	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN - Gestão de continuidade de negócios	R$	R$
94	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN – Sistemas de gestão de segurança da informação	R$	R$
95	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN - Gestão de riscos em TI	R$	R$
96	PAR	10	Treinamentos do Corpo Técnico de TI da SETIN – Diretrizes para gestão da segurança da informação para organizações de telecomunicações	R$	R$
97	UND	01	Treinamentos dos integrantes do Comitê de Segurança da Informação - Sistemas de gestão de segurança da informação	R$	R$
98	UND	01	Workshop para a alta Administração do TJCE	R$	R$
99	UND	01	PLANO DE TRABALHO	R$	R$
100	PRO	01	RELATÓRIOS DE ACOMPANHAMENTO	R$	R$
101	UND	01	APRESENTAÇÃO INICIAL	R$	R$
				TOTAL	**R$**

ANEXO 04

TERMO DE RECEBIMENTO PROVISÓRIO

Finalidade

Este documento tem como finalidade declarar formalmente para a contratada que os serviços foram prestados ou os bens foram recebidos para posterior análise de conformidades de qualidade, baseadas nos critérios de aceitação definidos no contrato.

1. Identificação

Contrato Nº:		**N. da OS/OFB**	
Objeto:			
Contratante	Matricula:		
Contratada	CNJP		

Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 25, inciso III, alínea "a" da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 12/11/2010, que os serviços (ou bens), relacionados na O.S. acima identificada, foram recebidos nesta data e serão objetos de avaliação quanto à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos pela Contratante.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até ___ dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

2. Aprovação

Contratante Nome do fiscal técnico do contrato Matricula	Contratada Nome do Preposto Qualificação

ANEXO 05

TERMO DE RECEBIMENTO DEFINITIVO

Finalidade

Este documento tem como finalidade declarar formalmente para a contratada que os serviços foram prestados ou os bens fornecidos foram devidamente avaliados e atendem aos requisitos estabelecidos em contrato.

1. Identificação

Contrato Nº:		**N. da OS/OFB**	
Objeto:			
Gestor do Contrato:			
Fiscal Requisitante do Contrato:			

Por este instrumento, os servidores acima identificados atestam, para fins de cumprimento do disposto no art. 25, inciso III, alínea "g" da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 12/11/2010, que o(s) serviço(s) ou bem(ns) integrantes da Ordem de Serviço ou de Fornecimento de Bens acima identificada possui(em) qualidade compatível com a especificada no Termo de Referência / Projeto Básico do Contrato supracitado.

2. Aprovação

_____

Contratada
Nome do Fiscal Requisitante do Contrato
Qualificação

De Acordo,

_____

Contratante
Nome do Gestor do Contrato
Matricula

ANEXO 06

MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO Nº XXX /2010					**DATA: xx/xx/xxxx**
SERVIÇO DESTINADO AO					
NOME DO CONTRATADO: COMERCIAL XXXXXXXXXX LTDA **CNPJ MF Nº: XX.XXX.XXX/XXXX-XX** **ENDEREÇO: RUA XXXXXXX , Nº XXX – BAIRRO:** **CEP: FONE: E-MAIL:**					
Banco		Agência		C/C	
CONTRATO Nº			LICITAÇÃO:		
PRAZO DE EXECUÇÃO:			EMPENHO Nº		
Autorizo V. Sa., a executar para esta universidade os serviços abaixo discriminados					
item	quant	unid	DISCRIMINAÇÃO DOS SERVIÇOS	Preço Unitário R$	Preço Total R$
Autorizado em xx / xx / xxxx			Recebido em xx / xx / xxxx		

ANEXO 07

PLANO DE MUDANÇA E LIBERAÇÃO – PML

Descrição:	[Descrição da atividade]
Solicitante - Cargo:	
Data da Solicitação:	[Data solicitada]

1. Autorizadores

Nome	Cargo

2. Motivação da Mudança
[Descrição da atividade a ser realizada]

3. Descrição da Mudança
[Descrever detalhadamente a mudança]

4. Janela de Execução

Horário Previsto	Data Prevista
[Horário para execução]	[Data da execução]

5. Serviços Afetados

Nome do Serviço	Impacto Previsto
[Preencher]	[Preencher]

6. Plano de Comunicação

[preencher ou remover se necessário.]

Nome Parceiro / Contratado / Funcionário	Motivo

7. Material necessário

[descrição de material extra, necessário para a mudança]

Descrição	Motivo	Quantidade
[Preencher]	[Preencher]	[Preencher]

8. Detalhamento de Execução

TEMPO TOTAL DA ATIVIDADE	[Preencher]

9. Plano de contingência / rollback
[Preencher em caso de retornar ao estado anterior a mudança]

10. Necessidades Adicionais

ITEM	OPÇÃO	DESCRIÇÃO
	[sim / não]	

11. Documentação a Ser Atualizada

ARQUIVO	LOCAL

[Preencher]	[Preencher]

12. Equipe Necessária

NOME	ESPECIALIDADE

13. Revisão Pós-implementação

[Preencher com testes ou verificações para após a mudança]

ANEXO 08

TERMO DE CIÊNCIA

Contrato N°:			
Objeto:			
Gestor do Contrato:		**Matr.:**	
Contratante (Órgão):			
Contratada:		**CNPJ:**	
Preposto da Contratada:		**CPF:**	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer a declaração de manutenção de sigilo e das normas de segurança vigentes na Contratante.

_____,_____ de _____ de 20_____.

Ciência

CONTRATADA
Funcionários

_____	_____
<Nome>	***<Nome>***
Matrícula: <*Matr.*>	**Matrícula: <*Matr.*>**
_____	_____
<Nome>	***<Nome>***
Matrícula: <*Matr.*>	**Matrícula: <*Matr.*>**
_____	_____
<Nome>	***<Nome>***
Matrícula: <*Matr.*>	**Matrícula: <*Matr.*>**
_____	_____
<Nome>	***<Nome>***
Matrícula: <*Matr.*>	**Matrícula: <*Matr.*>**
_____	_____
<Nome>	***<Nome>***
Matrícula: <*Matr.*>	**Matrícula: <*Matr.*>**
_____	_____
<Nome>	***<Nome>***
Matrícula: <*Matr.*>	**Matrícula: <*Matr.*>**

ANEXO 09

TERMO DE COMPROMISSO

Finalidade

Este documento tem como finalidade obter comprometimento formal dos empregados da contratada sobre o sigilo dos dados e informações de uso da contratante, bem como suas normas e políticas de segurança

1 Condições do Termo

O <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n.° <CNPJ>, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.° <CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;
CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;
CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;
Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

1.1 Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 4.553 de 27/12/2002 - Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

1.2 Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:
Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.
Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.
Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.
Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.
Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

1.3 Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de idéias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro – Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:
I – Sejam comprovadamente de domínio público no momento da revelação;
II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

1.4 Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.
I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.
I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:
I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;
III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

1.5 Cláusula Quinta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

1.6 Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

1.7 Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da eqüidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:
I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;
II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.
III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;
IV – Todas as condições, TERMOs e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;
V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;
VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;
VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;
VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

1.8 Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.
Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer a declaração de manutenção de sigilo e das normas de segurança vigentes na Contratante.

21. Aprovação

_____ de _____ de _____

Nome do Contratante Matricula Nº:	Nome da Contratada Qualificação

ANEXO 10

RECIBO DE RETIRADA DO EDITAL PELA INTERNET

PREGÃO ELETRÔNICO N.º _____/2014

OBS 1: Visando a possibilidade de comunicação futura entre este Tribunal de Justiça e essa empresa, solicitamos de Vossa Senhoria, preencher o formulário de recibo de retirada do Edital pela Internet e remete-lo à Comissão Permanente de Licitação por meio do *fax (085) 3207-7098 ou 3207-7100*, antes do início da sessão.

OBS 2: CASO O EDITAL SEJA RETIRADO NO SITE DO www.licitações-e.com.br ESTA EXIGÊNCIA NÃO É NECESSÁRIA.

EMPRESA (RAZÃO SOCIAL:

CNPJ N.º:

ENDEREÇO:

E-MAIL:

FONE/FAX:

CIDADE:

ESTADO:

PESSOA RESPONSÁVEL:

IDENTIDADE:

Retiramos, através do acesso à página ***www.*** _____, nesta data, cópia do Edital nº /20___, do TJCE.

_____, _____ de _____ de 2014.
(Local) **(Data)**

_____
Assinatura do Licitante

ANEXO 11

MODELO DE DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

A empresa _____, através de seu representante legal, o(a) Sr(a). _____, portador(a) da Carteira de Identidade n.º _____ e do CPF n.º_____, DECLARA para fins do Pregão Eletrônico n.º _____/2014, sob as sanções administrativas cabíveis e sob as penas da lei, que esta empresa, na presente data, é considerada:

( ) MICROEMPRESA, conforme incisos I e II, do artigo 3º, da Lei Complementar n.º 123, de 14/12/2006; ou
( ) EMPRESA DE PEQUENO PORTE, conforme incisos I e II, do artigo 3º, da Lei Complementar n.º 123, de 14/12/2006.

DECLARA ainda, que a empresa não se encontra alcançada por qualquer das hipóteses descritas no § 4º, do artigo 3º, da Lei Complementar n.º 123, de 14/12/2006.

Fortaleza-CE, em ____ de _____ de 2014.

_____
Empresa Proponente

À Sra.
Georgeanne Lima Gomes Botelho
Presidente da Comissão Permanente de Licitação

ANEXO 12

MODELO DE DECLARAÇÃO DE QUE NÃO EMPREGA MENOR

PREGÃO ELETRÔNICO Nº. _____/2014

DECLARAÇÃO

....., inscrita no CNPJ nº ....., por intermédio de seu representante legal o(a) Sr(a) ....., portador (a) da Carteira de Identidade nº ..... e do CPF nº ..... DECLARA, para fins do disposto no inciso V do art. 27 da Lei nº 8.666, de 21 de junho de 1993, acrescida pela Lei nº 9.854, de 27 de outubro de 1999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( ).

(DATA)

.....
(NOME)

(Observação: em caso afirmativo, assinalar a ressalva acima).

À Sra.
Georgeanne Lima Gomes Botelho
Presidente da Comissão Permanente de Licitação

ANEXO 13

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATOS IMPEDITIVOS SUPERVENIENTE À HABILITAÇÃO

A empresa _____(razão social), inscrita com o CNPJ nº _____, por intermédio do seu representante legal _____, portador da Carteira de Identidade nº _____ e do CPF _____, DECLARA, para fins de habilitação no Pregão Eletrônico nº _____/2014, em cumprimento a exigência contida no artigo 32, parágrafo 2º da Lei n° 8.666/93, não apresentar fato impeditivo e superveniente à sua habilitação, estando ciente da obrigação de declarar ocorrências posteriores.

Fortaleza, _____ de _____ de 2014.

_____
Empresa Proponente

À Sra.
Georgeanne Lima Gomes Botelho
Presidente da Comissão Permanente de Licitação

ANEXO 14

MODELO DE DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA

[IDENTIFICAÇÃO COMPLETA DO REPRESENTANTE DA LICITANTE], como representante devidamente constituído de [IDENTIFICAÇÃO COMPLETA DA LICITANTE] (doravante denominado [Licitante]), para fins do disposto no item 7.2.9 do Edital do Pregão Eletrônico nº 03/2014, declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

a) a proposta anexa foi elaborada de maneira independente [pelo Licitante], e que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº 03/2014, por qualquer meio ou por qualquer pessoa;
b) a intenção de apresentar a proposta anexa não foi informada a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº 03/2014, por qualquer meio ou por qualquer pessoa;
c) não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº 03/2014 quanto a participar ou não da referida licitação;
d) o conteúdo da proposta anexa não será, no todo ou em parte, direta ou indiretamente, comunicado a, ou discutido com qualquer outro participante potencial ou de fato do Pregão Eletrônico nº 03/2014 antes da adjudicação do objeto da referida licitação;
e) o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer integrante do(a) Tribunal de Justiça do Estado do Ceará antes da abertura oficial das propostas; e
f) está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

_____, em ___de _____ de _____.

_____
([REPRESENTANTE LEGAL DO LICITANTE NO ÂMBITO DA LICITAÇÃO, COM IDENTIFICAÇÃO COMPLETA])

À Sra.
Georgeanne Lima Gomes Botelho
Presidente da Comissão Permanente de Licitação

ANEXO 15

MINUTA DO CONTRATO (LOTE 1)

CONTRATO PARA EXECUÇÃO DOS SERVIÇOS ESPECIALIZADOS, SOB DEMANDA, DE ADMINISTRAÇÃO, GERENCIAMENTO E MONITORAMENTO DAS SOLUÇÕES DE SEGURANÇA DO TJCE E TRATAMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA DAS SOLUÇÕES DO TJCE, QUE ENTRE SI CELEBRAM O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ E A EMPRESA _____ (Processo Administrativo nº _____).

CT Nº /2014

O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, situado no Centro Administrativo Governador Virgílio Távora, Distrito de São José do Cambeba em Fortaleza – Ce, inscrito no CGC sob o número 09.444.530/0001-01, doravante denominado simplesmente de TJCE ou CONTRATANTE, neste ato representado pro seu Presidente, Des. _____ e por sua Secretária Geral, Dra. _____, e seu Secretário de Tecnologia da Informação,_____e a empresa_____, representada neste ato por_____ _____, portador da carteira de identidade n.º _____/___, CPF n.º _____, com endereço na _____, inscrita no CNPJ sob o número _____, daqui por diante simplesmente denominada CONTRATADA, pactuam o presente Contrato, que se regerá pela Lei Federal nº 10.520/02, pela Lei Federal n.º 8.666/93, com suas alterações e atualizações posteriores.

Cláusula Primeira – Da Fundamentação Legal

Fundamenta-se o presente Instrumento na proposta apresentada pela CONTRATADA e no resultado da Licitação realizada sob a modalidade Pregão Eletrônico n.° 03/2014, devidamente homologada pelo Exmo. Desembargador Presidente do Tribunal de Justiça do Estado do Ceará, tudo de conformidade com as disposições da Lei Federal nº 10.520/02 e da Lei Federal nº 8.666, com suas alterações e atualizações posteriores, e o processo administrativo nº _____.

Cláusula Segunda – Do Objeto

O Objeto deste Instrumento consiste na **Contratação de serviços especializados, sob demanda, de administração, gerenciamento e monitoramento das soluções de segurança do TJCE, e tratamento de resposta a incidentes de segurança, para atender as necessidades do Poder Judiciário do Estado do Ceará (Lote I)**, conforme especificações contidas no Edital do Pregão Eletrônico nº 03/2014 e seus anexos, bem nos Anexos_____ deste Contrato, todos partes integrantes do mesmo.

Parágrafo Único – A prestação dos serviços obedecerá ao estipulado neste Contrato, bem como às disposições assumidas na proposta firmada pela CONTRATADA, dirigida ao CONTRATANTE, independentemente da transcrição, a qual faz parte integrante e complementar deste Contrato, no que não o contrarie.

Cláusula Terceira – Das Obrigações das partes

São obrigações das partes no respectivo contrato:

I - DO CONTRATANTE:

a) Proporcionar todas as facilidades para a Contratada executar o fornecimento do objeto do presente Contrato, permitindo o acesso dos profissionais da Contratada às suas dependências. Esses profissionais ficarão sujeitos a todas as normas internas do TJCE, principalmente as de segurança, inclusive àquelas referentes à identificação, trajes, trânsito e permanência em suas dependências;

b) Promover o acompanhamento e a fiscalização da execução do objeto do presente Contrato, sob o aspecto quantitativo e qualitativo, anotando em registro próprio as falhas detectadas;

c) Comunicar prontamente à CONTRATADA qualquer anormalidade na execução do objeto, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014;

d) Fornecer à Contratada todo tipo de informação interna essencial à realização dos fornecimentos e dos serviços;

e) Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando esta estiver em conformidade com os padrões de informação e qualidade exigidos;

f) Homologar os serviços prestados, quando estes estiverem de acordo com o especificado no Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014;

g) Efetuar o pagamento à CONTRATADA;

II - DA CONTRATADA:

a) Atender a todas as condições descritas no Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014 e respectivo Contrato;

b) Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, contribuições previdenciárias, impostos e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que estes não têm nenhum vínculo empregatício com o TJCE;

c) Responsabilizar-se pelo fornecimento do objeto deste Contrato, respondendo civil e criminalmente por todos os danos, perdas e prejuízos que, por dolo ou culpa sua, de seus empregados, prepostos, ou terceiros no exercício de suas atividades, vier a, direta ou indiretamente, causar ou provocar à TJCE;

d) Obter todas as autorizações, aprovações e franquias necessárias à execução dos serviços, pagando os emolumentos prescritos por lei e observando as leis, regulamentos e posturas aplicáveis. É obrigatório o cumprimento de quaisquer formalidades e o pagamento, à sua custa, das multas porventura impostas pelas autoridades, mesmo daquelas que, por força dos dispositivos legais, sejam atribuídas à Administração Pública;

e) Não ceder ou transferir, total ou parcialmente, parte alguma do contrato. A fusão, cisão ou incorporação só será admitida com o consentimento prévio e por escrito do TJCE;

f) Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades objeto do Contrato, sem prévia autorização do TJCE;

g) Dar ciência, imediatamente e por escrito, de qualquer anormalidade que verificar na execução do objeto bem como prestar esclarecimentos que forem solicitados pelo TJCE;

h) Manter sigilo absoluto sobre informações, dados e documentos provenientes da execução do Contrato e também às demais informações internas do TJCE a que a Contratada tiver conhecimento;

i) Não deixar de executar qualquer atividade necessária ao perfeito fornecimento do objeto, sob qualquer alegação, mesmo sob pretexto de não ter sido executada anteriormente qualquer tipo de procedimento;

j) Somente desativar hardware, software e qualquer outro recurso computacional relacionado à execução do objeto mediante prévia autorização do TJCE;

k) Prestar qualquer tipo de informação solicitada pelo TJCE sobre os serviços contratados bem como fornecer qualquer documentação julgada necessária ao perfeito entendimento do objeto deste Contrato;

l) Elaborar e apresentar documentação técnica dos fornecimentos e serviços executados nas datas aprazadas, visando sua homologação pelo TJCE;

m) Alocar profissionais devidamente capacitados e habilitados para os serviços contratados;

n) Providenciar a substituição imediata dos profissionais alocados ao serviço que,

eventualmente, não atendam aos requisitos deste Contrato ou por solicitação do TJCE devidamente justificada;

o) Implementar rigorosa gerência de contrato com observância a todas as disposições constantes deste Contrato;

p) Em até 10 (dez) dias após a assinatura do contrato, a CONTRATADA disporá de profissionais com capacidade técnica suficiente e necessária ao desempenho dos serviços Objeto do Contrato, exigindo-se:

p.1) Todos os profissionais deverão possuir experiência mínima comprovada de 03 (três) anos na área de Segurança da Informação e terem participado de projetos similares;

p.2) A equipe de profissionais envolvida para exercer as funções, deve possuir as seguintes certificações ou equivalentes:

p.2.1) 01 (uma) Certificação CISSP (Certified Information Systems Security Professional);

p.2.2) 01 (uma) Certificação PMI-PMP Project Management Professional ou PMI-ACP - Profissional Certificado em Métodos Ágeis, práticas e ferramentas e técnicas através de metodologias ágeis.

p.2.3) 01 (uma) Certificação em alguma solução de mercado em Firewall/VPN;

p.2.4) 01 (uma) Certificação em alguma solução de mercado em IPS – Intrusion Prevent System;

p.2.5) 01 (uma) Certificação em alguma solução de mercado em SIEM – Security Information and Event Management;

p.2.6) 01 (uma) Certificação em alguma solução de mercado em Mail Security;

p.2.7) 01 (uma) Certificação em alguma solução de mercado em Web Security;

p.2.8) 01 (uma) Certificação em alguma solução de mercado em Endpoint Security;

p.3) A comprovação de que os profissionais compõem o quadro permanente da licitante se fará mediante a apresentação de cópia da Carteira de Trabalho (CTPS) ou do contrato social da licitante, no caso de sócio, ou contrato de prestação de serviços pelo prazo de vigência do contrato.

p.4) A comprovação de que os profissionais são detentores de experiência se dará com o fornecimento de Atestado(s) de Capacidade Técnica (fornecido(s) por pessoa jurídica de direito público ou privado, em documento timbrado) e a comprovação de que os profissionais são detentores de conhecimento com apresentação de documentos comprobatórios de diplomas e das certificações exigidas.

q) Da Visita Técnica ao ambiente da CONTRATADA:

q.1) Em até 15 (quinze) dias, após a assinatura do contrato, 02 (dois) representantes da equipe de servidores do TJCE realizarão vistoria técnica ao ambiente do SOC da CONTRATADA, de forma a averiguar o atendimento aos requisitos do ITEM 20.3 e seus subitens do termo – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014. Caso não esteja em conformidade a empresa terá o contrato rescindido.

q.2) Todos os custos da visita ao ambiente da CONTRATADA com passagens (FORTALEZA/DESTINO/FORTALEZA), estadia, translados e qualquer outro que seja necessário será da CONTRATADA, devendo ser considerado 02 (dois) participantes da CONTRATANTE para a realização da vistoria no ambiente.

r) De acordo com a resolução nº 7, de 18 de outubro de 2005, do CNJ, não contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao respectivo Tribunal (CONTRATANTE);

s) Manter as condições de habilitação e qualificação exigidas durante toda a vigência do Contrato.

Cláusula Quarta – Descrição da Solução

A solução ofertada deverá atender a descrição a seguir:

4.1 DESCRIÇÃO DETALHADA DOS SERVIÇOS DE ADMINISTRAÇÃO, GERENCIAMENTO E MONITORAMENTO DOS ATIVOS DE SEGURANÇA

4.1.1 A CONTRATADA deverá prestar serviço de Administração, Gerenciamento e Monitoramento para as soluções abaixo, no formato 24x7x365 dias:

4.1.1.1 Firewall/VPN – Matriz;

4.1.1.2 Firewall/VPN – Localidades Remotas;

4.1.1.3 IPS – Intrusion Prevent System;

4.1.1.4 SIEM – Security Information and Event Management;

4.1.2 A CONTRATADA deverá realizar configuração, ajustes, testes dos hardwares e softwares relacionados para as soluções descritas;

4.1.3 A instalação dos equipamentos do tipo concentrador para ativação da solução de monitoração devem ser realizadas nos Data Centers do CONTRATANTE, localizado em Fortaleza/CE;

4.1.4 Todas as atividades envolvidas serão acompanhadas e apoiadas por analistas e técnicos da CONTRATANTE;

4.1.5 A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades realizadas após o expediente (horários noturnos ou em finais de semana e feriados);

4.1.6 Todas as soluções deste lote devem ser revisadas na etapa de ativação das soluções (inicial) e revisões periódicas, validando regras/políticas das soluções, garantindo proteção da rede e usuários que trafegam na rede;

4.1.7 A CONTRATADA deverá instalar e incluir um link de dados dedicado a ser instalado no Data Center da CONTRATANTE (ponta A) tendo na outra extremidade o SOC da CONTRATADA (ponta B) com throughput suficiente para a realização dos serviços de gerenciamento, às custas da CONTRATADA,

4.1.8 A CONTRATADA deverá instalar e incluir uma Conexão VPN (Virtual private Network), compatível com a solução atualmente usada pelo Tribunal, usada como redundância da conexão dedicada, para caso haja indisponibilidade do link de dados.

4.1.9 O atendimento deverá ser realizado por central de serviços da própria CONTRATANTE e/ou telefone;

4.1.10 Não sendo possível registrar o atendimento/chamado na central de serviços da CONTRATANTE, a CONTRATADA deverá disponibilizar a sua própria central de serviços para realização dos serviços;

4.1.11 Os serviços deverão ser prestados remotamente, a partir de Centros de Atendimento próprios, localizados no Brasil, estritamente de acordo com as especificações deste documento;

4.1.12 Para suporte técnico remoto: suporte prestado por meio de Central de Atendimento 0800 ou equivalente à ligação local, web, e-mail e fax;

4.1.13 Esclarecimento de dúvidas relacionadas à prestação dos serviços, políticas e regras implementadas, funcionalidade da solução, deverão ser de atendimento imediato;

4.1.14 Suporte técnico local: atendimento in-loco, prestados por técnicos capacitados para a solução de problemas relacionados aos equipamentos e softwares. Este suporte poderá ser solicitado pela CONTRATANTE sempre que necessário;

4.1.15 Visitas técnicas, quando necessárias, estarão restritas às instalações da Secretaria de Tecnologia da Informação do TJCE;

4.1.16 Os recursos humanos envolvidos na implantação e prestação do serviço de suporte deverão estar capacitados na solução envolvida. Entende-se por capacitação: certificados profissionais emitidos pelos fabricantes das soluções que serão ofertadas;

4.1.17 O TJCE é responsável pelo envio dos equipamentos de sua propriedade para o fabricante em caso de manutenção;

4.1.18 Os chamados abertos somente poderão ser fechados após autorização de funcionário designado pelo TJCE.

4.1.19 O fechamento por parte da contratada que não tenha sido previamente autorizado pelo TJCE poderá ensejar aplicação de multa a CONTRATADA no valor conforme termo de contrato do valor mensal pelos serviços por ocorrência;

4.1.20 O TJCE informará as pessoas autorizadas a abrir e fechar chamados junto a CONTRATADA, bem como o meio pelo qual a autorização de fechamento será formalizada;

4.1.21 Os serviços contemplam os seguintes itens:

4.1.21.1 Regras das soluções (de acesso, NAT, alertas, etc.) – inclusão, exclusão e alteração;

4.1.21.2 Usuários – inclusão, exclusão e alteração

4.1.21.3 Configuração das soluções;

4.1.21.4 Mudança das soluções;

4.1.21.5 Logs (configurações, armazenamento, organização e recuperação);

4.1.21.6 Criação e manutenção de regras para os ativos de segurança do escopo;

4.1.21.7 Criação e manutenção de contas e grupos de VPN;

4.1.21.8 A correta alocação de recursos necessários para restaurar a operação com a maior

brevidade possível;

4.1.21.9 Elaboração de análise crítica para cada inclusão/exclusão/alteração de regras nos ativos de segurança do escopo, a fim de garantir a gestão de mudanças no ambiente da CONTRATANTE;

4.1.21.10 Análise de logs dos ativos de segurança do escopo, com geração mensal de relatórios operacionais e gerenciais para a CONTRATANTE, classificando todos os eventos por nível de criticidade com descrição detalhada dos eventos e recomendações de ações;

4.1.21.11 Atualização de patches e novas versões de firmware nos equipamentos;

4.1.21.12 Nos serviços de Firewall, a CONTRATADA deverá se responsabilizar pela gravação de dados para auditoria, de forma detalhada para cada conexão efetivada, incluindo a origem, serviço, hora de conexão, destino e ação executada;

4.1.21.13 Condução e resolução remota de incidentes e requisições de serviço relacionadas à segurança das informações do TJCE;

4.1.21.14 Aplicação das mais recentes versões, patches e hotfixes nos ativos;

4.1.21.15 Backup das soluções;

4.1.21.16 Realização de testes de segurança periódicos nos ativos (auditoria/análise de segurança);

4.1.21.17 Otimização periódica bimestral de regras, baseada na utilização de regras, protocolos, usuários, etc.);

4.1.21.18 Documentação das soluções;

4.2 DESCRIÇÃO DETALHADA DOS SERVIÇOS DE TRATAMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA

4.2.1 A CONTRATADA deverá prestar serviço de Tratamento de Resposta a Incidentes de Segurança para as soluções abaixo, no formato 24x7x365 dias:

4.2.1.1 Firewall/VPN;

4.2.1.2 IPS – Intrusion Prevent System;

4.2.1.3 SIEM – Security Information and Event Management;

4.2.1.4 Mail Security

4.2.1.5 Web Security

4.2.1.6 Endpoint Security

4.2.2 Se o TJCE ainda não possuir o seu modelo de Tratamento de Resposta a Incidentes de Segurança, a CONTRATADA deverá apresentar o seu modelo de identificação de ocorrências, registro, ações de medidas corretivas e atualização dos chamados para o acompanhamento e resolução de incidentes;

4.2.3 Durante a fase de ativação, deve ser definido em conjunto, pelo TJCE e pela CONTRATADA, o plano de tratamento de resposta a incidentes, que incluirá detalhes deste processo.

4.2.4 A CONTRATADA deve dispor de um modelo deste plano, que deverá ser discutido e aprovado pelo TJCE.

4.2.5 A CONTRATADA deve estabelecer com o TJCE um plano de comunicação entre a CONTRATADA e o TJCE, garantindo a oficialização dos meios de comunicação e a matriz de escalonamento;

4.2.6 Os serviços de tratamento de resposta a incidentes de segurança contemplam os seguintes itens:

4.2.6.1 Geração de eventos de segurança;

4.2.6.2 Coleta;

4.2.6.3 Armazenamento;

4.2.6.4 Análise;

4.2.6.5 Reação;

4.2.6.6 Detectar incidentes através das soluções de monitoramento do SOC, informativos, reclamações de órgãos oficiais externos, solicitação do TJCE;

4.2.6.7 Receber informações relativas a incidentes, criar registro, e encaminhar o incidente em questão para resolução;

4.2.6.8 Comunicar o status dos incidentes ao TJCE conforme se faça necessário;

4.2.6.9 Fornecer ao TJCE as atualizações regulares do status dos incidentes;

4.2.6.10 Abrir processo de gerência de mudança, com aprovação do TJCE, para solucionar um

incidente, caso necessário;

4.2.6.11 Encerrar o registro dos incidentes, de acordo com os procedimentos estabelecidos.

4.2.6.12 Monitoramento e análise remota das informações dos incidentes de segurança registrados, incluindo os itens afetados por eles;

4.2.6.13 Investigação e diagnóstico remoto de incidentes de segurança registrados, incluindo resolução dos mesmos, sempre que possível;

4.2.6.14 O envolvimento da equipe de TI da CONTRATANTE, bem como especialistas de 3º nível da CONTRATADA, no tratamento do incidente;

4.2.6.15 Monitoração em tempo real de eventos de risco (intrusão, disponibilidade, falhas de acesso importantes etc.), com processo previamente formalizado de resposta a incidentes originados da Internet;

4.2.6.16 Análise e Correlação dos Logs, através de SIEM (Security information and event management), utilizando a solução da CONTRATANTE;

4.2.6.17 Resposta aos alertas de segurança;

4.2.6.18 Categorizar os níveis de alertas;

4.3 DESCRIÇÃO DETALHADA DOS SERVIÇOS DE PORTAL DE ATENDIMENTO

4.3.1 A CONTRATADA deverá disponibilizar um portal de atendimento e abertura de chamados;

4.3.2 A CONTRATADA deve assegurar que os chamados, eventos e/ou incidentes de rede e/ou segurança sejam transferidos para outros técnicos ou grupos de solucionadores conforme suas especialidades, com acompanhamento total de passos, histórico de registros, datas, horários e consumo de tempo;

4.3.3 Deverá armazenar os relatórios periódicos, permitindo que o TJCE realize download dos seus relatórios mensais (mês corrente e anteriores);

4.3.4 A CONTRATADA deve fornecer uma visão que permite observar o gerenciamento da fila de atendimento, utilizada pelos analistas, onde é apresentada a ordem em que os chamados devem ser atendidos, bem como, possibilita contínuo monitoramento de tempo e volume por chamados em fila;

4.3.5 A CONTRATADA deve utilizar uma Interface Web, permitindo com que os seus técnicos possam executar funções de abrir, escalar, atualizar o andamento do chamado e encerrá-lo;

4.3.6 A solução da CONTRATADA deve ser integrada com a solução do TJCE, prevista para ser contratada durante o período do contrato.

4.3.7 A contratada deve garantir a integração entre os componentes, funcionalidades ou aplicações de diferentes fabricantes por meio de Web Services ou Linha de Comando ou e-mail.

4.4 DESCRIÇÃO DETALHADA DO NMS (ACORDO DE NÍVEL MÍNIMO DE SERVIÇO)

4.4.1 A CONTRATADA deverá disponibilizar as atualizações e patches de segurança de cada produto contratado durante 24 (vinte e quatro) horas por dia, 07 (sete) dias da semana.

4.4.2 A CONTRATADA deverá prover as atualizações de "releases" e de versões dos produtos licenciados durante a vigência do contrato, sendo que estas atualizações deverão passar também a estarem cobertas pelas garantias, níveis de serviços e demais termos deste serviço de manutenção.

4.4.3 A CONTRATADA deverá garantir os serviços de suporte a customização, parametrização e configuração voltadas à atualização e utilização de funcionalidades disponibilizadas nos produtos licenciados ou em versões superiores que sejam lançadas durante a vigência do contrato, para todos os produtos fornecidos e disponibilizados pelo TJCE no ambiente de produção. Este suporte, customização, parametrização e configuração deverão ser efetuadas no prazo máximo de 10 (dez) dias úteis, contados a partir da abertura do chamado;

4.4.4 A CONTRATADA deverá resolver os atendimentos, em pelo menos 90% (noventa por cento) das solicitações, nos seguintes prazos máximos:

4.4.4.1 Dúvidas ou alteração de configuração (P3): 30 minutos, contados a partir da abertura do chamado;

- Prioridade (P3) - Ocorrência de baixo impacto na utilização da Solução de Segurança para resolver problemas de funcionamento ou resposta a incidentes que não ocasionem paradas nas aplicações/ativos que deles fazem uso.

4.4.4.2 Serviço com performance inadequada (P2): 1:30 horas, contadas a partir da abertura do chamado;

- Prioridade (P2) - Ocorrência de médio impacto/Falha verificada em uma determinada funcionalidade da Solução de Segurança que impeça a obtenção do resultado esperado, mas a solução ou serviço permanecem funcionando para outras finalidades;

4.4.4.3 Serviço indisponível (P1): 2 horas, contadas a partir da abertura do chamado.

- Prioridade (P1) - Ocorrência de alto impacto/Falha verificada em um componente da Solução de Segurança que ocasione parada total ou parcial das atividades do ambiente da CONTRATANTE;

4.4.5 A CONTRATADA deverá garantir o atendimento e suporte para um número ilimitado de solicitações.

4.4.6 A CONTRATADA deverá garantir Suporte on-site no caso de impossibilidade de resolução do problema remotamente em horário comercial, exceto para solicitações (P1) que poderá ser na modalidade de 24 (vinte e quatro) horas, 7 (sete) dias da semana, apenas aos equipamentos concentradores, instalados no Datacenter do TJCE na cidade de Fortaleza/CE.

4.4.7 A CONTRATADA deverá garantir o serviço de suporte aos softwares contratados que deverá ser executado obrigatoriamente, por especialistas em resolução de problemas, na modalidade de atendimento 24 (vinte e quatro) horas, 7 (sete) dias da semana.

4.4.8 A CONTRATADA deverá trabalhar, ininterruptamente, na solução dos problemas críticos (P1) até que a solução contratada esteja novamente operando em regime normal de produção. Caso a solução do problema reportado exija a presença de técnicos(s) da CONTRATADA, mesmo fora do horário comercial, este(s) deverá (ão) ficar dedicado(s) a resolução do problema até que ele esteja resolvido.

4.4.9 Os indicadores de desempenho deverão ser monitorados e servirão de base para a avaliação mensal da CONTRATADA no "Relatório de Acompanhamento de Execução do Contrato", onde será possível verificar a efetividade do atendimento e permitir a depuração do processo.

4.4.10 Os NMS's devem ser considerados e entendidos pela CONTRATADA como um compromisso de qualidade que assumirá junto a CONTRATANTE.

4.4.11 A análise dos resultados destas avaliações pela CONTRATANTE resultará em advertências ou penalizações caso a CONTRATADA, não cumpra com os seus compromissos de qualidade e desempenho.

4.5 DESCRIÇÃO DETALHADA DOS RELATÓRIOS

4.5.1 Durante a Etapa de Ativação do Serviço, a CONTRATANTE e a CONTRATADA definirão os tipos de relatórios técnicos que deverão ser gerados e enviados mensalmente.

4.5.2 A CONTRATADA deverá emitir até o 10º (décimo) dia útil do mês subsequente ao período analisado os seguintes relatórios gerenciais:

4.5.2.1 Atendimentos realizados no período;

4.5.2.2 Percentual do NMS de atendimento consumido;

4.5.2.3 Percentual do NMS de solução consumido;

4.5.2.4 Gráfico e análise das maiores origens/destinos/portas de tráfego no período;

4.5.2.5 Gráfico e análise dos maiores acessos de usuários VPN no período;

4.5.2.6 Tabela e análise dos maiores eventos das soluções no período;

4.5.2.7 Informações sobre atualização dos equipamentos;

4.5.2.8 Informações sobre a disponibilidade dos ativos;

Cláusula Quinta – Da Prestação dos Serviços

Os serviços a serem executados obedecerão às seguintes condições e peculiaridades:

5.1 Do Local:

5.1.1 TJCE: na Av. General Afonso Albuquerque Lima, S/N. - Cambeba CEP: 60822-325, Fortaleza-CE, na Secretaria de Tecnológica da Informação – SETIN.

5.2 Forma de Fornecimento:

5.2.1 Todo o fornecimento deverá estar de acordo com os critérios estabelecidos nos itens do Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014;

5.2.2 A Contratada deverá implementar rigorosa gerência de projeto, com observância às regras a seguir além de adotar a Metodologia de Gerenciamento de Projetos – MGP da SETIN;

5.2.3 Para a inicialização do projeto, a empresa Contratada deverá executar:

5.2.3.1 Abertura do projeto: deverá ser elaborado e apresentado **Termo de Abertura do Projeto**;

5.2.3.2 Apresentação do escopo do serviço: deverá ser elaborado e apresentado **Declaração de Escopo do Projeto**;

5.2.3.3 Pré-planejamento do projeto: deverá ser elaborado e apresentado Plano de Gerenciamento do Projeto;

5.2.3.4 A Contratada deverá apresentar Cronograma de Execução, constando atividades, subatividades e marcos, contemplando todas as ações previstas para a execução dos serviços,

datas de entrega de documentação, datas das reuniões de ponto de controle, dentre qualquer outro evento que se julgar relevante e necessário;

5.2.3.5 A Contratada deverá agendar reunião ("kick-off meeting") junto aos responsáveis técnicos da Contratante, objetivando dar início ao acompanhamento da execução do Contrato;

5.2.3.6 Na reunião de "kick-off", a Contratada deverá apresentar sua equipe de trabalho, composta, no mínimo, por 01 (um) Gerente de Projeto e Equipe de Técnicos Especialistas;

5.2.3.7 Para apoio ao Gerente de Projeto, deverão ser alocados todos os técnicos necessários para a execução dos serviços;

5.2.3.8 Caberá ao Gerente de Projeto coordenar e orientar todo o processo de planejamento e execução dos serviços do Contrato, respeitando os prazos estabelecidos, atestando a qualidade dos serviços executados;

5.2.3.9 Deverá ser elaborada e apresentada Lista de Contatos do Projeto;

5.2.3.10 Definição das regras para execução do serviço;

5.2.3.11 Definição das responsabilidades de cada um dos envolvidos;

5.2.4 A contar da 1ª reunião do projeto, deverão ser executadas reuniões de controle do projeto ("Status do Projeto") entre as equipes técnicas envolvidas, onde o Gerente de Projeto posicionará os responsáveis do CONTRATANTE sobre o andamento do projeto e apresentando os documentos pertinentes;

5.2.5 As reuniões de status poderão ser realizadas semanalmente, quinzenalmente ou conforme a demanda, a critério da CONTRATANTE;

5.2.6 O Gerente será responsável pela elaboração e entrega de relatórios de progresso e ou situação do projeto ("Relatório de Acompanhamento"), onde deverão ser descritas as atividades pertinentes ao período, além de destacar as pendências e solicitações de mudança do projeto, dentre outros tópicos;

5.2.7 Os relatórios de progresso e ou situação do projeto deverão ser fornecidos por período, semanalmente, quinzenalmente ou conforme a demanda, a critério da CONTRATANTE;

5.2.8 Todas as reuniões do projeto deverão ser registradas em "Ata", a qual será de inteira responsabilidade do Gerente;

5.2.9 As atas deverão ser entregues em no máximo 48 (quarenta e oito) horas após a realização da reunião para verificação e revisão por parte do TJCE, para posterior emissão de aceite por ambas as partes;

5.2.10 Após a apresentação e aprovação dos documentos relacionados ao plano de projeto, a equipe do projeto dará início às demais Fases do cronograma;

5.2.11 Produtos da fase para entrega ao TJCE:

5.2.11.1 Documentação inicial do projeto, incluindo termo de abertura, declaração de escopo, plano de gerenciamento, cronograma de trabalho, matriz de responsabilidade e lista de contatos dos participantes;

5.2.11.2 Documentos de acompanhamento do projeto, incluindo relatórios de situação e atas de reunião;

5.2.11.3 Termo de Aceitação;

5.3 Oficialização da demanda dos serviços por meio da emissão de "Ordem de Serviço – OS":

5.3.1 A execução será sempre precedida da emissão pelo TJCE da competente "Ordem de Serviço – OS", contendo no mínimo: descrição do serviço, quantitativo, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço esperados;

5.3.2 A "Ordem de Serviço – OS" será emitida, assinada e autorizada pelo Fiscal do Contrato;

5.3.3 Toda "Ordem de Serviço – OS" deverá ser assinada pelo Gerente do Projeto / Preposto, representante da CONTRATADA perante o TJCE, declarando a concordância da CONTRATADA em executar as atividades descritas na "Ordem de Serviço – OS", de acordo com as especificações estabelecidas pelo TJCE;

5.3.4 Os serviços deverão estar sempre de acordo com as especificações constantes nas "Ordens de Serviços – OS";

5.3.5 O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução – quando a "Ordem de Serviço – OS" é emitida pelo TJCE, durante a execução – com o acompanhamento e supervisão de responsáveis do TJCE, e ao término da execução – com o fornecimento de "Relatório de Serviços" pela Contratada e atesto dos mesmos por responsáveis do TJCE;

5.3.6 Todos os serviços prestados pela Contratada deverão ser necessariamente documentados (passo-a-passo), registrados e entregues ao TJCE pela mesma, em cópias impressas e gravadas em

meio magnético, complementarmente ao “Relatório de Serviços”;

5.4 Do Recebimento

5.4.1 Todos os serviços terão suas métricas medidas a cada mês após a emissão da primeira orem de serviço – OS;

5.4.2 A CONTRATANTE atestará o recebimento dos mesmos, mensalmente, através da validação do Relatório de Níveis de Serviços.

5.4.3 Para aceite do recebimento e posterior encaminhamento ao pagamento, deverão ser apresentados os seguintes documentos:

5.4.3.1 Ordem de Serviços emitida e assinada, Relatório de Serviços e demais Documentos Técnicos pertinentes e comprobatórios de execução do serviço;

5.4.4 A frequência de aferição e avaliação dos níveis de serviços será mensal, devendo, a CONTRATADA, elaborar relatório gerencial de serviços, apresentando-o, à CONTRATANTE, até o 5º. (quinto) dia útil do mês subsequente ao da prestação dos serviços.

5.4.5 Devem constar desse relatório, dentre outras informações, os indicadores/metas de níveis de serviços definidos e alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual.

5.4.6 O conteúdo detalhado e a forma do relatório gerencial serão definidos pelas partes.

5.4.7 Independentemente da aceitação no recebimento, a Contratada deverá garantir a qualidade do serviço executado pelo prazo estabelecido nas especificações e nas condições constantes do Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014, obrigando-se a corrigir aquele que apresentar inconsistência no prazo estabelecido pelo TJCE.

5.4.8 Os Fiscais do Contrato verificarão a conformidade dos serviços e/ou da entrega e da documentação requerida e, no caso de estarem conformes, atestará a Nota Fiscal e encaminhará para pagamento. No caso de não estarem conformes, as devolverá, com as ressalvas devidas, no prazo de até 10 (dez) dias da apresentação, para a Contratada providenciar a sua conformidade e novo encaminhamento para o TJCE.

5.4.9 No caso dos serviços em não conformidade, a contagem dos prazos aqui estabelecidos será reiniciada a contar da data do saneamento das ressalvas pela CONTRATADA, devidamente certificadas pelo Fiscal do Contrato.

5.4.10 O TJCE rejeitará, no todo ou em parte, os serviços executados em desacordo com o disposto. Se, após o recebimento, constatar-se que os serviços foram executados em desacordo com o especificado, com defeito ou incompleto, os responsáveis do TJCE notificarão, por escrito, à CONTRATADA, interrompendo-se os prazos de recebimento e ficando suspenso o pagamento até que seja sanada a situação.

5.4.11 Os valores da(s) NF(s) / Fatura(s) deverão ser os mesmos consignados na Nota de Empenho, sem o que não será liberado o respectivo pagamento. Em caso de divergência, será estabelecido prazo para a Contratada fazer a substituição desta(s) NF(s) / Fatura(s).

5.4.12 São critérios de mensuração dos serviços prestados para controle dos pagamentos:

Item	Métrica	Indicador	Valor
Serviços técnicos	Unidade	Serviço Especificado na OS	100% executado

5.5 Os Serviços estarão passíveis de recusa quando:

5.5.1 Apresentarem especificações técnicas diferentes das estabelecidas no Termo – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014 e nos seus anexos;

5.5.2 Em casos de impactos insatisfatórios no ambiente. Os ajustes necessários no procedimento de execução dos serviços deverão ocorrer no prazo não superior a 48 (quarenta e oito) horas corridas contadas do momento da comunicação do ocorrido através de documento emitido pelos setores responsáveis pela contratação;

5.5.3 Os ajustes referentes aos serviços ora autorizados pelo TJCE e executados pela Contratada deverão ocorrer por conta da mesma sem gerar qualquer ônus ao Tribunal de Justiça do Estado do Ceará, sem isentar a CONTRATADA de qualquer sanção prevista neste documento.

5.6 Do Prazo

5.6.1 Os serviços deverão ser executados a partir de notificação para fornecimento dos serviços a ser emitida pelo TJCE posterior à assinatura do contrato;

5.6.2 Em até 10 (dez) dias corridos a partir da data de emissão da notificação para fornecimento dos serviços pelo TJCE, a empresa CONTRATADA deverá efetuar a inicialização do projeto;

5.6.3 Efetuada a inicialização do projeto, com o competente aceite de abertura do projeto, todos os

serviços contemplados pelo Objeto deverão estar disponíveis para demanda do TJCE via emissão de Ordem de Serviços – OS;

5.7 Tabela de Acordo de Níveis Mínimos de Serviços

Descrição	Definição	Cálculo	Aferição	Tempo de Atendimento	Glosa	Meta
DISPONIBILIDADE DA SOLUÇÃO DE GERNCIAMENTO e TRATAMENTO DE RESPOSTAS A INCIDENTES	É o tempo em que a solução de gerenciamento deverá estar operacional com todos as ferramentas disponíveis, inclusive link de dados, interface WEB, DASHBORD e central 0800	∑ Minutos Disponíveis ----------x100 ∑ Minutos Contratados	Verificado através dos tickets de indisponibilidade da solução de gerenciamento registrados na solução de service desk e disponibilizados na Solução;	NA	1% do valor da parcela mensal do serviço a cada ponto percentual abaixo de 99%	99%
Dúvidas ou alteração de configuração (P3);	É o tempo para registro e abertura de incidente no Service Desk da CONTRATANTE / CONTRATADA e identificar a causa raiz, tomando as medidas para a resolução do incidente (troubleshooting) em conformidade com os processos de incidente e mudança do CONTRATANTE e potencial de impacto na disponibilidade do serviço.	∑ Chamados Registrados dentro do tempo acordado ---------x100 ∑ Chamados Registrados	Verificado através dos tickets registrados na solução de Service Desk para cada solução;	90% dos atendimentos realizados em até 30 minutos	1% do valor da parcela mensal do serviço a cada ponto percentual abaixo de 90%	90%
Serviço com performance inadequada (P2);				90% dos atendimentos realizados em até 1 hora e 30 minutos		90%
Serviço indisponível (P1);				90% dos atendimentos realizados em até 2 horas		90%

Cláusula Sexta – Dos Preços e Condições de Pagamento

A CONTRATANTE pagará à CONTRATADA, pelos serviços prestados, o valor global de R$_____ (_____), referente aos serviços descritos no Anexo_____ deste Contrato.

Parágrafo Primeiro – Os faturamentos dos serviços, executados pela CONTRATADA, serão efetuados conforme abaixo;

a) A CONTRATANTE deverá emitir ordem de serviço para cada atividade a ser iniciada, conforme a quantidade das unidades discriminadas na Ordem de Serviço;

b) Os serviços poderão ser faturados após a solicitação de pagamento por parte da CONTRATADA e entrega/aceite do Relatório de Níveis de Serviços;

c) Quando houver divergência entre a solicitação de pagamento apresentada e a prestação dos serviços verificada pela CONTRATANTE, a parte incontrovérsia poderá ser faturada ficando a parte controversa para ser discutida e COMPENSADA na fatura posterior.

Parágrafo Segundo – As notas fiscais deverão ser emitidas em nome do Fundo de Especial de Reaparelhamento e Modernização do Judiciário – FERMOJU, CNPJ nº. 41.655.846/0001-47;

Parágrafo Terceiro – O pagamento será realizado através de depósito bancário nas agências do BANCO BRADESCO S/A, devendo as faturas ou notas fiscais, referentes à execução dos serviços previamente autorizadas, serem entregues até o dia 10 (dez) do mês subsequente à prestação dos mesmos, e estas deverão ser pagas, sem quaisquer acréscimos e atualização monetária, até o último dia útil do referido mês, devidamente atestado pelo(s) setor(es) competente(s) deste Tribunal de Justiça;

Parágrafo Quarto – O valor do pagamento será aquele apresentado na Nota Fiscal, conforme definido no contrato e devidamente atestado, descontadas as glosas, conforme definido neste Contrato;

Parágrafo Quinto – O Tribunal de Justiça reserva-se o direito de recusar o pagamento, no ato da ATESTAÇÃO, caso o objeto não esteja em conformidade com as condições deste instrumento;

Parágrafo Sexto – Nenhum pagamento será efetuado à empresa vencedora do certame antes de paga à multa que por ventura lhe tenha sido aplicada;

Parágrafo Sétimo – Nenhum pagamento será efetuado à CONTRATADA na pendência de qualquer uma das situações abaixo especificadas, sem que isso gere direito a alteração de preços ou compensação financeira: Apresentação da Certidão Negativa de Débito da Previdência Social – CND; Apresentação de Certidão Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida Ativa da União; Apresentação de Certidão Negativa de Débitos junto aos Governos Estadual e Municipal; Apresentação de Certificado de Regularidade do FGTS – CRF; Certidão Negativa de Débitos Trabalhistas.

Parágrafo Oitavo – Caso existam penalidades a serem aplicadas a CONTRATADA será notificada, conforme especificado no item **MECANISMOS FORMAIS DE COMUNICAÇÃO** do Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014, sendo o prazo do atesto da respectiva ORDEM DE SERVIÇO interrompido até a entrega das justificativas pela CONTRATADA;

Cláusula Sétima – Dos Reajustes e dos Recursos Orçamentários

Os preços oferecidos serão fixos e irreajustáveis pelo período mínimo de 01(um) ano.

Parágrafo Primeiro – Após 12 meses da data de apresentação da proposta e o contrato sendo prorrogado, a CONTRATADA, mediante justificativa, poderá solicitar reajuste com base na variação do IPCA.

Parágrafo Segundo – Ficará a critério do TJCE concordar ou não, integral ou parcialmente, com o reajuste de preços propostos.

Parágrafo Terceiro – As despesas decorrentes da execução deste Contrato correrão por conta do Fundo Especial de Reaparelhamento e Modernização do Judiciário – FERMOJU, tendo como Fonte dos Recursos – Recursos Diretamente Arrecadados, na seguinte dotação orçamentária:

04200001.02.061.500.21360.01.33903900.70.1.20

Cláusula Oitava – Da Vigência

O prazo de vigência deste contrato é de 12 (doze) meses contados a partir da sua assinatura, podendo ser prorrogado**,** tudo em conformidade com o disposto no Art. 57, inciso II, da Lei Federal n° 8.666/1993, por ser considerado pela CONTRATANTE, serviço de natureza contínua.

Cláusula Nona – Da Garantia Contratual

Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive pagamento de multas eventualmente aplicadas, a licitante prestará garantia no percentual de 5% (cinco por cento) do valor total do contrato, podendo a CONTRATADA optar por qualquer das modalidades previstas no art. 56 da Lei 8.666/93, a saber:

a) Caução em dinheiro ou títulos da dívida pública, cuja exigibilidade não seja contestada pelo TJCE;

b) Quando se tratar de caução em dinheiro, deverá ser recolhido na Secretaria de Finanças do TJCE;

c) Seguro garantia;

d) Fiança bancária.

Parágrafo Primeiro - Em se tratando de fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil;

Parágrafo Segundo - Se o valor da garantia for utilizado em pagamento de qualquer obrigação, a CONTRATADA deverá re-integralizar o seu valor, no prazo não superior a 10 (dez) dias corridos, contados da data em que for notificada;

Parágrafo Terceiro - A não apresentação da garantia até a assinatura contratual significará recusa à assinatura do contrato, ensejando aplicação das sanções previstas;

Parágrafo Quarto – No caso de rescisão do contrato, a garantia se presta a cobrir prejuízos comprovados;

Parágrafo Quinto - A garantia ofertada deverá cobrir multas aplicadas, bem como obrigações trabalhistas e previdenciárias, não deverá ser proporcional ao tempo de vigência do contrato, garantindo sua

totalidade durante todo o período de vigência. Não será aceita cláusula que preveja a realização do contrato por terceiros, bem como cláusula que preveja a subrogação da seguradora nos créditos da segurada. Deve, também, ser concedido pela seguradora, prazo mínimo de 30(trinta) dias para comunicação pelo TJCE das falhas cometidas pela segurada.

Cláusula Décima – Da Forma de Acompanhamento do Contrato

O acompanhamento e a fiscalização da execução do Contrato serão realizados por servidores do TJCE e designados como Fiscais do Contrato, os quais obedecerão às disposições de normas e resoluções internas do Tribunal, assim como o artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010.

Parágrafo Primeiro – Conforme alínea "a" do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, caberá à fiscalização providenciar elaboração do Plano de Inserção da contratada.

Parágrafo Segundo – Conforme alínea "b" do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, deverá ser realizada reunião inicial com participação dos Fiscais do Contrato, do Representante Legal da Contratada (apresentando o Preposto da mesma) e demais intervenientes identificados.

Parágrafo Terceiro – Conforme item 2 da alínea "b" do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, entrega, por parte da Contratada, a pauta da reunião mencionada acima contemplará a entrega do Termo de Compromisso e do Termo de Ciência.

Parágrafo Quarto – É importante informar que o Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014 é fruto da sequência de trabalhos da etapa de Planejamento da Contratação conforme a INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, a qual dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional.

Parágrafo Quinto – Conforme a instrução normativa acima, os documentos de planejamento (Análise de Viabilidade, Plano de Sustentação, Análise de Riscos e Estratégia de Contratação) foram devidamente elaborados e se encontram aprovados.

Cláusula Décima Primeira – Da Metodologia de Avaliação da Qualidade

Todo o trabalho realizado pela CONTRATADA estará sujeito à avaliação técnica, sendo homologado quando estiver de acordo com o padrão de qualidade exigido pelo Órgão e de acordo com os prazos definidos;

Parágrafo Único - A documentação técnica gerada deverá seguir o padrão definido pelo TJCE ou pelo CONTRATANTE, sendo devidamente verificada por responsável técnico e atestada pelo Fiscal do Contrato. O padrão de documentação técnica deverá ser informado na reunião inicial entre a CONTRATANTE e a CONTRATADA. A reunião inicial ocorrerá em até 07 (sete) dias corridos após o TJCE emitir a ordem de fornecimento.

Cláusula Décima Segunda – Das Sanções Administrativas

Pela inexecução total ou parcial do objeto definido neste Contrato, o TJCE poderá, garantida a prévia defesa, aplicar à Contratada, as sanções a seguir, de acordo com o grau do prejuízo causado pelo descumprimento das respectivas obrigações:

a) Advertência escrita quando se tratar de infração leve, a juízo da fiscalização, no caso de descumprimento das obrigações e responsabilidades assumidas no contrato ou ainda no caso de outras ocorrências que possam acarretar prejuízos ao TJCE desde que não caiba a aplicação de sanção mais grave;

b) 0,3% (três décimos por cento) por dia sobre o valor dos serviços entregues com atraso, até o percentual de 8% (oito por cento). Decorridos 30 (trinta) dias de atraso o TJCE poderá decidir pela rescisão, em razão da inexecução total;

c) 1% (um por cento) por dia sobre o valor da garantia contratual, pela não apresentação/atualização, até o percentual de 10% (dez por cento) no prazo estabelecido neste instrumento, da garantia de execução contratual;

d) 0,5% (meio por cento) por evento sobre o valor global atualizado do contrato, pela não manutenção das condições de habilitação e qualificação exigidas no instrumento convocatório;

e) 10 % (dez por cento) sobre o valor do contrato, nas hipóteses de rescisão contratual por inexecução total do contrato;

f) Suspensão temporária de participar em licitação e impedimento de contratar com a Administração, pelo prazo não superior a 5 (cinco) anos;

g) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos que determinaram sua punição ou até que seja promovida a sua reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

Parágrafo Único - As eventuais penalidades por descumprimento de Acordos de Níveis Mínimos de Serviços (NMS's) serão calculadas de acordo com o ITEM 5.7 - Tabela de Acordo de Níveis Mínimos de Serviços deste Contrato e abatidas na fatura do mês da prestação de serviços, conforme a validação do Relatório de Níveis de Serviços.

Cláusula Décima Terceira – Da Rescisão

Constituem motivo para rescisão contratual:

a) O não cumprimento de cláusulas contratuais, especificações ou prazos;

b) O cumprimento irregular de cláusulas contratuais, especificações e prazos;

c) A lentidão do seu cumprimento, levando o Tribunal a comprovar a impossibilidade da execução do serviço, nos prazos estipulados;

d) O atraso injustificado no início dos serviços;

e) A paralisação dos serviços, sem justa causa e prévia comunicação ao Tribunal;

f) Não será permitida a subcontratação total ou parcial de qualquer item, a associação da CONTRATADA com outrem, a cessão ou transferência total ou parcial das obrigações contraídas, bem como a fusão, cisão ou incorporação da CONTRATADA, que afetem a boa execução do Contrato, sem prévio conhecimento e expressa autorização do Tribunal;

g) O desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a execução do Contrato, assim como as de seus superiores;

h) O cometimento reiterado de faltas na execução do Contrato, anotadas pelo Tribunal;

i) A decretação de falência ou a instauração de insolvência civil da CONTRATADA;

j) A dissolução da CONTRATADA;

k) A alteração social ou a modificação da finalidade ou da estrutura da CONTRATADA que prejudique a execução do Contrato;

l) Razões de interesse público, justificadas e determinadas, de alta relevância e amplo conhecimento, pela máxima autoridade do Tribunal, e exaradas no Processo Administrativo a que se refere este Contrato;

m) A não liberação, por parte do Tribunal, de área ou local para execução dos serviços, nos prazos contratuais;

n) A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do Contrato;

o) O descumprimento do disposto no Inciso V, do Artigo 27, da Lei 8.666/93, sem prejuízo das sanções cabíveis;

p) A rescisão do Contrato poderá ser determinada por ato unilateral e escrita do TJCE;

q) Este Contrato poderá ser rescindido por acordo entre as partes, mediante aviso prévio e escrito, desde que haja conveniência para o Tribunal, conforme previsto no Artigo 79, Inciso II da Lei 8666/93.

r) Poderá o Tribunal rescindir imediatamente este Contrato, sem qualquer ônus, no caso de persistência no inadimplemento de obrigações pela CONTRATADA, e pelas quais já tenha a mesma, sido notificada para providenciar as devidas regularizações.

s) O Contrato poderá ser rescindido a qualquer tempo, sem ônus de qualquer espécie, a exclusivo critério do Tribunal, desde que devidamente notificado, devendo este notificar a CONTRATADA de sua intenção rescisória, com antecedência mínima de 30 (trinta) dias corridos.

Cláusula Décima Quarta – Da Propriedade, Sigilo e Restrições

A contratada cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do art. 111, da Lei Federal N.º 8.666/93, combinado com o art. 4.º, da Lei Federal N.º 9.609/98, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência dos serviços contratados, entendendo-se por resultados quaisquer estudos, relatórios, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presenta contratação, em papel ou em mídia eletrônica;

Parágrafo Primeiro – Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a CONTRATADA, zelar por si, por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e

comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados;

Parágrafo Segundo – A obrigação assumida de Confidencialidade permanecerá válida durante o período de vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA, previstas no CONTRATO e na legislação pertinente;

Parágrafo Terceiro - Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados, a qualquer título, da equipe executante do Objeto deste Contrato, a assinatura do ANEXO 09 - TERMO DE COMPROMISSO, bem como a assinatura do ANEXO 08 – TERMO DE CIÊNCIA do Edital de Pregão Eletrônico nº 03/2014 onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.

Cláusula Décima Quinta – Da Legislação

Este contrato rege-se pela Lei nº 10.520/2002 e Lei nº 8.666/93, alterada pelas Leis nº 9.648/1998, nº 9.854/1999, legislação correlata, medidas provisórias, bem como pelos preceitos de Direito Público, regulamentos, instruções normativas e ordens de fornecimento, emanados de órgãos públicos, aplicando-se-lhes, supletivamente, nos casos omissos, os princípios gerais dos contratos e demais disposições de Direito Privado.

Cláusula Décima Sexta – Do Foro

Fica eleito o foro de Fortaleza (CE) para dirimir quaisquer dúvidas oriundas do presente Contrato, caso não possam ser resolvidas por via administrativa, com renúncia de qualquer outro por mais privilegiado que seja.

E, por estarem justos e acertados, firmam o presente em 02(duas) vias de igual teor e forma, nas presenças da(s) testemunha(s) que também o assinam, para que produza seus jurídicos e legais efeitos, devendo seu extrato ser publicado no Diário da Justiça.

Fortaleza, xx de xxxxxxxx de 2014.

_____

CONTRATANTE

_____

CONTRATANTE

_____

EMPRESA – CONTRATADA (ASSINATURA/CARIMBO)

Testemunhas: _____

_____

ANEXO 16

MINUTA DO CONTRATO (LOTE 2)

CONTRATO PARA EXECUÇÃO DOS SERVIÇOS ESPECIALIZADOS, SOB DEMANDA, DE ESTRUTURAÇÃO DA SEGURANÇA DA INFORMAÇÃO DO TJCE, COM FORNECIMENTO DE SOFTWARE GRC, QUE ENTRE SI CELEBRAM O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ E A EMPRESA _____ (Processo Administrativo nº _____).

CT Nº /2014

O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, situado no Centro Administrativo Governador Virgílio Távora, Distrito de São José do Cambeba em Fortaleza – Ce, inscrito no CGC sob o número 09.444.530/0001-01, doravante denominado simplesmente de TJCE ou CONTRATANTE, neste ato representado pro seu Presidente, Des. _____ e por sua Secretária Geral, Dra. _____, e seu Secretário de Tecnologia da Informação,_____e a empresa_____, representada neste ato por_____ _____, portador da carteira de identidade n.º _____/___, CPF n.º _____, com endereço na _____, inscrita no CNPJ sob o número _____, daqui por diante simplesmente denominada CONTRATADA, pactuam o presente Contrato, que se regerá pela Lei Federal nº 10.520/02, pela Lei Federal n.º 8.666/93, com suas alterações e atualizações posteriores.

Cláusula Primeira – Da Fundamentação Legal

Fundamenta-se o presente Instrumento na proposta apresentada pela CONTRATADA e no resultado da Licitação realizada sob a modalidade Pregão Eletrônico n.° 03/2014, devidamente homologada pelo Exmo. Desembargador Presidente do Tribunal de Justiça do Estado do Ceará, tudo de conformidade com as disposições da Lei Federal nº 10.520/02 e da Lei Federal nº 8.666, com suas alterações e atualizações posteriores, e o processo administrativo nº _____.

Cláusula Segunda – Do Objeto

O Objeto deste Instrumento consiste na contratação dos ***serviços especializados, por demanda de Estruturação da segurança da informação do TJCE, com o fornecimento de software de GRC – Governança, Riscos e Compliance, para automatizar a Gestão de Segurança da Informação, incluindo levantamentos, inventários, diagnósticos, análises, avaliações, testes, e tratamento dos ativos, com a gestão da continuidade dos negócios e elaboração dos planos de contingência, com divulgação, planejamento, treinamento, elaboração e revisão dos normativos para sua implementação, para atender as necessidades do Poder Judiciário do Estado do Ceará (Lote II)***, conforme especificações contidas no Edital do Pregão Eletrônico nº 03/2014 e seus anexos, bem nos Anexos_____ deste Contrato, todos partes integrantes do mesmo.

Parágrafo Único – A prestação dos serviços obedecerá ao estipulado neste Contrato, bem como às disposições assumidas na proposta firmada pela CONTRATADA, dirigida ao CONTRATANTE, independentemente da transcrição, a qual faz parte integrante e complementar deste Contrato, no que não o contrarie.

Cláusula Terceira – Das Obrigações das partes

São obrigações das partes no respectivo contrato:

I - DO CONTRATANTE:

a) Proporcionar todas as facilidades para a Contratada executar o fornecimento do objeto do presente Contrato, permitindo o acesso dos profissionais da Contratada às suas dependências. Esses profissionais ficarão sujeitos a todas as normas internas do TJCE, principalmente as de segurança, inclusive àquelas referentes à identificação, trajes, trânsito e permanência em suas dependências;

b) Promover o acompanhamento e a fiscalização da execução do objeto do presente Contrato, sob o aspecto quantitativo e qualitativo, anotando em registro próprio as falhas detectadas;

c) Comunicar prontamente à CONTRATADA qualquer anormalidade na execução do objeto, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014;

d) Fornecer à Contratada todo tipo de informação interna essencial à realização dos fornecimentos e dos serviços;

e) Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando esta estiver em conformidade com os padrões de informação e qualidade exigidos;

f) Homologar os serviços prestados, quando estes estiverem de acordo com o especificado no Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014;

g) Efetuar o pagamento à CONTRATADA;

II - DA CONTRATADA:

a) Atender a todas as condições descritas no Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014 e respectivo Contrato;

b) Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, contribuições previdenciárias, impostos e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que estes não têm nenhum vínculo empregatício com o TJCE;

c) Responsabilizar-se pelo fornecimento do objeto deste Contrato, respondendo civil e criminalmente por todos os danos, perdas e prejuízos que, por dolo ou culpa sua, de seus empregados, prepostos, ou terceiros no exercício de suas atividades, vier a, direta ou indiretamente, causar ou provocar à TJCE;

d) Obter todas as autorizações, aprovações e franquias necessárias à execução dos fornecimentos e dos serviços, pagando os emolumentos prescritos por lei e observando as leis, regulamentos e posturas aplicáveis. É obrigatório o cumprimento de quaisquer formalidades e o pagamento, à sua custa, das multas porventura impostas pelas autoridades, mesmo daquelas que, por força dos dispositivos legais, sejam atribuídas à Administração Pública;

e) Não ceder ou transferir, total ou parcialmente, parte alguma do contrato. A fusão, cisão ou incorporação só será admitida com o consentimento prévio e por escrito do TJCE;

f) Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades objeto do Contrato, sem prévia autorização do TJCE;

g) Dar ciência, imediatamente e por escrito, de qualquer anormalidade que verificar na execução do objeto bem como prestar esclarecimentos que forem solicitados pelo TJCE;

h) Manter sigilo absoluto sobre informações, dados e documentos provenientes da execução do Contrato e também às demais informações internas do TJCE a que a Contratada tiver conhecimento;

i) Não deixar de executar qualquer atividade necessária ao perfeito fornecimento do objeto, sob qualquer alegação, mesmo sob pretexto de não ter sido executada anteriormente qualquer tipo de procedimento;

j) Somente desativar hardware, software e qualquer outro recurso computacional relacionado à execução do objeto mediante prévia autorização do TJCE;

k) Prestar qualquer tipo de informação solicitada pelo TJCE sobre os fornecimentos e sobre os serviços contratados bem como fornecer qualquer documentação julgada necessária ao perfeito entendimento do objeto deste Contrato;

l) Elaborar e apresentar documentação técnica dos fornecimentos e serviços executados nas datas aprazadas, visando sua homologação pelo TJCE;

m) Alocar profissionais devidamente capacitados e habilitados para os serviços contratados;

n) Providenciar a substituição imediata dos profissionais alocados ao serviço que,

eventualmente, não atendam aos requisitos deste Contrato ou por solicitação do TJCE devidamente justificada;

o) Implementar rigorosa gerência de contrato com observância a todas as disposições constantes deste Contrato;

p) Em até 10 (dez) dias após a assinatura do contrato, a CONTRATADA disporá de profissionais com capacidade técnica suficiente e necessária ao desempenho dos serviços Objeto do Contrato, exigindo-se:

p.1) Todos os profissionais deverão possuir experiência mínima comprovada de 03 (três) anos na área de Segurança da Informação e terem participado de projetos similares;

p.2) A equipe de profissionais envolvida para exercer as funções, deve possuir as seguintes certificações ou equivalentes:

p.2.1) 01 (uma) Certificação Auditor Líder ISO 27001;

p.2.2) 01 (uma) Certificação Auditor Líder ISO 22301;

p.2.3) 01 (uma) Certificação GCIA - GIAC Certified Intrusion Analyst;

p.2.4) 01 (uma) Certificação CBCP – Certified Business Continuity Professional;

p.2.5) 01 (uma) Certificação CISSP (Certified Information Systems Security Professional);

p.2.6) 01 (uma) Certificação CGEIT - Certified Governance Enterprise IT (ISACA),

p.2.7) 01 (uma) Certificação CISA - Certified Information Systems Auditor;

p.2.8) 01 (uma) Certificação CISM - Certified Information Security Manager;

p.2.9) 01 (uma) Certificação CRISC - Certified em Risk Control;
p.2.10) 01 (uma) Certificação ITIL Expert – Information Technology Infrastructure Library;

p.2.11) 01 (uma) Certificação PMI-PMP Project Management Professional ou 01 (uma) Certificação PMI-ACP Profissional Certificado em Métodos Ágeis, práticas e ferramentas e técnicas através de metodologias ágeis.

p.3) A comprovação de que os profissionais compõem o quadro permanente da licitante se fará mediante a apresentação de cópia da Carteira de Trabalho (CTPS) ou do contrato social da licitante, no caso de sócio, ou contrato de prestação de serviços pelo prazo de vigência do contrato.

p.4) A comprovação de que os profissionais são detentores de experiência se dará com o fornecimento de Atestado(s) de Capacidade Técnica (fornecido(s) por pessoa jurídica de direito público ou privado, em documento timbrado) e a comprovação de que os profissionais são detentores de conhecimento com apresentação de documentos comprobatórios de diplomas e das certificações exigidas.

q) De acordo com a resolução nº 7, de 18 de outubro de 2005, do CNJ, não contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao respectivo Tribunal (CONTRATANTE);

r) Manter as condições de habilitação e qualificação exigidas durante toda a vigência do Contrato.

Cláusula Quarta – Descrição da Solução

A solução ofertada deverá atender a descrição a seguir:

4.1 FORNECIMENTO E IMPLANTAÇÃO DE SOFTWARE de GRC – GOVERNANÇA, RISCOS E COMPLIANCE PARA AUTOMATIZAR A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

4.1.1 Implementar ferramentas para automatizar a gestão da segurança da informação, integrando as ações, permitindo o inventário dos processos, indicadores, documentos das normas, processos, políticas, análises, avaliação e tratamento de riscos, geração de recomendações e planos de ação e acompanhamento através de workflow para gestão de incidentes, tratamento das não conformidades e gestão de alertas.

4.1.2 Os softwares deverão ter interfaces e manuais no idioma Português (Brasil), permitindo a customização dos relatórios.

4.1.2.1 O software deverá ser instalado no ambiente a ser disponibilizado pelo TJCE.

4.1.2.2 Deverão ser entregues como produtos da instalação os seguintes itens:

4.1.2.2.1 Relatório de instalação do Software.

4.1.2.2.2 Documento que comprove a licença de uso do software.

4.1.2.2.3 CD de instalação do software.

4.1.2.2.4 Manual do Software em Português (Brasil).

4.1.3 BENEFÍCIOS:

4.1.3.1 Conduzir de forma otimizada projetos de análise de Gaps em Governança, Riscos e Compliance.

4.1.3.2 Criar Risk Scorecard, fornecendo visão executiva dos Riscos, incluindo índices e métricas que facilitam estabelecer critérios e apoiar a tomada de decisões.

4.1.3.3 Obter resultados precisos no processo de conformidade com normas e regulamentações internacionais e de mercado.

4.1.3.4 Consolidar os Riscos permitindo priorizar investimentos conforme a importância de cada ativo para a organização Acompanhar a evolução dos Riscos.

4.1.3.5 Gerenciar de forma centralizada Riscos e Compliance, incluindo a evolução histórica.

4.1.3.6 Realizar auditorias mais eficientes e com menores custos.

4.1.3.7 Gerenciar os requisitos de segurança em múltiplas auditorias, eliminando custos redundantes e controles desnecessários.

4.1.3.8 Apoiar a implementação dos requisitos de Certificação para SOx, PCI DSS, ISO 27002, ISO 27001, BS 25999, CobiT, Basiléia II, BITS/FISAP e outros.

4.1.3.9 Apoiar a gestão de Planos de Continuidade facilitando a manutenção e recuperação rápida das informações e procedimentos, alinhada à norma ABNT NBR ISO 22301:2013.

4.1.3.10 Facilitar a Gestão de Eventos e Incidentes.

4.1.4 REQUISITOS DO SOFTWARE

4.1.4.1 Os requisitos do software serão avaliados conforme a sua capacidade de atender aos quesitos da estrutura de implementação dos processos automatizados de Segurança da Informação.

4.1.4.2 Deve ser baseado em padrões e normas internacionais, como: ABNT ISO 27000, ABNT ISO/IEC Guia 73:2005, ABNT ISO 27005, ABNT 15999, NBR ISO 31000:2009 e ABNT NBR ISO 22301:2013.

4.1.4.3 Deve possuir recurso de auditoria das atividades realizadas e permitir a proteção de dados com criptografia.

4.1.4.4 Deve ser totalmente web não requerendo instalações de agentes ou clientes nas estações de trabalho.

4.1.4.5 Todas as mensagens devem ser no idioma Português (Brasil).

4.1.4.6 Deve possuir suporte web integrado ao software em idioma Português (Brasil).

4.1.4.7 Deve possuir área dedicada ao usuário, onde sejam possíveis:

4.1.4.7.1 Consultar pendências.

4.1.4.7.2 Receber corporativas administradas pelos gestores.

4.1.4.7.3 Visualizar perfis e acessos aos sistemas.

4.1.4.8 Deve inventariar os processos de SI, os indicadores recomendados de SI, os documentos das normas processos e políticas de SI e os ativos críticos de TI e de SI.

4.1.4.9 Deve realizar a gestão de ativos considerando: pessoas, equipamentos, edificações, processos de negócio e ativos definidos pelos usuários. Deve permitir a criação de atributos conforme os tipos de ativos.

4.1.4.10 Deve possuir definição de política de senha como: tamanho, tipo de caracteres que deverão ser utilizados, validade, tempo para time-out e número de tentativas inválidas para que o usuário seja bloqueado.

4.1.4.11 Deve possuir mecanismos de concessão de permissões na solução com base nos perfis e papéis exercidos pelos usuários.

4.1.4.12 Deve possuir perfis de acesso por usuários com funções de gestão, administrativas e operacionais.

4.1.4.13 Deve ter a capacidade para realização do gerenciamento dos elementos da organização, considerando:

4.1.4.13.1 Visualizar, inserir, editar e excluir elementos do inventário e seus atributos.

4.1.4.13.2 Visualizar com estruturação em árvore e os ativos cadastrados.

4.1.4.13.3 Possuir consultas para todas as informações registradas no inventário.

4.1.4.13.4 Integrar os ativos com os processos de negócios a eles vinculados.

4.1.4.14 Deve permitir a gestão dos ativos cadastrados, sendo capaz de:

4.1.4.14.1 Incluir, editar ou deletar as áreas físicas da organização ou lógicas, processos, grupos de sistemas, dentre outras visões que permitam a organização dos componentes de informação.

4.1.4.15 Definir os responsáveis, por cada área da estrutura funcional, obtendo ainda, o cadastro do e-mail, telefone, função, dentre os outros aspectos relevantes.

4.1.4.16 Definir os responsáveis por área da estrutura funcional, com a finalidade de perfil de acesso.

4.1.4.17 Incluir os componentes de informação tecnológicos, humanos, processuais e ambientais em cada área da estrutura funcional.

4.1.4.18 Definir os valores de grau de importância em cada item inventariado.

4.1.4.19 Deve gerar informações consolidadas sobre análise de riscos e conformidade originadas das análises, fiscalizações, inspeções e auditorias.

4.1.4.20 Possuir base de conhecimento que permite realizar análise de riscos nos ativos de tecnologia da informação possuindo as bases de conhecimento devendo conter no mínimo 30 controles relacionados para cada um dos itens relacionais a seguir.

4.1.4.20.1 Ativos envolvidos: processos, pessoas, tecnologias e ambientes.

4.1.4.21 Deve permitir o monitoramento das respostas às análises de forma consolidada, possuindo:

4.1.4.21.1 A situação das respostas aos itens inventariados.

4.1.4.21.2 Situação dos dados dessas análises (índice de respostas, indicadores e controle).

4.1.4.22 Deve permitir a automatização da análise de controles do TJ-CE através da criação de questionários que sejam aplicados pela estrutura de controle ou encaminhada manualmente por email para as áreas.

4.1.4.23 Deve permitir atribuição de responsabilidades sobre análises efetuadas.

4.1.4.24 Deve permitir a visualização dos percentuais de completude da gestão de riscos.

4.1.4.25 Deve permitir a visualização gráfica do “status” da gestão de riscos.

4.1.4.26 Deve permitir a criação de filtros dinâmicos aos itens da gestão de riscos.

4.1.4.27 Deve permitir avaliação das não conformidades identificadas nas análises, decidindo se deverão ser encaminhados para tratamento.

4.1.4.28 Deve permitir que os itens em tratamento possam ser analisados por meio de gráficos e informações estatísticas.

4.1.4.29 Deve permitir o acompanhamento do tratamento dos itens e sua avaliação perante a simulação de tratamento.

4.1.4.30 Deve permitir a inserção de modelos de análises (normas, legislação, políticas, instruções) e sua associação aos itens criados nas bases de conhecimento.

4.1.4.31 Deve possuir bases de conhecimento de melhores práticas de análise de segurança física em datacenter e edificações que guardem ativos de tecnologia da informação.

4.1.4.32 Deve possuir bases de conhecimento com a análise de riscos das aplicações baseada na norma ISO 15403.

4.1.4.33 Deve permitir a análise integrada à avaliação de riscos em TI.

4.1.4.34 Deve permitir cadastrar os processos críticos.

4.1.4.35 Deve implementar o método de cálculo do BIA.

4.1.4.36 Deve possuir questionários automatizados ou manuais para que os usuários pesquisem a relevância.

4.1.4.37 Deve emitir o relatório de BIA (Análise de Impacto no Negócio).

4.1.4.38 Deve possuir recursos de armazenar as referências a informações consideradas críticas e vinculá-los a ativos.

4.1.4.39 Deve permitir que estes ativos sejam classificados conforme a política de classificação de informação.

4.1.4.40 Deve emitir relatórios e permitir consultas para que os usuários conheçam a classificação de cada informação.

4.1.4.41 Deve permitir a implementação dos recursos exigidos pela legislação de acesso a informação que a TJ-CE deva atender.

4.1.4.42 Deve cadastrar os processos críticos definidos pela atividade de BIA.

4.1.4.43 Deve possuir recursos de gestão e aprovação de documentos por diferentes colaboradores através de workflow.

4.1.4.44 Deve permitir o armazenamento e consulta dos planos de continuidade de negócios, vinculando-os a ativos e processos.

4.1.4.45 Deve controlar a versão dos planos gerados.

4.1.4.46 Deve permitir a simulação dos planos a partir de testes de mesa automatizados em workflow.

4.1.4.47 Deve atender as exigências da norma ABNT 15999.

4.1.4.48 Deve realizar a gestão de incidentes através de workflow.

4.1.4.49 Deve armazenar os documentos de políticas e permitir consultas conforme o perfil dos usuários.

4.1.4.50 Deve permitir o armazenamento de conhecimento, procedimentos e práticas de testes de invasão do ambiente do TJ-CE.

4.1.4.51 Deve possuir recursos de workflow para encaminhamento e monitoramento da implementação das recomendações.

4.1.4.52 Implementar Workflow de Gestão de Incidentes.

4.1.4.53 Deve permitir o cadastro de ações com no mínimo os seguintes itens:

4.1.4.53.1 Descritivo da ação.

4.1.4.53.2 Resumo (Título).

4.1.4.53.3 Grau de urgência no tratamento da ação.

4.1.4.53.4 Grau de severidade para o processo.

4.1.4.53.5 Atribuição do responsável a ação.

4.1.4.54 Deve possuir controle de acesso para usuários e perfis.

4.1.4.55 Deve possuir a possibilidade de mensuração da ação conforme critérios do TJ-CE.

4.1.4.56 Definição de prazo de conclusão da ação.

4.1.4.57 Deve permitir o acompanhamento das ações, com os seguintes atributos:

4.1.4.57.1 Permitir incluir novas ações.

4.1.4.57.2 Possibilidade de fechar a ação.

4.1.4.57.3 Possibilidade de anexar arquivos como evidência.

4.1.4.58 Deve permitir filtros dinâmicos nas ações;

4.1.4.59 Deve permitir a geração dos seguintes relatórios das ações:

4.1.4.59.1 Por status da ação (aberta, fechada, etc.).

4.1.4.59.2 Por data (Dia de abertura, fechamento, atualização).

4.1.4.59.3 Pelo grau de urgência.

4.1.4.59.4 Por áreas associadas aos eventos.

4.1.4.59.5 Visualização rápida das ações mais urgentes.

4.1.4.60 Implementar workflow para tratamento das não conformidades.

4.1.4.61 Deve ser integrado à avaliação de riscos em TI.

4.1.4.62 Implementar Gestão de Alertas

4.1.4.63 Deve emitir alertas e trocar atributos conforme condições específicas.

4.1.4.64 Deve permitir a pontuação dos alertas.

4.1.4.65 Gerar Relatórios, Gerir Métricas, Praticar Melhoria Contínua.

4.1.4.66 Deve permitir a geração de relatórios, tabelas, gráficos, mapas e estatísticas dos inventários, análise e workflow.

4.1.4.67 Deve permitir a geração de relatórios e exportações nos formatos (xls, rtf, pdf) sem a necessidade de instalação de pacotes escritórios nas estações de trabalho.

4.1.4.68 Deve permitir a geração de relatório de nível estratégico contendo informações de toda a organização, de ameaças possíveis, risco para as macrodimensões, dimensões e os itens de inventário que os suportam, além de orientações para a gestão de riscos em tecnologia da informação.

4.1.4.69 Deve permitir a geração de relatório com a representação gráfica da interdependência de item do inventário com uma dimensão e sua macrodimensão, projetos, bem como os riscos encontrados no momento de fiscalização, inspeção e auditoria.

4.1.4.70 Deve permitir a geração de relatório de nível tático contendo informações gerais sobre as fiscalizações, inspeções e auditorias, mostrando os itens do inventário que foram analisados, bem

como seus níveis de risco e possíveis estratégias de tratamento.

4.1.4.71 Deve permitir a geração de relatório de nível operacional visualizando os comentários realizados nas fiscalizações, inspeções e auditorias cada item do inventário, as boas práticas existentes, bem como os riscos encontrados.

4.1.4.72 Deve permitir a filtragem para todos os relatórios possibilitando que apenas parte da fiscalização, inspeção e auditoria seja avaliada.

4.1.4.73 Deve permitir a criação de gráficos a partir das análises realizadas.

4.1.4.74 Deve possibilitar filtros gráficos criados a partir de:

4.1.4.74.1 Risco encontrado.

4.1.4.74.2 Ativos.

4.1.4.74.3 Índice de conformidade.

4.1.4.74.4 Quantidade de elementos cadastrados no sistema.

4.1.4.74.5 Quantidade de questionamentos conformes.

4.1.4.74.6 Quantidade de questionamentos inconformidades.

4.1.4.75 Deve permitir agrupamentos dos gráficos em:

4.1.4.75.1 Ameaças aos elementos cadastrados.

4.1.4.75.2 Bases de conhecimentos geradas.

4.1.4.75.3 Elementos avaliados nas análises.

4.1.4.75.4 Responsável pelos elementos cadastrados.

4.1.4.76 Deve permitir a visualização em tipos distintos de gráficos, dentre eles:

4.1.4.76.1 Radar.

4.1.4.76.2 Pizza.

4.1.4.76.3 Barras.

4.1.4.76.4 Linhas.

4.1.4.77 Deve possibilitar a visualização gráfica do histórico das análises por:

4.1.4.77.1 Determinada época.

4.1.4.77.2 Série Histórica.

4.1.4.78 Deve permitir a inserção de filtros baseadas em:

4.1.4.78.1 Escolha por elementos cadastrados.

4.1.4.78.2 Responsável pelos elementos cadastrados.

4.1.4.78.3 Agrupamentos criados dentro das bases de conhecimento.

4.1.4.78.4 Nível do risco identificado.

4.1.4.78.5 Fontes potenciais de danos.

4.1.4.78.6 Causador da fonte potencial de dano.

4.1.4.79 Deve permitir o agrupamento dos gráficos criados em painéis de controles pré-selecionados.

4.1.4.80 Deve aumentar e/ou diminuir o nível de detalhamento dos gráficos, imergindo em um de seus componentes formadores.

4.1.4.81 Deve permitir a mudança do tipo de gráfico mesmo após sua definição inicial.

4.1.4.82 Deve mostrar legendas dos gráficos.

4.1.5 PRODUTOS ESPERADOS:

4.1.5.1 Software de gestão de segurança da informação instalado e em operação.

4.1.5.2 Serviço de suporte, manutenção e atualização de software durante todo o período de vigência do contrato.

4.1.6 PRAZO DE ENTREGA:

4.1.6.1 O fornecimento deverá ser executado em até 15 (quinze) dias corridos contados a partir da emissão de Ordem de Fornecimento – OF;

4.2 DESCRIÇÃO DETALHADA PARA ELABORAÇÃO DAS METODOLOGIAS DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO:

4.2.1 Elaborar e desenvolver metodologia de gestão de riscos em Segurança da Informação para o TJCE com base na análise, levantamento, mapeamento, consolidação e documentação de situações, ambientes, pessoas e processos que apresentem riscos relativos ao manuseio e circulação da informação institucional. No desenvolvimento e na consolidação da metodologia de gestão de riscos

em questão deverá ser levando em consideração, no que couber, os seguintes normativos:

4.2.1.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.

4.2.1.2 NORMATIVOS ABNT: ABNT NBR ISO Guia 73:2005; ABNT NBR ISO/IEC 27005:2008; ABNT NBR ISO/IEC 27001:2006; ABNT NBR ISO/IEC 27002:2005 e ISO 31000;

4.2.1.3 Caso haja mudança dos normativos relacionados acima, estas deverão ser, necessariamente, observadas e aplicadas durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas demandas normativas apresentadas;

4.2.1.4 Caso os normativos acima sejam, em sua totalidade ou em parte, substituídos, os novos normativos deverão ser, necessariamente, observados e aplicados;

4.2.1.5 Durante a execução dos serviços, deverão ser observadas pela Contratada tantas mudanças quanto forem necessárias para adequar o TJCE aos novos normativos em vigência;

4.2.2 Deverão ser observados os seguintes aspectos na elaboração das metodologias:

4.2.2.1 Comunicação e consulta - Comunicar e consultar as partes envolvidas internas e externas, conforme apropriado, em cada etapa do processo de gestão de riscos e em relação ao processo como um todo.

4.2.2.2 Estabelecimento dos contextos - Estabelecer os contextos: externo, interno e da gestão de riscos nos quais se desenvolverá o restante do processo. Devem ser estabelecidos os critérios em relação aos quais os riscos serão avaliados e deverá ser definida a estrutura de análise.

4.2.2.3 Identificação de riscos - Identificar onde, quando, por que e como os eventos podem impedir, atrapalhar, atrasar ou melhorar a consecução dos objetivos.

4.2.2.4 Análise de riscos - Identificar e avaliar os controles existentes. Determinar as consequências e a probabilidade e, por conseguinte, o nível de risco. Tal análise deve considerar as diversas consequências potenciais e como elas podem ocorrer.

4.2.2.5 Avaliação de riscos - Comparar os níveis de risco estimados com os critérios estabelecidos previamente e considerar o balanço entre os benefícios potenciais e os resultados adversos. Isso possibilita que sejam tomadas decisões quanto à extensão, natureza dos tratamentos necessários e prioridades.

4.2.2.6 Tratamento de riscos - Desenvolver e implementar estratégias e planos de ação específicos e econômicos, para aumentar os benefícios potenciais e reduzir os custos potenciais.

4.2.2.7 Monitoramento e análise crítica – Deverá ser monitorada e demonstrada a real eficácia de todas as etapas do processo de gestão de riscos, com o objetivo de se garantir a manutenção das prioridades mapeadas, independentemente de alterações que envolvam o manuseio e trato das informações institucionais.

4.2.3 PRODUTOS ESPERADOS:

4.2.3.1 Metodologia de gestão de risco documentada (processos e responsabilidades): Comunicação e consulta, Estabelecimento dos contextos, Identificação e estimativa de Riscos, Análise, Avaliação e Tratamento do Risco, Monitoramento e análise crítica;

4.2.3.2 Piloto para validação da metodologia de gestão de riscos.

4.2.4 ATIVIDADES DE APOIO:

4.2.4.1 PLANO DE TRABALHO com o detalhamento do escopo da metodologia e cronograma de execução;

4.2.4.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;

4.2.4.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

4.2.5 PRAZO DE ENTREGA:

4.2.5.1 O serviço deverá ser executado em até 30 (trinta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.3 DESCRIÇÃO DETALHADA PARA ANÁLISE DE RISCOS E VULNERABILIDADES EM SEGURANÇA DA INFORMAÇÃO

4.3.1 Inventariar, analisar, avaliar e tratar os riscos relacionados aos ativos de informação do TJCE, determinando as consequências e probabilidades e, por conseguinte, o nível de risco, considerando, no que couber, os seguintes normativos:

4.3.1.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.

4.3.1.2 NORMATIVOS ABNT: ABNT NBR ISO Guia 73:2005; ABNT NBR ISO/IEC 27005:2008; ABNT NBR ISO/IEC 27001:2006; ABNT NBR ISO/IEC 27002:2005 e ISO 31000;

4.3.1.3 Caso haja mudança dos normativos relacionados acima, estas deverão ser, necessariamente, observadas e aplicadas durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas demandas normativas apresentadas;

4.3.1.4 Caso os normativos acima sejam, em sua totalidade ou em parte, substituídos, os novos normativos deverão ser, necessariamente, observados e aplicados;

4.3.1.5 Durante a execução dos serviços, deverão ser observadas pela Contratada tantas mudanças quanto forem necessárias para adequar o TJCE aos novos normativos em vigência;

4.3.2 Deverão ser observados os seguintes aspectos para a ANÁLISE DE RISCOS:

4.3.2.1 Análise do Faltante (GAP Analisys) de acordo com normativos e melhores práticas;

4.3.2.2 Deverão ser inventariados os ativos de tecnologia, sistemas e serviços de tecnologia da informação, pessoas e ambientes físicos.

4.3.2.3 Deverá ser gerado um relatório de inventário de ativos para validação por representante do TJCE, contendo:

4.3.2.4 Tipo de ativo (Ativos de Negócios do TJCE; Ativos de Segurança da Informação do TCJE);

4.3.2.5 Relevância do ativo para o atendimento da missão institucional do TJCE;

4.3.2.6 Deverão ser analisados os ativos inventariados considerando seus respectivos componentes constantes no relatório de inventário entregue e validado na etapa anterior.

4.3.2.7 Deverão ser gerados relatórios gerenciais, apresentando indicadores que possibilitem a avaliação por parte dos gestores do atual nível de risco do TJCE;

4.3.3 O RELATÓRIO GERENCIAL DE RISCOS demonstrando como foi avaliada cada situação de risco e como foram valorados os ativos de negócio, de segurança da informação, humanos, processuais e tecnológicos, obedecendo a seguinte relação entre os itens abaixo relacionados e a base normativa indicada:

4.3.3.1 Ativos (ISO/IEC 13335-1:2004 e ISO/IEC 27001:2006):

4.3.3.2 Tipo de ativo (ISO/IEC 27001:2006 e ISO/IEC 27005:2008):

4.3.3.3 Ativos de Negócios do TJCE;

4.3.3.4 Ativos de Segurança da Informação do TJCE

4.3.3.5 Relevância do ativo para o atendimento da missão institucional do TJCE;

4.3.3.6 Risco (ISO/IEC Guide 73, AS/NZS 4360 e ISO 31000):

4.3.3.7 Impacto [COSO (Risk Solutions, 2007)];

4.3.3.8 Evento [COSO (Risk Solutions, 2007 e ISO/IEC Guide 73:2002)];

4.3.3.9 Vulnerabilidade (ISO/IEC 13335-1:2004 e ISO 31000);

4.3.3.10 Efeito;

4.3.3.11 Ameaça (ISO/IEC 27000:2009):

4.3.3.12 Tipo de ameaça;

4.3.3.13 Agente da ameaça;

4.3.3.14 Tratamento de riscos (ISO 31000, ISO/IEC Guide 73:2002 e ISO/IEC 31010:2009):

4.3.3.15 Evitar o risco;

4.3.3.16 Reduzir o risco;

4.3.3.17 Transferir o risco;

4.3.3.18 Reter o risco;

4.3.3.19 Requisitos de segurança;

4.3.3.20 Controles:

4.3.3.21 Referência do controle;

4.3.3.22 Justificativa do controle;

4.3.3.23 Recomendações para a implementação do controle;

4.3.3.24 Custo/esforço aproximado para implementação do controle.

4.3.4 Os RELATÓRIOS DE OCORRÊNCIA DE RISCOS IDENTIFICADOS que tragam consigo recomendações para o tratamento das não conformidades acima identificadas, ainda que estas não possam ser tratadas.

4.3.5 O processo de análise de riscos deverá envolver profissionais especialistas em análise de riscos e especialistas no negócio do Tribunal (identificados pela contratada quando do levantamento dos ativos de segurança da informação do TJCE).

4.3.6 Entrevistas com os usuários e técnicos de TI do TJCE deverão ser realizadas e documentadas com o intuito de medir o nível de conscientização de cada um no que se refere a Segurança da Informação.

4.3.7 Deverão ser levantados, identificados, listados, documentados e quantificados os ambientes físicos sensíveis, onde gestores tratam informações confidenciais. Após o levantamento deverá ser realizada análise de risco detalhada de cada um dos mencionados ambientes levantados.

4.3.8 A análise dos insumos identificados no RELATÓRIO GERENCIAL DE RISCOS deverá contemplar, no mínimo, o quantitativo amostral abaixo relacionado. Caso o quantitativo em questão não consiga demonstrar, claramente, a situação de segurança atual do parque tecnológico do TJCE, nova análise deverá ser feita com agregação de tantos itens quanto necessário para demonstrar a real situação em comento:

4.3.8.1 Servidores de rede, físicos e virtuais: 150 itens de verificação;

4.3.8.2 Equipamentos / ativos de conectividade: 200 itens de verificação;

4.3.8.3 Estações de trabalho: 100 itens de verificação;

4.3.8.4 Pessoas (Gestores/Usuários/Técnicos): 250 itens de verificação. As entrevistas deverão refletir o nível de conhecimento dos colaboradores alocados em TODOS os setores do TJCE. Ademais, os detentores de cargo em comissão do TJCE deverão ser entrevistados e, particularmente, entrevistas pessoais deverão ser realizadas com TODOS os Secretários do Tribunal;

4.3.8.5 Ambientes Físicos (Escritórios/Datacenters);

4.3.9 Na análise deverão ser considerados, no mínimo, os seguintes ativos de tecnologia e respectivos desdobramentos:

4.3.9.1 Servidores

4.3.9.2 Sistema Operacional;

4.3.9.3 Aplicação de banco de dados;

4.3.9.4 Serviços de TI.

4.3.9.5 Estações de Trabalho

4.3.9.6 Sistema Operacional;

4.3.9.7 Aplicativos de Escritório;

4.3.9.8 Softwares de Comunicação.

4.3.9.9 Equipamentos de Conectividade

4.3.9.10 Configurações de Segurança dos sistemas;

4.3.9.11 Regras de Segurança (Firewalls, IPS);

4.3.9.12 Disposição física.

4.3.9.13 Ambientes Físicos (Escritórios/Datacenters);

4.3.9.14 Boas práticas para Datacenters;

4.3.9.15 Boas práticas para Escritórios.

4.3.9.16 Sistemas

4.3.9.17 Processo de Desenvolvimento (desenvolvimento seguro de aplicações).

4.3.9.18 Situações de risco

4.3.9.19 Interferência eletromagnética, indisponibilidade de serviços ou informações, altas temperaturas ou umidade, falha de energia, falha de hardware, falha de software, queda de desempenho, código malicioso, acesso lógico não autorizado, fraude ou sabotagem, paralisação dos serviços ou informações, erros humanos, omissões ou uso indevido, acesso físico não autorizado, incêndio, furto ou roubo, falta de mão-de-obra essencial, falha em meios de comunicação, violação de propriedade intelectual, perda de rastreabilidade, multas, indenizações ou sanções legais, repúdio, não atendimento à regulamentação, dano a pessoas e instalações, perda de integridade de dados.

4.3.9.20 Quaisquer outras ameaças deverão ser consideradas nas análises de riscos quando necessárias à adequada execução dos serviços e/ou demandas do TJCE.

4.3.10 Com base nos resultados das análises mencionadas, deverá ser gerado o RELATÓRIO DE MITIGAÇÃO DE RISCOS, contendo soluções para cada item de insegurança levantado no "RELATÓRIO DE OCORRÊNCIAS DE RISCOS IDENTIFICADOS";

4.3.11 Nesta etapa, a Contratada deverá disponibilizar para a Equipe Técnica do TJCE um PLANO DE TRATAMENTO DE RISCOS, contemplando ações de controle de riscos e viabilidade de implantação, contendo no mínimo: Ações a serem implantadas; Prazos para Implantação; Áreas Funcionais responsáveis por implantar e manter controle sobre os riscos;

4.3.12 A Contratada deverá realizar Workshop(s) para prestar orientação e capacitação à Equipe Técnica do TJCE, visando o correto entendimento e a correta execução do PLANO DE TRATAMENTO DE RISCOS.

4.3.13 Durante a vigência do Contrato:

4.3.13.1 O acompanhamento do nível de risco dos ativos do TJCE deverá ser realizado pela Contratada de forma constante e por meio de um plano chamado "PLANO DE TRATAMENTO DE RISCOS ANUAL", a ser apresentado, previamente, ao TJCE, que o analisará e o aprovará antes de sua efetiva aplicação em ambiente de produção. Este plano deverá apresentar os índices de riscos esperados com base no tratamento sugerido pela Contratada.

4.3.13.2 A Contratada deverá atualizar os índices de riscos com base nas informações fornecidas pelo TJCE dos controles de riscos que forem sendo tratados. Os novos índices de riscos deverão ser apresentados trimestralmente aos gestores do TJCE. A empresa contratada deverá, a partir da atualização oficial de fontes normativas de pesquisa de risco que tragam novas vertentes identificadas de risco, adaptar sua metodologia de avaliação de risco para atender a esses novos indicativos normativos. Os ativos tecnológicos deverão ser analisados pela Contratada antes de sua entrada em ambiente de produção na Entidade. Deverá ser gerado um novo relatório de riscos do ativo analisado antes de sua entrada em ambiente de produção com as evidências de que os riscos foram tratados.

4.3.14 Os resultados das análises de riscos trimestrais deverão ser consolidados e apresentados por meio de relatórios, em formato gerencial e técnico, denominados:

4.3.14.1 RELATÓRIO TRIMESTRAL DE RISCOS DOS ATIVOS TECNOLÓGICOS DO TJCE;

4.3.14.2 RELATÓRIO CONSOLIDADO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO DO TJCE.

4.3.14.3 Os relatórios deverão compreender, no mínimo, informações sobre:

4.3.14.3.1 Avaliação de riscos dos ativos analisados, indicando os critérios, requisitos, metodologias e ponderações utilizadas;

4.3.14.3.2 As evidências necessárias apuradas;

4.3.14.3.3 As ameaças e vulnerabilidades encontradas;

4.3.14.3.4 A classificação de riscos e criticidades atribuídas;

4.3.14.3.5 A mensuração financeira estimada para auxiliar na decisão de tratamento do risco;

4.3.14.3.6 A identificação dos responsáveis e processos de negócio;

4.3.14.3.7 A análise de impactos;

4.3.14.3.8 Os controles propostos para a mitigação e tratamento do risco;

4.3.14.3.9 Indicadores quantitativos e qualitativos de riscos, dentre outras informações;

4.3.14.3.10 Observações pertinentes para o julgamento da análise.

4.3.15 Todo relatório/plano sobre análise de risco deverá identificar ações e definições para evitar, transferir, reter, reduzir ou mitigar os riscos apresentados. Também deverá identificar possíveis prejuízos, caso o Tribunal opte por não tratar os riscos previamente observados pela Contratada. Todo relatório, ao ser apresentado ao TJCE, deverá demonstrar a(s) metodologia(s) aplicada(s) bem como se esta(s) possui(em) aderência normativa ao compêndio identificado.

4.3.16 PRODUTOS ESPERADOS:

4.3.16.1 Na 1ª execução:

4.3.16.1.1 Relatório Análise do Faltante (Gap Analisys) com observância dos normativos;

4.3.16.1.2 Relatório de Inventário de Ativos de Informação com observância dos normativos;

4.3.16.1.3 Relatório Gerencial de Riscos;

4.3.16.1.4 Relatório de Ocorrência de Riscos Identificados e Recomendações;

4.3.16.1.5 Relatório de Mitigação de Riscos;

4.3.16.1.6 Plano de Tratamento de Riscos;

4.3.16.2 Nas demais execuções na vigência do contrato:

4.3.16.2.1 Plano de Tratamento de Riscos Anual;

4.3.16.2.2 Relatório Trimestral de Riscos dos Ativos;

4.3.16.2.3 Relatório Consolidado de Riscos;

4.3.17 ATIVIDADES DE APOIO:

4.3.17.1 PLANO DE TRABALHO com o detalhamento do escopo da análise e cronograma de execução;

4.3.17.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;

4.3.17.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

4.3.18 PRAZO DE ENTREGA:

4.3.18.1 Na 1ª execução: o serviço deverá ser executado em até 90 (noventa) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.3.18.2 Nas demais execuções na vigência do contrato: o serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.4 DESCRIÇÃO DETALHADA PARA TESTES DE INVASÃO INTERNOS E EXTERNOS;

4.4.1 A atividade de Testes de Invasão Externos e Internos tem como objetivo principal identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica do TJCE. Estes testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações do TJCE.

4.4.2 Para a realização dos testes de invasão deverão ser observadas as orientações e técnicas emanadas pelos seguintes padrões internacionais, além de outros apresentados pela empresa contratada, caso haja, em seu portfólio, normativos que, comprovadamente, complementem os demonstrados abaixo:

4.4.2.1 OSSTMM 3 (The Open Source Security Testing Methodology Manual);

4.4.2.2 ISSAF/PTF (Information Systems Security Assessment Framework);

4.4.2.3 NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment);

4.4.2.4 NIST Special Publication 800-42 (Guideline on Network Security Testing);

4.4.2.5 OWASP TESTING GUIDE 3.0 - The Open Web Application Security Project.

4.4.3 O teste de invasão deverá obedecer às seguintes fases: 1ª) Planejamento; 2ª) Descoberta; 3ª) Ataque (exploração); 4ª) Relatório de recomendações;

4.4.4 A Contratada deverá observar que os testes, simulações de invasão ilícita e não autorizada a ativos e informações (Teste de Invasão), a serem executadas internamente (através da rede interna do TJCE) ou externamente (através da Internet), deverão ter duração máxima de até 20 (vinte) dias para cada simulação realizada.

4.4.5 Os alvos dos “Testes de Invasão” bem como as premissas e condições para realização dos mesmos serão, necessariamente, definidas e aprovadas pelo TJCE.

4.4.6 Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas pelo TJCE. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada ao TJCE, haja vista a necessidade de manter a disponibilidade dos ambientes ativos e serviços do Tribunal.

4.4.7 Deverá ser utilizada, pelo menos, 01 (uma) ferramenta de análise de vulnerabilidade comercial e 01 (uma) ferramenta de análise de vulnerabilidade gratuita. As ferramentas deverão ser apresentadas ao TJCE para ciência e aprovação em sua utilização, antes de sua efetiva utilização.

4.4.8 Deverá realizar análise de vulnerabilidades em até 1.000 (hum mil) endereços IPs do ambiente computacional do TJCE, sendo servidores, desktops, ativos de rede e outros equipamentos relacionados ao teste de vulnerabilidades.

4.4.9 Deverá ser elaborado o “PLANO DE TESTE DE INVASÃO”, para cada teste que será realizado, contemplando as informações de PLANEJAMENTO do teste, tais como:

4.4.9.1 Objetivos, premissas e escopo do teste, datas e horas dos testes, metodologia de análise de vulnerabilidades, descrição das ações realizadas, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas.

4.4.9.2 Também na fase de planejamento, deverão ser atendidas e apresentadas, no mínimo, as seguintes informações:

4.4.9.2.1 Detalhes da infraestrutura alvo dos testes de invasão;

4.4.9.2.2 Equipamentos e recursos demandados para este teste;

4.4.9.2.3 Tipos de ataque;

4.4.9.2.4 Prazos (janelas de tempo para execução dos testes);

4.4.9.2.5 Pontos de contato da contratada (responsáveis para tratamento de questões não abordadas nos testes);

4.4.9.2.6 Tipos de testes a serem realizados pelos especialistas em segurança da informação, devendo-se observar:

4.4.9.2.7 Quanto à abordagem:

4.4.9.2.7.1 Coletar informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas;

4.4.9.2.7.2 Técnica da caixa-preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista);

4.4.9.2.7.3 Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste);

4.4.9.2.7.4 Técnica da caixa cinza ou híbrida (conhecimento limitado sobre o alvo);

4.4.9.2.8 Quanto à forma de publicidade:

4.4.9.2.8.1 Teste informado (a equipe de segurança de TI do TJCE terá conhecimento dos testes);

4.4.9.2.8.2 Teste não informado (a equipe de segurança de TI do TJCE NÃO terá conhecimento dos testes);

4.4.9.3 Informações detalhadas dos testes em si;

4.4.9.4 Nesta fase de planejamento deverá ser obtido, formalmente:

4.4.9.4.1 A aprovação dos responsáveis do TJCE para o início dos testes, por meio de documentação chamada: TERMO DE AUTORIZAÇÃO PARA REALIZAÇÃO DE TESTES DE INVASÃO;

4.4.9.4.2 O preenchimento e a assinatura de TERMO DE CIÊNCIA de TODOS os técnicos da empresa contratada que atuarão nestes testes;

4.4.9.4.3 O preenchimento e a assinatura de TERMO DE COMPROMISSO do(s) representante (s) da contratada;

4.4.9.4.4 A especificação dos endereços IP a serem testados;

4.4.9.4.5 Restrição de ambiente computacional (ex: computadores, servidores, sistemas e sub-redes a NÃO serem testados);

4.4.9.4.6 Lista de técnicas de teste aplicáveis (engenharia social, DOS, etc) e ferramentas (decodificadores de senha, “sniffers” de rede, etc);

4.4.9.4.7 Momentos em que os testes serão conduzidos (ex. durante hora de trabalho, depois de horário de trabalho, etc);

4.4.9.4.8 Endereço IP das máquinas nas quais o teste de invasão será aplicado, de forma que os administradores possam diferenciar o legítimo ataque da empresa contratada dos ataques de hackers;

4.4.9.4.9 Forma de manuseio das informações coletadas pela equipe do teste de invasão.

4.4.10 Na fase da DESCOBERTA deverão ser atendidos os seguintes quesitos e apresentado “RELATÓRIO DE DESCOBERTA DE TESTE DE INVASÃO”, entre outros:

4.4.10.1 Coleta de informações, sendo classificadas em:

4.4.10.1.1 Coleta passiva, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

4.4.10.1.1.1 Whois e nslookup (consultas DNS);

4.4.10.1.1.2 Sites de busca;

4.4.10.1.1.3 Listas de discussão;

4.4.10.1.1.4 Blogs de colaboradores;

4.4.10.1.1.5 Dumpster diving ou trashing;

4.4.10.1.1.6 Informações livres;

4.4.10.1.1.7 Packet sniffing “passive eavesdropping”;

4.4.10.1.1.8 Captura de banner.

4.4.10.1.2 Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

4.4.10.1.2.1 Port scanning (Mapeamento de rede);

4.4.10.1.2.2 Varredura de vulnerabilidade.

4.4.10.2 A varredura de vulnerabilidade deverá verificar/identificar, entre outros:

4.4.10.2.1 Hosts ativos na rede;

4.4.10.2.2 Portas e serviços em execução;

4.4.10.2.3 Serviços ativos e vulneráveis nos hosts;

4.4.10.2.4 Sistemas operacionais;

4.4.10.2.5 Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas;

4.4.10.2.6 Configurações feitas nos hosts sem observância de boas práticas em segurança computacional;

4.4.10.2.7 Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas;

4.4.10.2.8 Identificação de vetores de ataque e cenários para exploração;

4.4.10.2.9 Vulnerabilidades Detectadas (CVE);

4.4.10.2.10 Vulnerabilidades de Alto Risco;

4.4.10.2.11 Vulnerabilidades de Médio Risco;

4.4.10.2.12 Vulnerabilidades de Baixo Risco;

4.4.10.2.13 Informações a serem aplicadas na 3ª fase (fase de ataques);

4.4.10.2.14 Dos serviços e aplicações web:

4.4.10.2.14.1 Uso indevido de sistema de arquivos e arquivos temporários;

4.4.10.2.14.2 Evasão de informação por configurações default de tratamento de erros;

4.4.10.2.14.3 Tratamento indevido de entrada;

4.4.10.2.14.4 Problemas relacionados a má configuração dos serviços;

4.4.10.2.14.5 Gerenciamento inseguro de sessões web;

4.4.10.2.14.6 Verificação de trilhas de auditoria;

4.4.10.2.14.7 Escalação de privilégios;

4.4.10.3 Observa-se que a varredura em questão NÃO poderá:

4.4.10.3.1 Provocar paradas nos serviços prestados pelo ambiente computacional do TJCE;

4.4.10.3.2 Apresentar alta taxa de FALSO/POSITIVO;

4.4.10.3.3 Apresentar base de dados desatualizada (antes da realização de qualquer varredura, deverá ser apresentado ao TJCE provas de que a base de assinaturas das ferramentas utilizadas pela Contratada está atualizada com sua última versão).

4.4.10.4 Observa-se, ainda, que a varredura em questão deverá ser realizada em:

4.4.10.4.1 Redes corporativas autorizadas pelo TJCE;

4.4.10.4.2 Computadores autorizados pelo TJCE;

4.4.10.5 Mapeamento de rede, devendo ser verificado/identificado, entre outros:

4.4.10.5.1 Ativos conectados a rede corporativa do TJCE sem autorização;

4.4.10.5.2 Serviços vulneráveis;

4.4.10.5.3 Serviços autorizados que não estão em conformidade com a atual política de segurança da informação do Tribunal;

4.4.10.5.4 Fragilidades apresentadas pelos sistemas de IDS/IPS corporativos.

4.4.11 Na fase de ATAQUE deverão ser apresentadas, dentro do “RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO”, as seguintes informações:

4.4.11.1 Confirmação ou refutação de a existência de vulnerabilidades;

4.4.11.2 Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade;

4.4.11.3 Obtenção de acesso e possível escalada de privilégios;

4.4.11.4 Deverão ser aplicados, no mínimo, os seguintes tipos de ataques:

4.4.11.4.1 Violações do protocolo HTTP;

4.4.11.4.2 SQL Injection;

4.4.11.4.3 LDAP Injection;

4.4.11.4.4 Cookie Tampering;

4.4.11.4.5 Cross-Site Scripting (XSS);

4.4.11.4.6 Directory Transversal;

4.4.11.4.7 Buffer Overflow;

4.4.11.4.8 OS Command Execution;

4.4.11.4.9 Command Injection;

4.4.11.4.10 Remote Code Inclusion;

4.4.11.4.11 Server Side Includes (SSI) Injection;

4.4.11.4.12 File disclosure;

4.4.11.4.13 Information Leak;

4.4.11.4.14 Zero day attacks;

4.4.11.4.15 DDos (Distribuited Denial of Service);

4.4.11.4.16 Dos (Denial of Service);

4.4.11.4.17 Contra protocolo TCP;

4.4.11.4.18 Ataques contra a aplicação.

4.4.11.5 Os ataques de negação de serviços, contra protocolo TCP e em nível da aplicação deverão, cada qual, explorar/demonstrar/utilizar as seguintes técnicas:

4.4.11.5.1 Para ataques de negação de serviços:

4.4.11.5.1.1 Bugs em serviços, aplicativos e sistemas operacionais;

4.4.11.5.1.2 SYN flooding;

4.4.11.5.1.3 Fragmentação de pacotes de IP;

4.4.11.5.1.4 Smurf e fraggle;

4.4.11.5.1.5 Teardrop, nuke e land.

4.4.11.5.1.6 Para ataques contra o protocolo TCP:

4.4.11.5.1.7 Seqüestro de conexões;

4.4.11.5.1.8 Prognóstico de número de seqüência do protocolo TCP;

4.4.11.5.1.9 Ataque de Mitnick;

4.4.11.5.1.10 Source routing.

4.4.11.5.1.11 Para ataques em nível da aplicação:

4.4.11.5.1.12 Buffer Overflow ;

4.4.11.5.1.13 Problemas com o SNMP;

4.4.11.5.1.14 Vírus, worms e cavalos de tróia.

4.4.12 Observa-se que, antes da utilização de qualquer técnicas acima, o TJCE abrirá janelas de manutenção em seu ambiente tecnológico.

4.4.13 Captura de Tráfego para testar se os algoritmos e protocolos utilizados na comunicação dos sistemas garantem a integridade e privacidade das informações em trânsito;

4.4.13.1 Quebra de Senha de perfis determinados pelo TJCE;

4.4.13.2 Injeção de Código;

4.4.13.3 Ataques XSS (Cross-site Script);

4.4.13.4 Comprometimento do acesso remoto do TJCE;

4.4.13.5 Manutenção de acesso;

4.4.13.6 Encobrimento de rastros da invasão.

4.4.14 Para testes de invasão direcionados, especificamente, aos serviços do TJCE prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados, no mínimo, os seguintes testes baseados na publicação OWASP TESTING GUIDE 3.0 (The Open Web Application Security Project):

4.4.14.1 Para testes de coleta de informações, aplicar padrão: OWASP-IG-001, OWASP-IG-002, OWASP-IG-003, OWASP-IG-004, OWASP-IG-005 e OWASP-IG-006;

4.4.14.2 Para testes de gerenciamento de configuração, aplicar padrão: OWASP-CM-001, OWASP-CM-002, OWASP-CM-003, OWASP-CM-004, OWASP-CM-005, OWASP-CM-006, OWASP-CM-007, OWASP-CM-008;

4.4.14.3 Para testes de autenticação, aplicar padrão: OWASP-AT-001, OWASP-AT-002, OWASP-AT-003, OWASP-AT-004, OWASP-AT-005, OWASP-AT-006, OWASP-AT-007, OWASP-AT-008, OWASP-AT-009 e OWASP-AT-010;

4.4.14.4 Para testes de gerenciamento de sessão, aplicar padrão: OWASP-SM-001, OWASP-SM-001, OWASP-SM-002, OWASP-SM-003, OWASP-SM-004, OWASPSM-005;

4.4.14.5 Para testes de autorização, aplicar padrão: OWASP-AZ-001, OWASP-AZ-002 e OWASP-

AZ-003;

4.4.14.6 Para testes de negócio lógico, aplicar padrão: OWASP-BL-001;

4.4.14.7 Para testes de validação de dados, aplicar padrão: OWASP-DV-001; OWASPDV-002, OWASP-DV-003, OWASP-DV-004, OWASP-DV-005, OWASP-DV-006, OWASP-DV-007, OWASP-DV-008, OWASP-DV-009, OWASP-DV-010, OWASP-DV-011, OWASP-DV-012, OWASP-DV-013, OWASP-DV-014, OWASP-DV-015 e OWASP-DV-016;

4.4.14.8 Para testes de negação de serviços, aplicar padrão: OWASP-DS-001, OWASP-DS-002, OWASP-DS-003, OWASP-DS-004, OWASP-DS-005, OWASP-DS-006, OWASP-DS-007 e OWASP-DS-008;

4.4.14.9 Para testes de serviços web, aplicar padrão: OWASP-WS-001, OWASP-WS-002, OWASP-WS-003, OWASP-WS-004, OWASP-WS-005, OWASP-WS-006 e OWASP-WS-007.

4.4.15 Observa-se que o resultado de cada teste deverá vir acompanhado de relatórios contendo:

4.4.15.1 Referência-base (Whitepaper);

4.4.15.2 Ameaças encontradas;

4.4.15.3 Riscos levantados ao ambiente computacional;

4.4.15.4 Contramedidas para mitigar as ameaças achadas.

4.4.16 Observa-se que cada relatório contendo o resultado de testes deverá ser claro e conciso e fornecer ao TJCE completo entendimento sobre as ameaças e riscos encontrados. Também se observa a necessidade de a empresa apresentar os resultados em tabelas, seguindo o padrão apresentado abaixo:

Categoria	Número de Referência	Nome do Teste	Ameaças	Solução	Riscos

4.4.17 O "RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO" deverá apresentar todas as informações necessárias e completas para o correto entendimento de cada teste realizados em ambiente do TJCE, contemplando no mínimo:

4.4.17.1 Objetivos, premissas e escopo do teste;

4.4.17.2 Metodologia de análise de vulnerabilidades;

4.4.17.3 Descrição das ações realizadas;

4.4.17.4 Vulnerabilidades encontradas;

4.4.17.5 Categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades;

4.4.17.6 Apresentação das evidências apuradas;

4.4.17.7 Fontes de pesquisa, referências e ferramentas utilizadas.

4.4.18 Ao final dos trabalhos, a Contratada deve também apresentar um "RELATÓRIO DE RETORNO SOBRE INVESTIMENTO", onde deverão ser expostas todas as falhas, vulnerabilidades, riscos e ameaças de segurança da informação, identificadas em ambiente corporativo, com FOCO GERENCIAL, ou seja, contendo informações com vista à conscientização e tomada de decisão, pela alta Administração do Tribunal, sobre os riscos a que a instituição está exposta e os gastos necessários para se aumentar o nível de segurança da informação hoje praticado pelo Tribunal.

4.4.19 Deverão ser entregues:

4.4.19.1 Avaliação e relatório da SEGURANÇA FÍSICA do Tribunal, com a finalidade de indicar se o ambiente físico onde se encontram os sistemas críticos do TJCE é adequado e atende a normas e boas práticas internacionais de segurança física relacionadas a ambientes de alta criticidade computacional;

4.4.19.2 Avaliação e relatório da SEGURANÇA TÉCNICO-ADMINISTRATIVA do Tribunal, com a finalidade de indicar o nível de gerenciamento do corpo administrativo e técnico do TJCE com relação às ações de manutenção da proteção dos dados computacionais do Tribunal.

4.4.20 Por fim, a empresa contratada fica ciente de que:

4.4.20.1 Todas as fases dos "Testes de Invasão" deverão ser acompanhadas e supervisionadas a qualquer momento pelo TJCE;

4.4.20.2 A Contratada deverá fazer todo o possível para evitar comprometer o funcionamento normal da infraestrutura de TI do TJCE, bem com resguardar a confidencialidade, integridade e disponibilidade de todas as suas informações;

4.4.20.3 Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo corporativo deverá ser imediatamente reportada ao TJCE;

4.4.20.4 Caso ocorra algum efeito imprevisto na infraestrutura do TJCE em função dos testes, a

Contratada deverá interromper os trabalhos, contatar a Equipe de TI do TJCE e trabalhar em conjunto com a mesma para acelerar a recuperação.

4.4.21 Durante a vigência do Contrato:

4.4.21.1 A Contratada deverá fornecer um "PLANO DE TESTES ANUAL", com datas previstas para execução, conforme acordado com o TJCE

4.4.22 PRODUTOS ESPERADOS:

4.4.22.1 Na 1ª execução:

4.4.22.1.1 PLANO DE TESTE DE INVASÃO: com exposição integral das informações e ações demandadas pela fase de PLANEJAMENTO (término da fase);

4.4.22.1.2 RELATÓRIO DE DESCOBERTA DE TESTE DE INVASÃO: com exposição integral das informações e ações demandadas pela fase de DESCOBERTA (término da fase);

4.4.22.1.3 RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO: com exposição integral das informações e ações demandadas pela fase de ATAQUES (término da fase);

4.4.22.1.4 RELATÓRIO DE RETORNO SOBRE INVESTIMENTO;

4.4.22.1.5 RELATÓRIO DA SEGURANÇA FÍSICA;

4.4.22.1.6 RELATÓRIO DA SEGURANÇA TÉCNICO-ADMINISTRATIVA;

4.4.22.2 Nas demais execuções durante a vigência do contrato:

4.4.22.2.1 PLANO DE TESTE DE INVASÃO ANUAL obedecendo aos mesmos moldes das demandas emanadas pelos PLANO DE TESTE DE INVASÃO e os relatórios da 1ª execução.

4.4.22.2.2 RELATÓRIO DE ATAQUES DO TESTE DE INVASÃO – mensal, trimestral e semestral segundo o observado pelo PLANO DE TESTES ANUAL.

4.4.23 ATIVIDADES DE APOIO:

4.4.23.1 PLANO DE TRABALHO com o detalhamento do escopo dos testes e cronograma de execução;

4.4.23.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;

4.4.23.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

4.4.24 PRAZO DE ENTREGA:

4.4.24.1 Na 1ª execução: o serviço deverá ser executado em até 90 (noventa) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.4.24.2 Nas demais execuções durante a vigência do contrato: o serviço deverá ser executado em até 45 (quarenta e cinco) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.5 DESCRIÇÃO DETALHADA PARA ELABORAÇÃO DAS METODOLOGIAS DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

4.5.1 Definir processo e atividades para o correto tratamento de incidentes, com o foco na identificação, análise, avaliação, tratamento, dentre outras atividades, proporcionando como principal benefício a capacidade de resposta aos incidentes de forma unificada pelo TJCE, considerando, no que couber, os seguintes normativos:

4.5.1.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.

4.5.1.2 NORMATIVOS ABNT: ABNT NBR ISO/IEC 27001:2006;

4.5.1.3 NORMATIVOS NIST (National Institute of Standards and Technology): Handbook for Computer Security Incident Response Teams (CSIRTs) – HANDBOOK CMU/SEI-2003-HB-002; NIST Special Publication 800-61 Revision 1 (Computer Security Incident Handling Guide); NIST Special Publication 800-83 (Guide to Malware Incident Prevention and Handling); NIST Special Publication 800-86 (Guide to Integrating Forensic Techniques into Incident Response);

4.5.1.4 Caso haja mudança dos normativos relacionados acima, estas deverão ser, necessariamente, observadas e aplicadas durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas demandas normativas apresentadas;

4.5.1.5 Caso os normativos acima sejam, em sua totalidade ou em parte, substituídos, os novos normativos deverão ser, necessariamente, observados e aplicados durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas demandas normativas apresentadas;

4.5.1.6 Durante a execução dos serviços, deverá ser observada pela Contratada tantas mudanças

quanto forem necessárias para adequar o Tribunal aos novos normativos em vigência;

4.5.2 Deverá ser gerada uma proposta para implantação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR considerando a estrutura funcional do TJCE e estratégia para sua criação;

4.5.3 A empresa Contratada deverá, necessariamente, após análise do parque computacional do TJCE, bem como da missão institucional do Tribunal, produzir documentação que determine a MISSÃO DA ETIR junto ao Tribunal:

4.5.3.1 Esta declaração deverá conter concisa e inequívoca descrição dos objetivos e a função da ETIR do TJCE.

4.5.3.2 Observa-se que a ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede;

4.5.4 A empresa deverá pautar suas ações na CRIAÇÃO da ETIR do TJCE com base em modelos de organização CENTRALIZADOS, observando-se:

4.5.4.1 A Equipe deverá ser composta, necessariamente, por pessoal com dedicação exclusiva às atividades de tratamento e resposta aos incidentes em redes computacionais.

4.5.4.2 Deverá ser realizado o estudo prévio das atividades/funções de TI em operação no Tribunal, do número de sistemas e plataformas suportadas, do número de serviços a serem oferecidos pela ETIR e do conhecimento técnico necessário do pessoal a ser alocado à equipe de tratamento de incidentes em questão. A estrutura organizacional da ETIR criada deverá observar/atender TODAS AS DEMANDAS LEVANTADAS pelo resultado do estudo prévio.

4.5.5 A AUTONOMIA COMPARTILHADA será o modelo de autonomia a ser observada na constituição da ETIR e esta autonomia deverá obedecer às seguintes características:

4.5.5.1 A ETIR deverá trabalhar em acordo com os outros setores da organização a fim de participar do processo de tomada de decisão;

4.5.5.2 A equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os outros membros da organização;

4.5.6 Deverá ser apresentado documento de CONSTITUIÇÃO DA ETIR onde deverão ser indicados TODOS os membros do processo decisório do Tribunal envolvidos com TODA a tomada de decisão relacionada a incidentes identificados em âmbito do Tribunal.

4.5.6.1 Apresentam-se, abaixo, as especialidades (membros) que poderão compor a ETIR, entre outros julgados pertinentes ao incidente a ser tratado:

4.5.6.1.1 Administradores de sistema ou de segurança;

4.5.6.1.2 Administradores de banco de dados;

4.5.6.1.3 Administradores de rede;

4.5.6.1.4 Analistas de suporte;

4.5.6.1.5 Representantes legais de áreas específicas da organização;

4.5.6.1.6 Controle interno.

4.5.7 A empresa contratada deverá apresentar ao TJCE procedimentos a serem aplicados a TODOS OS MEMBROS DA ETIR QUE DEIXAREM A EQUIPE EM QUESTÃO. Abrangendo, no mínimo:

4.5.7.1 Mudança de senhas (pessoais e de sistemas);

4.5.7.2 Devolução de todos os dispositivos/ferramentas em posse do membro em questão;

4.5.7.3 Revogação de chaves;

4.5.7.4 Entrevista de saída com a finalidade de relembrar ao colaborador das responsabilidades assumidas e ciência de sigilo profissional;

4.5.7.5 Informações sobre novo contato do colaborador (e-mail, telefone).

4.5.8 A empresa contratada deverá documentar, descrever e estruturar 02 (dois) tipos de serviços proativos e reativos da ETIR, com detalhamento de tarefas e ações específicas;

4.5.9 A empresa Contratada deverá produzir e apresentar ao TJCE uma política de classificação de incidentes computacionais. Esta política deverá conter uma taxonomia comum que possibilite identificação e classificação correta dos vários tipos de incidentes de TI.

4.5.10 A empresa Contratada deverá propor modelo de formulário específico para reporte de incidentes computacionais.

4.5.11 A empresa deverá indicar ao TJCE a necessidade ou não da aplicação de turnos diferenciados de trabalhos para a ETIR, recomendando práticas de sucesso adotadas em outros órgãos federais e/ou iniciativa privada.

4.5.12 A empresa deverá apresentar ao TJCE proposta de ferramentas para limpeza completa de dados em processo de descarte, bem como orientar o Tribunal sobre a forma e modo de eliminação de informações geradas pelos trabalhos realizados pela ETIR.

4.5.13 A empresa Contratada deverá padronizar procedimento de comunicação da ETIR do TJCE em relação à ocorrência de incidentes de segurança em redes de computadores.

4.5.14 A empresa Contratada deverá padronizar rotinas junto a ETIR do TJCE que possibilite aos membros desta equipe:

4.5.14.1 Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;

4.5.14.2 Observar os procedimentos para preservação das evidências exigindo consulta às orientações sobre cadeia de custódia, conforme ato normativo específico a ser expedido;

4.5.14.3 Priorizar a continuidade dos serviços da ETIR do TJCE e da missão institucional da organização, observando os procedimentos previstos no item acima.

4.5.15 A empresa deverá apresentar ao TJCE uma proposta de treinamento para TODOS OS MEMBROS DA ETIR, devendo atender, no mínimo, conhecimentos relacionados a:

4.5.15.1 Procedimentos operacionais de ETIRs;

4.5.15.2 Políticas de segurança do Tribunal;

4.5.15.3 Identificação e entendimento de técnicas de intrusão;

4.5.15.4 Procedimento de comunicação com as partes envolvidas;

4.5.15.5 Análise de incidentes;

4.5.15.6 Gravação e manutenção de incidentes;

4.5.15.7 Distribuição de tarefas/ações pertinentes;

4.5.15.8 Produção de relatórios de tratamento de incidentes com informações detalhadas, no mínimo, sobre: descrição do incidente de segurança, indicação do método utilizado para coleta de evidências, ações de contenção realizadas, evidências apuradas, recomendações de controles, ações corretivas e preventivas para evitar a reincidência do incidente de segurança e observações pertinentes ao tratamento do incidente em questão.

4.5.16 PRODUTOS ESPERADOS:

4.5.16.1 Modelo de Gestão de Resposta a Incidentes;

4.5.16.2 Proposta de Implantação;

4.5.16.3 Documento com Missão da ETIR;

4.5.16.4 Documento de constituição da ETIR;

4.5.16.5 Documento com detalhamento de tipos de serviços, tarefas e ações da ETIR;

4.5.16.6 Política de classificação de incidentes computacionais;

4.5.16.7 Modelo de formulário para reporte de incidentes computacionais;

4.5.16.8 Proposta de utilização de ferramentas para limpeza completa de dados;

4.5.16.9 Procedimento de comunicação da ETIR do TJCE em caso de indícios de ilícitos criminais;

4.5.16.10 Proposta de treinamento;

4.5.16.11 Treinamento para os membros do ETIR;

4.5.17 ATIVIDADES DE APOIO:

4.5.17.1 PLANO DE TRABALHO com o detalhamento do escopo da metodologia e cronograma de execução;

4.5.17.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;

4.5.17.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

4.5.18 PRAZO DE ENTREGA:

4.5.18.1 O serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.6 DESCRIÇÃO DETALHADA PARA CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DO MODELO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

4.6.1 Criação ou revisão da forma de estruturação e atuação do Comitê Gestor de Segurança da Informação do TJCE em conformidade com o regimento interno e as portarias vigentes no Órgão, assim como dos Normativos: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.

4.6.2 Deverão ser revisadas ou criadas, neste serviço, as definições de infraestrutura de Segurança

da Informação para:

4.6.2.1 Processos componentes;

4.6.2.2 Funções dos processos componentes;

4.6.2.3 Fluxos de informações entre os processos componentes bem como com os demais processos corporativos;

4.6.2.4 Responsáveis pelos processos componentes;

4.6.2.5 Estrutura organizacional necessária ao perfeito funcionamento da infraestrutura;

4.6.2.6 Estratégia de implementação da infraestrutura de Segurança da Informação.

4.6.3 Deverá ser efetuada, ainda, a inclusão dos processos de infraestrutura de segurança da informação na estrutura organizacional do TJCE, a ser representada graficamente por meio do organograma da instituição.

4.6.4 Deverá ser observado que algumas das funções definidas não terão, necessariamente, unidade operacional exclusiva sendo, portanto, desempenhadas por unidades já existentes;

4.6.5 A infraestrutura de Segurança da Informação a ser revisada deverá estar em conformidade com os tópicos relacionados ao assunto das normas ABNT NBR ISO/IEC 27002:2005 e ABNT NBR ISO/IEC 27001:2006.

4.6.6 O Modelo de Gestão de Segurança da Informação deverá contemplar toda a infraestrutura operacional e organizacional existente no TJCE.

4.6.7 PRODUTOS ESPERADOS:

4.6.7.1 Relatório com análise da estruturação e atuação do Comitê;

4.6.7.2 Relatório de Propostas de Melhoria;

4.6.7.3 Definições de infraestrutura de Segurança da Informação;

4.6.7.4 Modelo de gestão documentado, contendo: Descrição dos processos definidos; Funções definidas; Fluxo de informações entre os processos; Responsáveis pelos processos; Relatório de Modelo de Gestão de Segurança da Informação e Comunicações; Estratégia de implantação com a superposição dos processos definidos sobre as áreas responsáveis já existentes.

4.6.8 ATIVIDADES DE APOIO:

4.6.8.1 PLANO DE TRABALHO com o detalhamento do escopo da revisão e cronograma de execução;

4.6.8.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;

APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

4.6.9 PRAZO DE ENTREGA:

4.6.9.1 O serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.7 DESCRIÇÃO DETALHADA PARA CRIAÇÃO, REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

4.7.1 Estabelecer diretrizes, critérios e procedimentos para análise, revisão, complementação, elaboração, atualização, institucionalização e divulgação da Política de Segurança da Informação – PSI do TJCE, retificando, ratificando ou incluindo normas, e da ABNT:

4.7.1.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.

4.7.1.2 Sistemas de gestão de segurança da informação - Requisitos - ABNT NBR ISO/IEC 27001:2006;

4.7.1.3 ABNT NBR ISO/IEC 27002:2005 - Código de Prática;

4.7.1.4 Gestão de riscos de segurança da informação - ABNT NBR ISO/IEC 27005:2008;

4.7.1.5 Gestão de continuidade de negócios - Parte 1: Código de prática ABNT NBR 15999-1:2007 e Parte 2: Requisitos - ABNT NBR 15999-2:2008.

4.7.2 Em legislação brasileira deverá ser observado, necessariamente, a seguinte legislação pertinente: Lei nº 9.983, de 14 de julho de 2000 (Código Penal).

4.7.3 Caso haja mudança dos normativos relacionados acima, as mudanças deverão ser, necessariamente, observadas e aplicadas durante toda a vigência contratual. Caso os trabalhos/relatórios/entregáveis já tiverem sido aceitos/assimilados pelo TJCE, a empresa contratada, em sua próxima execução contratual do item demandado, adequará sua metodologia de trabalho às novas demandas normativas apresentadas;

4.7.4 Caso os normativos acima sejam, em sua totalidade ou em parte, substituídos, os novos normativos deverão ser, necessariamente, observados e aplicados;

4.7.5 Durante a execução dos serviços, deverá ser observada pela Contratada tantas mudanças quanto forem necessárias para adequar o Tribunal aos novos normativos em vigência;

4.7.6 Deverão ser considerados os resultados da análise de riscos, quanto aos aspectos relativos à falta de padronização e normatização das práticas de tratamento da informação corporativa;

4.7.7 Política de Segurança da Informação deverá ser revisada em conjunto com Grupo de Trabalho constituído por representantes dos diferentes setores do TJCE;

4.7.8 A Política de Segurança da Informação deverá ser composta por 3 (três) níveis:

4.7.8.1 Diretrizes Gerais – compreendendo as diretrizes e políticas de segurança, definidas de acordo com a estrutura organizacional, administrativa e funcional do TJCE, devendo conter, no mínimo, os temas abaixo, considerando as Normas específicas vigentes no ordenamento jurídico:

4.7.8.1.1 Tratamento da Informação;

4.7.8.1.2 Tratamento e Resposta de Incidentes de Rede;

4.7.8.1.3 Gestão de Risco;

4.7.8.1.4 Gestão de Continuidade;

4.7.8.1.5 Auditoria e Conformidade;

4.7.8.1.6 Controles de Acesso;

4.7.8.1.7 Uso de e-mail; e

4.7.8.1.8 Acesso a Internet.

4.7.8.2 Tático - compreende as regras de normatização das permissões e proibições no âmbito da segurança corporativa da informação e comunicações;

4.7.8.3 Operacional – compreende as definições dos procedimentos de execução das ações de segurança e os padrões a serem adotados.

4.7.9 A empresa Contratada deverá rever e atualizar, necessariamente os normativos de segurança da informação, atualmente em vigor no tribunal:

4.7.10 Deverão ser elaborados, também, modelos de documentos auxiliares à implementação da Política de Segurança e Comunicações, como Termos de Compromisso, Termo de Ciência, dentre outros que se fizerem necessários;

4.7.11 Todos os documentos gerados deverão conter, no mínimo, as seções:

4.7.11.1 Objetivo;

4.7.11.2 Público alvo;

4.7.11.3 Descrição;

4.7.11.4 Definições;

4.7.11.5 Data de publicação;

4.7.11.6 Data de validade;

4.7.11.7 Data da última atualização;

4.7.11.8 Condições obrigatórias de atualização do documento;

4.7.11.9 Responsável pela atualização;

4.7.11.10 Dicionário de referência contendo os termos técnicos.

4.7.12 Para a divulgação da Política de Segurança da Informação deverão ser elaborado e fornecido pela contratada material informativo com os princípios gerais da Política de Segurança da Informação na forma de guia de consulta rápida;

4.7.13 A empresa contratada deverá elaborar e submeter à apreciação do TJCE um novo conjunto de normativos não contemplados, especificamente, pela atual política de segurança da informação do TJCE, conforme definido a seguir:

4.7.13.1 Norma de conformidade legal – Estabelece procedimento de checagem (checklist) da aderência legal dos contratos e procedimentos administrativos internos, em atendimento a legislação civil ou criminal, estatutos, regulamentações, normativos ou obrigações contratuais e requisitos de segurança da informação;

4.7.13.2 Norma de segregação de funções – Estabelece critérios para evitar controle total de um processo por parte de um único usuário do Tribunal, impedindo, assim, acúmulo de autoridade bem como uso acidental ou deliberado dos ativos corporativos em prejuízo do Tribunal e terceiros;

4.7.13.3 Norma de segurança para equipe técnica de TI do TJCE – Estabelece regras gerais para a administração/operacionalização de recursos de tecnologia da informação do Tribunal;

4.7.13.4 Norma para instalação e configuração segura de dispositivos de roteamento computacional – Estabelece regras de instalação e configuração segura, específicas para

dispositivos de roteamento computacional, com revisão de procedimentos atualmente aplicados pelo Tribunal;

4.7.13.5 Norma para instalação e configuração segura de dispositivos de segurança da informação do TJCE - Estabelece regras de instalação e configuração segura a serem implementadas nos dispositivos de segurança da informação do TJCE, com revisão de procedimentos atualmente aplicados pelo Tribunal;

4.7.13.6 Norma para instalação e configuração segura de sistemas operacionais – Estabelece regras seguras que deverão ser observadas quanto à instalação e configuração de sistemas operacionais corporativos, com revisão de procedimentos atualmente aplicados pelo Tribunal;

4.7.13.7 Norma para instalação e configuração de aplicações – Estabelece regras seguras que deverão ser observadas quanto à instalação e configuração de aplicações, com revisão de procedimentos atualmente aplicados pelo Tribunal;

4.7.13.8 Norma de Segurança para SLA (Servise Level Agreement) Acordo de Nível de Serviço – Estabelece regras seguras que deverão ser observadas e utilizadas nos contratos baseados em acordo de nível de serviço;

4.7.13.9 Norma de aspectos da Gestão da Continuidade de Negócio – Estabelece regras seguras que deverão ser observadas e utilizadas na gestão da continuidade do negócio;

4.7.13.10 Norma com aspectos da Gestão de Riscos – Estabelece regras seguras que deverão ser observadas e utilizadas na gestão de riscos;

4.7.13.11 Norma de Computação Móvel e Trabalho Remoto – Estabelece regras seguras que deverão ser observadas e utilizadas para a computação móvel e trabalho remoto;

4.7.13.12 Norma de Uso de Redes Sociais – Estabelece regras seguras que deverão ser observadas e utilizadas no uso de redes sociais, regulação, monitoramento e código de conduta;

4.7.13.13 Norma de Classificação e Tratamento de Incidentes Computacionais – Estabelece regras seguras que deverão ser observadas e utilizadas no tratamento de incidentes, contendo no mínimo:

4.7.13.13.1 O que constitui um incidente de segurança da informação;

4.7.13.13.2 Como este incidente deve ser tratado;

4.7.13.13.3 Quais os ativos críticos que devem ser protegidos.

4.7.13.13.4 Termos a serem abordados na norma:

4.7.13.13.4.1 Atividades de tratamento de incidente; Artefatos; Ataques; Eventos; Incidentes; Intrusão; Reporte de incidente; Probe/Scan; Vulnerabilidade e Tratamento da vulnerabilidade.

4.7.13.14 Norma de implementação, operacionalização, manutenção e acesso às redes sem fio do TJCE – Estabelece procedimento de implementação, operacionalização, manutenção e acesso às redes sem fio do TJCE. Esta norma deverá conter:

4.7.13.14.1 As melhores práticas de segurança da informação relativas às redes sem fio comercialmente oferecidas no mundo;

4.7.13.14.2 Orientações para a realização periódica de testes de invasão e análise de riscos e vulnerabilidades em redes sem fio;

4.7.13.14.3 Segregação de tarefas na administração da solução de redes sem fio do TJCE;

4.7.13.14.4 Política de educação dos usuários com relação à segurança no manuseio da solução em questão;

4.7.13.14.5 Regras de instalação, configuração, gerenciamento, administração, localização e aprovação de Pontos de Acesso nas dependências do Tribunal;

4.7.13.14.6 Modo de operação de cartões de rede que acessam as redes sem fio do Tribunal;

4.7.13.14.7 Concessão e revogação de privilégios de acesso para usuários comuns e usuários privilegiados (técnicos);

4.7.13.14.8 Orientações com relação à atualização desta norma, a partir da mudança do parque computacional do TJCE que suporta esta solução sem fio (manter a norma sempre coerente com a evolução tecnológica das redes sem fio do Tribunal);

4.7.13.14.9 Indicação de que todos os técnicos envolvidos com o constante suporte desta solução deverão passar por treinamento específico, a partir da alteração/mudança/atualização dos ativos de TI relacionados às redes sem fio do Tribunal;

4.7.13.14.10 Orientações com relação à requisição de níveis específicos de autenticação para acesso a aplicações críticas do Tribunal;

4.7.13.14.11 A exigência de que todos os dispositivos de rede sem fio operem somente em

modo de infraestrutura (infrastructure mode);

4.7.13.14.12 Orientações de como proceder, caso o usuário necessite utilizar os dispositivos de rede sem fio do TJCE (notebooks) fora das dependências do Tribunal (acesso a redes sem fio públicas).

4.7.13.15 Norma sobre uso de dispositivos móveis dentro do TJCE – Estabelece procedimento de implementação, operacionalização e manutenção de regras e diretrizes no uso de dispositivos móveis nos aspectos relativos a Segurança da Informação e Comunicação em âmbito do Tribunal. Esta norma deverá criar os seguintes atores responsáveis pelo manuseio dos dispositivos móveis:

4.7.13.15.1 Agentes públicos com dispositivos móveis corporativos;

4.7.13.15.2 Agentes públicos com dispositivos móveis particulares;

4.7.13.15.3 Agente Responsável;

4.7.13.15.4 Dispositivos móveis;

4.7.13.15.5 Usuários visitantes com dispositivos móveis;

4.7.13.15.6 Dispositivos móveis removíveis de armazenamento;

4.7.14 PRODUTOS ESPERADOS:

4.7.14.1 Relatório com Análise das Normas vigentes;

4.7.14.2 Relatório de Propostas de Melhoria das Normas vigentes;

4.7.14.3 Documento de Política de Segurança da Informação, com o novo conjunto de normativos;

4.7.14.4 Documento para formalização e aprovação por parte da autoridade máxima responsável;

4.7.14.5 Dicionário dos termos técnicos utilizados nos documentos;

4.7.14.6 Sumário executivo para apresentação à alta Administração;

4.7.14.7 Guia de consulta rápida com os princípios gerais da Política de Segurança da Informação e para a divulgação da Política de Segurança da Informação;

4.7.15 ATIVIDADES DE APOIO:

4.7.15.1 PLANO DE TRABALHO com o detalhamento do escopo da revisão e cronograma de execução;

4.7.15.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;

4.7.15.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

4.7.16 PRAZO DE ENTREGA:

4.7.16.1 O serviço deverá ser executado em até 90 (noventa) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.8 DESCRIÇÃO DETALHADA PARA ELABORAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL

4.8.1 Implantar processos de Gestão de Continuidade de Negócios buscando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do TJCE, além de permitir que sejam recuperados ativos da informação a um nível aceitável por intermédio de ações de prevenção, resposta e recuperação.

4.8.2 Deverão ser considerados os resultados da análise de riscos, quanto aos aspectos relativos ao levantamento de risco físico e valoração dos ativos e sistemas de informação.

4.8.3 O escopo do projeto será definido com base na análise de impacto onde deverão ser considerados apenas os ativos que fazem parte da missão critico-institucional do Tribunal, levantados e identificados previamente pela empresa Contratada e acordados com o TJCE.

4.8.4 Deverá ser realizada coleta de dados junto aos responsáveis da Secretaria de Tecnologia da Informação - SETIN para a definição das operações críticas realizadas pela área, definir e elaborar os planos de recuperação.

4.8.4.1 A SETIN poderá solicitar que seja realizada coleta de dados junto às áreas gestoras, responsáveis pela alimentação dos sistemas e bancos de dados;

4.8.5 Deverá ser gerado um documento descrevendo o plano de recuperação de desastres em ambiente computacional do TJCE (PRDAC-TJCE) para o escopo definido na análise de riscos, considerando os normativos aplicáveis.

4.8.5.1 O programa deverá prover o TJCE com ações e ferramentas que possibilitem a recuperação de sistemas e redes computacionais ao seu estado normal de operação no MENOR TEMPO POSSÍVEL (tempo a ser definido com base no resultado do levantamento realizado pela contratada em relação aos processos e tecnologias críticas que mantêm os negócios essenciais do TJCE com clara concordância do Tribunal).

4.8.6 Normativos aplicáveis quando da elaboração, implantação e manutenção do PRDAC-TJCE:

4.8.6.1 NORMATIVOS: Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário; Resolução TCE/CE Nº 3.550/2010; Decreto Estadual do CE Nº 29.227/2008.

4.8.6.2 Normativos internacionais - deverá se observado, NO QUE FOR PERTINENTE, a seguinte base normativa:

4.8.6.2.1 NIST SP 800-34;

4.8.6.2.2 NIST SP 800-34 REV1

COBIT v4.1, em especial os processos AI2, DS1, DS2, DS4, DS8, **4.8.6.2.3** DS11, DS13, PO2 e PO9;

4.8.6.2.4 ITIL v3, em especial os processos SD4.5, CSI5.6.3, SD4.4.5.2 e SO5.2;

4.8.6.2.5 ISO/IEC 24762;

4.8.6.2.6 BS 25777;

4.8.6.2.7 BS 25999;

4.8.6.3 Normativos ABNT - deverá ser observado, NO QUE FOR PERTINENTE, os seguintes normativos da ABNT:

4.8.6.3.1 ABNT NBR ISO/IEC 15999#1:2007;

4.8.6.3.2 ABNT NBR ISO/IEC 27005:2008;

4.8.6.3.3 ABNT NBR ISO/IEC 27002:2005.

4.8.6.3.4 ABNT NBR ISO 22301:2013.

4.8.7 A empresa Contratada deverá identificar e sugerir mudanças na infraestrutura das redes computacionais do TJCE para atender a continuidade das atividades de TI do Tribunal dentro dos novos padrões de recuperação tecnológica propostos.

4.8.8 O plano de recuperação de desastres em ambiente computacional do TJCE a ser implementado precisará abordar:

4.8.8.1 Requisitos estratégicos de continuidade computacional relativos aos processos e às atividades operacionais;

4.8.8.2 Ações para mitigação de riscos, reação durante um evento e recuperação depois de um evento;

4.8.8.3 Priorização de processos críticos de negócio suportados pela TI.

4.8.9 A produção do plano de recuperação de desastres em ambiente computacional do TJCE deverá considerar:

4.8.9.1 A conformidade com os requisitos de segurança da informação e comunicações necessárias à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, o que inclui pessoas, processos, infraestrutura e recursos de tecnologia da informação e comunicações do Tribunal;

4.8.9.2 Os requisitos de uma atualização anual do Programa;

4.8.10 A empresa contratada deverá:

4.8.10.1 Obedecer, no mínimo, as seguintes fases para a produção do PRDAC:

4.8.10.1.1 PREVENÇÃO/REDUÇÃO/MITIGAÇÃO;

4.8.10.1.2 REAÇÃO;

4.8.10.1.3 RECUPERAÇÃO;

4.8.10.2 Apresentar, no mínimo, os seguintes planos, componentes do PRDAC e seus sub-planos claramente identificados dentro deste programa:

4.8.10.2.1 PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;

4.8.10.2.2 PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS;

4.8.10.2.3 PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA);

4.8.10.2.4 PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;

4.8.10.2.5 PLANO DE TESTES E EXERCÍCIOS;

4.8.10.2.6 PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE;

4.8.10.2.7 PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL;

4.8.10.2.8 PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS.

4.8.11 Na fase de PREVENÇÃO/REDUÇÃO/MITIGAÇÃO a empresa contratada deverá:

4.8.11.1 Apresentar o PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE, onde deverão ser abordadas as necessidades de recuperação de desastres computacionais do Tribunal, a organização e administração do PRDAC -TJCE;

4.8.11.2 Avaliar os riscos computacionais associados aos processos críticos e atividades operacionais do TJCE e apresentar o PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS;

4.8.11.3 Apresentar o PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA), onde serão identificadas as operações críticas do Tribunal apoiadas pela TI, bem como os recursos necessários para sustentar estas operações;

4.8.11.4 Apresentar o PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE, onde deverá ser demonstrada a metodologia de desenvolvimento do PRDAC –TJCE, bem como sua organização, forma de implantação e documentação;

4.8.11.5 Apresentar o PLANO DE TESTES E EXERCÍCIOS, onde deverão constar os tipos de testes e exercícios a serem aplicados no ambiente computacional do Tribunal de acordo com a suas peculiaridades e características;

4.8.11.6 Apresentar o PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE, onde deverão ser abordadas as metodologias de auditoria, revisão e manutenção do PRDAC-TJCE;

4.8.11.7 Estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho da entidade, bem como as técnicas para quantificar e qualificar esses impactos. Deverá ser estimado, também, a criticidade dos processos computacionais do Tribunal, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

4.8.12 PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE

4.8.12.1 A empresa contratada deverá definir com o TJCE:

4.8.12.1.1 O objetivo do PRDAC;

4.8.12.1.2 A montagem/treinamento de equipes específicas para apoio do PRDAC.

4.8.12.2 Deverá conter, entre outros artefatos considerados importantes pela empresa contratada, os seguintes produtos:

4.8.12.2.1 Proposta de PRDAC para a TI;

4.8.12.2.2 Estrutura do PRDAC em detalhes que possam identificar TODAS AS AÇÕES E ATIVIDADES PERTINENTES À CORRETA RECUPERAÇÃO DE DESASTRES COMPUTACIONAIS DO TJCE;

4.8.12.2.3 Definição de terminologias e pontos essenciais aplicados ao PRDAC;

4.8.12.2.4 Método de gerenciamento de mudanças no PRDAC;

4.8.12.2.5 Papel, no mínimo, das seguintes equipes:

4.8.12.2.5.1 Planejamento:

4.8.12.2.5.1.1 Direção da SETIN;

4.8.12.2.5.1.2 Equipe de desenvolvimento e manutenção do PRDAC.

4.8.12.2.6 Resposta:

4.8.12.2.6.1 Equipe de resposta à emergência computacional;

4.8.12.2.6.2 Equipe de avaliação de danos;

4.8.12.2.6.3 Equipe de comunicação.

4.8.12.2.7 Recuperação:

4.8.12.2.7.1 Equipe de recuperação operacional e tecnológica;

4.8.12.2.7.2 Equipe associada de suporte.

4.8.12.3 As equipes acima poderão ser agrupadas caso não haja prejuízo das atividades a serem desenvolvidas e caso a direção da SETIN assim o determine.

4.8.13 PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS:

4.8.13.1 Deverão ser atendidos, no mínimo, os seguintes elementos-chave da gestão de continuidade de negócios do TJCE, pertinentes também a TI, segundo a norma ABNT NBR ISO/IEC 27002:2005:

4.8.13.1.1 Entendimento dos riscos a que a organização esta exposta;

4.8.13.1.2 Identificação de todos os ativos de TI envolvidos em processos críticos de negócio;

4.8.13.1.3 Entendimento do impacto que incidentes computacionais com envolvimento da segurança da informação terão sobre os negócios;

4.8.13.1.4 Probabilidade e impacto da interrupção de TODOS OS PROCESSOS COMPUTACIONAIS CRÍTICOS DO TRIBUNAL, tanto em escala de dano quanto em relação ao período de recuperação;

4.8.13.2 Deverão ser demonstradas a identificação, quantificação e priorização dos critérios baseados nos riscos, com a identificação e inclusão de TODOS OS RECURSOS CRÍTICOS COMPUTACIONAIS, IMPACTO DE INTERRUPÇÃO E PRIORIDADE DE RECUPERAÇÃO DESTES RECURSOS DO TJCE;

4.8.13.3 A empresa contratada deverá levar em consideração, no mínimo, os riscos advindos de:

4.8.13.3.1 Riscos naturais (inundações, incêndios, etc.);

4.8.13.3.2 Riscos humanos (greves, paralisações, empregados mal preparados, etc.);

4.8.13.3.3 Riscos técnicos (ambiente computacional, datacenter, comunicação de dados, rede telefônica, energia, etc.);

4.8.13.4 A empresa também deverá:

4.8.13.4.1 Classificar, pontuar os riscos e apresentar matrizes de riscos;

4.8.13.4.2 Agrupar os riscos interdependentes;

4.8.13.4.3 Reconhecer, documentar e priorizar riscos à organização;

4.8.13.4.4 Identificar e mapear os impactos qualitativos e quantitativos de um evento de risco;

4.8.13.4.5 Identificar e avaliar os tipos de controles em operação. Incluir custo de manutenção destes controles;

4.8.13.4.6 Sugerir melhoras nos controles existentes por meio de documentação, capacitação, reforço, manutenção e testes. Apresentar custo/benefício dos controles.

4.8.13.4.7 Recomendar controles adicionais;

4.8.13.4.8 Auditar funções e responsabilidades e apresentar recomendações de mudanças pertinentes;

4.8.13.5 O PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS deverá conter ainda, entre outros artefatos considerados importantes pela empresa contratada, os seguintes produtos:

4.8.13.5.1 Eventos e exposições de alta frequência e impacto;

4.8.13.5.2 Lista de controles e proteção;

4.8.13.5.3 Priorização dos riscos e investimentos;

4.8.13.5.4 Coleta externa e interna de dados para avaliação de riscos.

4.8.14 PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA):

4.8.14.1 Deverá ser realizada uma Análise de Impacto nos Negócios (Business Impact Analysis – BIA) do TJCE, com objetivo de:

4.8.14.1.1 Avaliar a criticidade dos processos tecnológicos de sistemas de informação;

4.8.14.1.2 Estimar a importância dos ativos de sustentação tecnológica da organização;

4.8.14.1.3 Definir os tempos máximos de parada e recuperação (RTO – Recovery Time Objective) e de perda de dados (RPO – Recovery Point Objective);

4.8.14.1.4 Levantar, mapear e propor solução para todo inter-relacionamento entre os fornecedores de TI do TJCE e os sistemas críticos do Tribunal, com relação ao adequado tempo de recuperação dos ativos computacionais críticos do Tribunal;

4.8.14.1.5 Levantar e mapear os conhecimentos internos associados à recuperação destes sistemas bem como sequências lógicas de ações para o correto reestabelecimento das atividades críticas do Tribunal;

4.8.14.1.6 Definir os processos e ativos que serão contemplados nos planos, bem como sua ordem de priorização.

4.8.14.2 Deverá, após identificação dos riscos computacionais, categorizar e priorizar as operações computacionais críticas do TJCE e seus inter-relacionamentos e sugerir orçamentos/recursos necessários para mantê-las em atividade.

4.8.14.3 Deverão ser observados e atendidos os seguintes itens:

4.8.14.3.1 Fornecer:

4.8.14.3.2 Alternativas de estratégias de recuperação de desastres;

4.8.14.3.3 Informações sobre possíveis perdas.

4.8.14.3.4 Estabelecer:

4.8.14.3.4.1 Objetivos de recuperação no tempo (RTO).

4.8.14.3.5 Determinar:

4.8.14.3.5.1 Prazos de recuperação e exigências mínimas de recursos.

4.8.14.3.6 Avaliar:

4.8.14.3.6.1 Os possíveis impactos da interrupção ao longo do tempo.

4.8.14.3.7 Identificar os seguintes fatores de impacto:

4.8.14.3.7.1 Operacionais;

4.8.14.3.7.2 Financeiros;

4.8.14.3.8 Apresentar:

4.8.14.3.8.1 Relatório executivo com informações relevantes levantadas na fase do BIA.

4.8.14.3.9 Realizar as seguintes fases com contextualização pertinente e apresentação de resultados:

4.8.14.3.9.1 Planejamento do projeto de BIA;

4.8.14.3.9.2 Coleta e análise de dados;

4.8.14.3.9.3 Documentação dos achados.

4.8.14.3.10 Definir, junto com o TJCE, as áreas foco da BIA;

4.8.14.3.11 Identificar e apresentar custos do impacto das interrupções dos processos computacionais críticos do TJCE nos seguintes aspectos:

4.8.14.3.11.1 Financeiro;

4.8.14.3.11.2 Cidadão;

4.8.14.3.11.3 Legal/regulamentação;

4.8.14.3.11.4 Ambiental;

4.8.14.3.11.5 Operacional;

4.8.14.3.11.6 Público interno;

4.8.14.3.11.7 Contratual.

4.8.14.3.12 Períodos de recuperação:

4.8.14.3.12.1 Determinar o RTO para as funções computacionais críticas identificadas;

4.8.14.3.12.2 Determinar a ordem de recuperação (criticidade) das atividades computacionais;

4.8.14.3.12.3 Determinar o RPO;

4.8.14.3.12.4 Determinar a necessidades de recursos para recuperação e continuidade das funções críticas e sistemas de suporte;

4.8.14.3.12.5 Determinar a época de substituição de recursos;

4.8.14.3.12.6 Apresentar cronograma de restauração de recursos.

4.8.15 PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE

4.8.15.1 A empresa contratada deverá demonstrar a metodologia de desenvolvimento do PRDAC-TJCE e apresentar a documentação, implementação e organização do plano em questão.

4.8.15.2 A empresa contratada também deverá:

4.8.15.2.1 Observar os seguintes elementos do PRDAC:

4.8.15.2.1.1 Pessoas;

4.8.15.2.1.2 Locais;

4.8.15.2.1.3 Informação;

4.8.15.2.1.4 Recursos;

4.8.15.2.1.5 Processos.

4.8.15.2.2 Definir no PRDAC:

4.8.15.2.2.1 Linhas de tempo;

4.8.15.2.2.2 Objetivos;

4.8.15.2.2.3 Produtos;

4.8.15.2.2.4 Documentação especifica;

4.8.15.2.2.5 Premissas;

4.8.15.2.2.6 Cenários;

4.8.15.2.2.7 Procedimento de distribuição e controle;

4.8.15.2.2.8 Tipos de segurança aplicadas aos documentos;

4.8.15.2.2.9 Períodos para revisões do PRDAC.

4.8.15.2.3 Na confecção do plano, abordar:

4.8.15.2.3.1 Locais;

4.8.15.2.3.2 Processos de negócio;

4.8.15.2.3.3 Catalogação, por níveis, dos possíveis impactos advindos da interrupção dos processos e serviços críticos do TJCE;

4.8.15.2.3.4 Estratégias recomendadas para a devida recuperação de desastres em ambiente computacional do TJCE;

4.8.15.2.3.5 Projeção de validade e atualização deste plano pelo prazo de 05 (cinco) anos.

4.8.15.2.4 Observar os seguintes componentes do PRDAC:

4.8.15.2.4.1 Visão geral;

4.8.15.2.4.2 Gerenciamento de incidentes;

4.8.15.2.4.3 Grupos e tarefas;

4.8.15.2.4.4 Processo críticos;

4.8.15.2.4.5 Contatos críticos;

4.8.15.2.4.6 Tecnologias envolvidas (Identificação dos ativos computacionais que suportam estes processos críticos);

4.8.15.2.4.7 Registros vitais e armazenamento externo;

4.8.15.2.4.8 Equipamentos e suprimentos;

4.8.15.2.4.9 Manutenção do plano;

4.8.15.2.4.10 Anexos.

4.8.15.3 O plano deverá ter CARÁTER GERENCIAL, com linguagem clara e objetiva, para exposição à DIRETORIA DE TECNOLOGIA do Tribunal, avaliação e validação.

4.8.15.4 A empresa contratada deverá apresentar PLANEJAMENTO para manutenção do PRDAC-TJCE.

4.8.15.5 Deverão ser apresentadas TODAS AS HIPÓTESES ONDE O PRDAC-TJCE PRECISARÁ SER ATUALIZADO, levando em conta a criticidade das operações internas e observando a metodologia de gerenciamento de mudanças já implantada corporativamente.

4.8.16 PLANO DE RECUPERAÇÃO DE OPERAÇÕES

4.8.16.1 Deverá ser baseado nos levantamentos/mapeamentos realizados na infraestrutura operacional do TJCE que suportam os processos computacionais críticos do Tribunal;

4.8.16.2 A empresa contratada deverá observar e apresentar roteiro / manuais / procedimentos que habilitem as pessoas a, em caso de situações de contingência corporativa, seguir determinadas linhas de ação para conter os danos provocados por paradas nas soluções computacionais críticas do TJCE. Estes roteiros/manuais/procedimentos deverão ser objetivos, claros e possibilitar, efetivamente, o contingenciamento das situações apresentadas. Deverá, também, identificar as ações a que cada equipe mapeada no processo de recuperação estará responsável.

4.8.16.3 O plano deverá prever, entre outros insumos:

4.8.16.4 Alternativas para evitar paradas dos processos computacionais críticos do TJCE, devendo ser considerado e analisado, de acordo com os níveis de criticidade das soluções de negócio do TJCE suportadas pela TI, a melhor alternativa, levando-se em considerações soluções de mercado como:

4.8.16.4.1 Plano COLD SITE;

4.8.16.4.2 Plano WARM SITE;

4.8.16.4.3 Plano HOT SITE;

4.8.16.4.4 Contratos de reciprocidade;

4.8.16.4.5 Plano SITE ESPELHO;

4.8.16.4.6 Os tipos de armazenamentos fora do TJCE, como armazenamento online de dados e logs críticos, espelhamentos de base de dados;

4.8.16.4.7 As frequências destes armazenamentos;

4.8.16.4.8 Os tipos de backups usados: incremental, completo, diferencial;

4.8.16.5 O armazenamento, fora das dependências do Tribunal, de seu PRDAC – TJCE, com a devida segurança/controle de acesso. Esta segurança deverá ser compatível e/ou superior à segurança aplicada em ambiente interno e observar os processos DS4.9 do COBIT, SO 5.2.3 do ITIL v3 e item 10.5.1 da ABNT NBR ISO/IEC 27002:2005.

4.8.16.6 Estabelecer metodologias para acionamento de equipes de recuperação computacional do TJCE, onde deverá constar TODAS AS TAREFAS AFETAS ÀS EQUIPES, os recursos necessários (tecnologia, pessoal, informações, etc), os detalhes de contatos internos e externos, quem, como e quando acionar, entre outros;

4.8.16.7 Propor prazos para que as equipes de recuperação sejam acionadas;

4.8.16.8 Apresentar custos estimados para atendimento das alternativas mencionadas;

4.8.16.9 Apresentar pré-requisitos operacionais / técnicos / corporativos e de infraestrutura computacional para manter as soluções críticas do TJCE em constante operação;

4.8.16.10 Propor, a partir da análise do PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS, as situações, condições e ocorrências que determinarão o acionamento das equipes de recuperação mencionadas.

4.8.17 PLANO DE TESTES E EXERCÍCIOS

4.8.17.1 A empresa contratada deverá:

4.8.17.1.1 Demonstrar os tipos de testes e exercícios pertinentes ao âmbito do Tribunal, incluindo:

4.8.17.1.1.1 Simulação de PARADA TOTAL dos sistemas críticos do TJCE;

4.8.17.1.1.2 Simulação de PARADA PARCIAL dos sistemas críticos do TJCE;

4.8.17.1.1.3 Simulação de checagem dos procedimentos pertinentes implementados junto à equipe de restauração/recuperação;

4.8.17.1.1.4 Indicação de como e quando cada elemento do plano será testado;

4.8.17.1.1.5 Simulação de diferentes cenários e diferentes formas de interrupção;

4.8.17.1.1.6 Apresentação de ações de recuperação em ambientes/locais alternativos;

4.8.17.1.1.7 As prioridades, frequência e tipos de testes e exercícios aplicáveis ao Tribunal.

4.8.17.2 Os testes e exercícios deverão ser realizados, também, de forma geral (testando se o TJCE, seu pessoal, equipamentos, recursos e processos podem enfrentar interrupções).

4.8.17.2.1 Definir testes em:

4.8.17.2.1.1 Equipamentos;

4.8.17.2.1.2 Tecnologias;

4.8.17.2.2 Selecionar método de testes/exercícios que:

4.8.17.2.2.1 Possam testar o plano em sua máxima extensão possível;

4.8.17.2.2.2 Custos não sejam proibitivos para o TJCE;

4.8.17.2.2.3 Interrupções de trabalho sejam mínimas;

4.8.17.2.2.4 Resultados possibilitem alto grau de confiabilidade na capacidade de recuperação;

4.8.17.2.2.5 Resultados demonstrem que as ações aplicadas foram efetivamente aprendidas pelo TJCE;

4.8.17.3 Realizar testes de interdependência entre diferentes tecnologias computacionais;

4.8.17.4 Estabelecer regras de confidencialidade pertinentes.

4.8.17.5 Observa-se que parte dos testes deste plano foram coletados e deverão obedecer a norma ABNT NBR ISO/IEC 27002:2005 com a devida aplicação junto a TI.

4.8.17.6 Deverá ser executado 1 (um) teste de mesa para validação dos planos elaborados.

4.8.17.7 Deverão ser definidos claramente os objetivos do(s) teste(s), sendo preparados checklists de acompanhamento e validação.

4.8.17.8 Deverá ser elaborado relatório contendo os resultados obtidos no(s) teste(s).

4.8.17.9 Ao final do(s) teste(s), o plano deverá ser atualizado de acordo com os resultados obtidos.

4.8.18 PLANOS DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC -TJCE

4.8.18.1 A empresa contratada deverá apresentar:

4.8.18.1.1 Metodologia de revisão/atualização do PRDAC-TJCE bem como respectiva

metodologia de auditoria;

4.8.18.1.2 Proposta e aplicação de manutenção do PRDAC-TJCE;

4.8.18.1.3 Fatores de mudança do Programa;

4.8.18.1.4 Procedimentos para controle da documentação do PRDAC-TJCE.

4.8.18.2 Deverão ser inseridos nos PLANOS DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE as seguintes atividades, dentre outras consideradas importantes pela empresa contratada:

4.8.18.2.1 No plano de MANUTENÇÃO:

4.8.18.2.1.1 Definição de responsabilidades;

4.8.18.2.1.2 Manutenção programada;

4.8.18.2.1.3 Manutenção não programada;

4.8.18.2.1.4 Inclusão de todos os ativos tecnológicos críticos do TJCE.

4.8.18.2.2 No plano de REVISÃO:

4.8.18.2.2.1 Aplicação de metas e métodos pertinentes;

4.8.18.2.2.2 Identificação de fatores de mudanças;

4.8.18.2.2.3 Revisão completamente documentada;

4.8.18.2.3 No plano de AUDITORIA a empresa deverá fornecer ao TJCE, após análise do PRDAC-TJCE, clara evidência da gestão eficiente e eficaz de TODO O PROCESSO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TRIBUNAL.

4.8.18.2.4 Os procedimentos de auditoria aplicados deverão obedecer, dentro da devida pertinência, aos requisitos elencados nos normativos federais, internacionais e da ABNT abordados neste programa, propondo, a partir do resultado de cada auditoria, melhorias e alterações pertinentes ao PRDAC-TJCE.

4.8.18.3 As auditorias acima referidas deverão ser realizadas nas instalações do TJCE e de forma SEMESTRAL enquanto perdurar a vigência contratual entre o Tribunal e a empresa contratada.

4.8.19 Na fase de REAÇÃO a empresa contratada deverá:

4.8.19.1 Apresentar o PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL, com a finalidade de:

4.8.19.1.1 Propor procedimentos de comunicação pertinentes;

4.8.19.1.2 Propor a estabilização dos locais afetados;

4.8.19.1.3 Propor a minimização de danos ocorridos;

4.8.19.1.4 Identificar:

4.8.19.1.4.1 Tipos de emergências pertinentes ao Tribunal;

4.8.19.1.4.2 Atuais procedimentos implementados pelo TJCE bem como recomendar novas ações de resposta a emergência;

4.8.19.1.4.3 Equipes e tarefas;

4.8.19.2 Estabelecer, junto com o TJCE, notificação de autoridades apropriadas em horário comercial e fora deste horário;

4.8.19.3 Desenvolver:

4.8.19.3.1 Notificação de emergência identificando:

4.8.19.3.1.1 Propósitos;

4.8.19.3.1.2 Objetivos;

4.8.19.3.1.3 Sequência de notificação;

4.8.19.3.2 Alarmes.

4.8.20 Na fase de RECUPERAÇÃO a empresa contratada deverá apresentar o PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS.

4.8.20.1 O plano terá por finalidade:

4.8.20.1.1 Apresentar diretrizes de uma comunicação eficaz, coleta e avaliação de informações relevantes, público-alvo da crise e porta-voz nomeado para representação do Tribunal em situações de crise;

4.8.20.1.2 Identificar ações necessárias para contenção dos danos advindos do desastre ocorrido;

4.8.20.1.3 Apresentar orientações sobre recuperação e avaliação de danos.

4.8.20.2 A empresa contratada deverá propor PLANO DE RECUPERAÇÃO DE ATIVOS

COMPUTACIONAIS que possibilite a manutenção da disponibilidade da informação no nível e escala de tempo requeridos pelo TJCE, após a ocorrência de interrupções ou falhas dos processos computacionais críticos do Tribunal, conforme observado pelo item 14.1.3 da norma ABNT NBR ISO/IEC 27002:2005.

4.8.20.3 A empresa deverá levantar e identificar, junto com o TJCE, as seguintes informações que comporão o plano em questão:

4.8.20.3.1 Objetivo e escopo;

4.8.20.3.2 Papéis e responsabilidades;

4.8.20.3.3 Autoridade responsável;

4.8.20.3.4 Detalhes de contato;

4.8.20.3.5 Lista de tarefas;

4.8.20.3.6 Fases do plano de recuperação;

4.8.20.3.7 Recursos necessários;

4.8.20.3.8 Perda aceitável de informações e serviços;

4.8.20.3.9 Implementação de procedimentos que possibilitem a recuperação e restauração das operações computacionais e da disponibilidade da informação nos prazos necessários (prazos a serem apresentados como resultado da análise de impacto computacional no negócio do TJCE - BIA). Estes procedimentos de recuperação deverão:

4.8.20.3.9.1 Descrever ações detalhadas para a transferência das atividades computacionais críticas do Tribunal para localidade alternativa temporária e reativação destas atividades no prazo determinado;

4.8.20.3.9.2 Descrever ações a serem adotadas quando do restabelecimento das operações;

4.8.20.3.10 Avaliação de dependências computacionais externas ao negócio e contratos existentes;

4.8.20.3.11 Procedimentos que permitam a finalização de restaurações e recuperações pendentes;

4.8.20.3.12 Documentação de processos e procedimentos de recuperação;

4.8.20.3.13 Treinamento adequado dos responsáveis pelo acompanhamento e ações relativas aos processos e procedimentos de recuperação;

4.8.20.3.14 Procedimentos operacionais temporários durante a conclusão da recuperação e restauração pertinentes;

4.8.20.3.15 Programação de manutenção que especifique quando e como este plano deverá ser testado e o modo de se proceder a sua manutenção;

4.8.20.4 Observa-se que os itens acima, a constituírem o PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS DO TJCE, refletem as instruções emanadas pelas normas ABNT NBR ISO/IEC 27002:2005, que deverão ser obedecidas pela empresa contratada.

4.8.20.5 Observa-se, ainda, que o plano deverá:

4.8.20.5.1 Apresentar períodos de tempo (dias/horas/minutos) para recuperação de atividades/sistemas/processos computacionais críticos do TJCE (RTO). Apresentar, ainda, método de classificação de itens, categorias de negócios críticos e relacioná-los aos períodos acima;

4.8.20.5.2 Apresentar planejamento que determine o ponto no tempo onde as atividades/sistemas/processos computacionais críticos do TJCE serão recuperadas após interrupções (RPO). Este planejamento deverá estar alinhado à metodologia de armazenamento e backup apresentada pelo PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;

4.8.20.5.3 Apresentar estimativas de tempo de recuperação para:

4.8.20.5.3.1 Datacenter corporativo;

4.8.20.5.3.2 Redes e comunicação de dados corporativos;

4.8.20.5.3.3 Help-Desk corporativo.

4.8.20.6 As equipes formadas para gerenciamento do processo de recuperação do ambiente computacional deverão ser plenamente capacitadas para responder às possíveis situações de crises levantadas neste Programa. Deverá ainda ser apresentado o mapeamento de TODAS AS TAREFAS AFETAS A ESTAS EQUIPES, DE FORMA ESPECÍFICA. Estas tarefas deverão possibilitar aos responsáveis o tratamento da crise do começo ao final, inclusive após a normalização das atividades/serviços críticos afetados.

4.8.20.7 O PLANO ainda deverá conter o REGISTRO DE INFORMAÇÃO DO PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAL, abaixo mencionado.

4.8.21 REGISTRO DE INFORMAÇÃO DO PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAL

4.8.21.1 A empresa contratada deverá apresentar planejamento para implementação de sistema que possibilite ao TJCE recuperar TODAS AS INFORMAÇÕES INERENTES A DESASTRES, PARADAS DE SISTEMAS e RECUPERAÇÃO DE SUAS OPERAÇÕES CRÍTICAS.

4.8.22 O PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS deverá compreender somente os dados e equipamentos da Sala Cofre, sob supervisão da área de Tecnologia da Informação.

4.8.23 PRODUTOS ESPERADOS:

4.8.23.1 Na 1ª execução:

4.8.23.1.1 Plano de Recuperação de Desastres em Ambiente Computacional (PRDACTJCE);

4.8.23.1.2 RELATÓRIO INICIAL para o TJCE, após levantamento realizado nas dependências da SETIN, de todas as soluções computacionais em vigência no Tribunal relativas à recuperação de seus ativos tecnológicos, com demonstrativo da situação atual do Tribunal e a situação futura (a partir do levantamento e apresentação do PRDAC-TJCE);

4.8.23.1.3 PROJETO DE GERENCIAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;

4.8.23.1.4 PLANO DE AVALIAÇÃO DE RISCOS COMPUTACIONAIS;

4.8.23.1.5 PLANO DE ANÁLISE DE IMPACTO COMPUTACIONAL NO NEGÓCIO DO TJCE (BIA);

4.8.23.1.6 PLANO ESTRATÉGICO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE;

4.8.23.1.7 PLANO DE RECUPERAÇÃO DE OPERAÇÕES;

4.8.23.1.8 PLANO DE TESTES E EXERCÍCIOS;

4.8.23.1.9 PLANO DE AUDITORIA, MANUTENÇÃO E REVISÃO DO PRDAC-TJCE;

4.8.23.1.10 PLANO DE RESPOSTA À EMERGÊNCIA COMPUTACIONAL;

4.8.23.1.11 PLANO DE RECUPERAÇÃO DE ATIVOS COMPUTACIONAIS.

4.8.23.1.12 Treinamento das equipes de recuperação de desastres;

4.8.23.1.13 Relatórios de testes realizados;

4.8.23.2 Nas demais execuções durante a vigência do contrato a empresa contratada deverá revisar o PRDAC-TJCE, incluídos todos os planos que fazem parte deste programa, nas seguintes hipóteses:

4.8.23.2.1 Mudança normativo-legal federal relativo à continuidade de negócios no que tange a TI;

4.8.23.2.2 Mudança em normativos internacionais afetos à continuidade de negócios no que tange a TI;

4.8.23.2.3 Mudança e acréscimos de normativos ABNT inerentes ao PRDAC -TJCE;

4.8.23.2.4 Criação de novos normativos nacionais e/ou internacionais que venham a agregar dados e informações que possibilitem a melhora do PRDAC-TJCE;

4.8.23.2.5 Sempre que for solicitado pelo TJCE com base em mudanças estruturais/organizacionais/lógicas/físicas de seu ambiente computacional, que determinem alterações necessárias no PRDAC-TJCE para manter válido todos os planos e ações inerentes à continuidade de negócios do Tribunal providas pela TI.

4.8.24 ATIVIDADES DE APOIO:

4.8.24.1 PLANO DE TRABALHO com o detalhamento do escopo da elaboração e cronograma de execução, de maneira a possibilitar que o TJCE verifique o integral cumprimento do item “PLANO DE RECUPERAÇÃO DE DESASTRES EM AMBIENTE COMPUTACIONAL DO TJCE”, bem como deste Termo de Referência;

4.8.24.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;

4.8.24.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

4.8.25 PRAZO DE ENTREGA:

4.8.25.1 Na 1ª execução: o serviço deverá ser executado em até 90 (noventa) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.8.25.2 Nas demais execuções na vigência do contrato: o serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.9 DESCRIÇÃO DETALHADA PARA ELABORAÇÃO DO PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO

4.9.1 Desenvolvimento de um plano estratégico de segurança da informação para a organização, alinhado com o Plano Estratégico Institucional (PEI) e o Plano Estratégico de Tecnologia da Informação (PETI) do Tribunal, com intuito de direcionar seus esforços de manutenção, inovação e melhoria da Segurança da Informação dentro de uma visão de gestão institucional, informacional e de riscos com a diminuição dos impactos decorrentes de falhas de segurança da informação.

4.9.2 Descrição detalhada das ações de segurança a serem implementadas, contendo seus objetivos, descrições, detalhamento de recursos mínimos necessários, prazo de execução e pré-requisitos obrigatórios;

4.9.3 Cronograma de Trabalho, com a representação gráfica das ações de segurança descritas no plano, distribuídas no tempo, contendo as datas de início e fim recomendadas para as atividades, sua duração e os recursos mínimos necessários para a sua execução.

4.9.4 O PDSI deverá ter o seguinte escopo:

4.9.4.1 Deverá abranger todas as possíveis e necessárias ações de segurança a serem executadas durante o prazo de 04 (quatro) anos;

4.9.4.2 Deverá possuir, não se restringindo aos mesmos, os controles constantes das normas ABNT NBR ISO/IEC 27002:2005 e ABNT NBR ISO/IEC 27001:2006 aplicáveis à realidade do TJCE, em conformidade com a fase de análise de riscos e testes de invasão;

4.9.4.3 Deverá observar, dentro da devida pertinência, o resultado dos levantamentos/testes/análises realizados.

4.9.5 Identificação das necessidades de segurança de novos serviços de proteção, de novos ativos e controles que precisarão ser implementados para elevar o grau de serviço prestado pelo TJCE, com base na análise de riscos e teste de invasão realizadas;

4.9.6 Emissão de relatório técnico com as necessidades que a arquitetura de segurança de TI do TJCE precisará satisfazer contemplando:

4.9.6.1 A confrontação das necessidades com as melhores práticas adotadas pelo mercado;

4.9.6.2 Os objetivos gerais a serem atendidos;

4.9.6.3 A lista de serviços a serem implementados;

4.9.6.4 Relação de ativos de segurança que necessitam ser implementados e ou aperfeiçoados;

4.9.7 Definição das arquiteturas de referência rede / serviços de TI capazes de satisfazer no curto, médio e longo prazo as necessidades identificadas, alinhadas com as tendências tecnológicas globais e em aderência às estratégias do Tribunal para Segurança da Informação;

4.9.8 PRODUTOS ESPERADOS:

4.9.8.1 Na 1ª execução:

4.9.8.1.1 Relatório técnico com as necessidades que a nova arquitetura de Segurança de TI do TJCE precisará satisfazer contemplando:

4.9.8.1.2 A confrontação das necessidades com as melhores práticas adotadas pelo mercado;

4.9.8.1.3 O estabelecimento dos objetivos gerais a serem atendidos pela nova arquitetura de tecnologia da informação do TJCE;

4.9.8.1.4 A lista de serviços de informação a serem prestados por esta nova arquitetura;

4.9.8.1.5 A relação de ativos de segurança que necessitam ser implementados e ou aperfeiçoados.

4.9.8.1.6 Documento com objetivos de evolução da rede corporativa do TJCE, delineando a topologia e arquitetura da rede, os aspectos relacionados com backbone principal, comunicação com organizações externas e as disciplinas de gerência necessárias à gestão desta estrutura;

4.9.8.1.7 Documento com ajustes necessários no núcleo básico da arquitetura de segurança do ambiente de informática decorrente da nova arquitetura de referência, com descrição das estratégias de contingência e recuperação (plano de contingência e recuperação de desastres);

4.9.8.1.8 Relatório do Plano Diretor de Segurança da Informação;

4.9.8.1.9 Cronograma de Trabalho anexo ao relatório, representando graficamente as ações de segurança descritas no Plano Diretor de Segurança da Informação e sua distribuição temporal.

4.9.8.2 Nas demais execuções durante a vigência do contrato, a empresa contratada deverá revisar o PDSI incluídos todos os documentos e cronogramas que fazem parte deste programa, nas seguintes hipóteses:

4.9.8.2.1 Mudança em normativo legal relativo à continuidade de negócios no que tange a TI;

4.9.8.2.2 Mudança em normativos internacionais afetos à continuidade de negócios no que tange a TI;

4.9.8.2.3 Mudança e acréscimos de normativos ABNT inerentes ao PDSI;

4.9.8.2.4 Criação de novos normativos nacionais e/ou internacionais que venham a agregar dados e informações que possibilitem a melhora do PDSI;

4.9.8.2.5 Mudanças no PDTI e no PEI que afetem a Segurança da Informação;

4.9.8.2.6 Sempre que for solicitado pelo TJCE com base em mudanças estruturais/organizacionais/lógicas/físicas de seu ambiente computacional, que determinem alterações necessárias no PDSI para manter válido todos os planos e ações inerentes à continuidade de negócios do Tribunal providas pela TI.

4.9.9 ATIVIDADES DE APOIO:

4.9.9.1 PLANO DE TRABALHO com o detalhamento do escopo do planejamento e cronograma de execução;

4.9.9.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;

4.9.9.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

4.9.10 PRAZO DE ENTREGA:

4.9.10.1 O serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.9.10.2 Nas demais execuções na vigência do contrato: o serviço deverá ser executado em até 45 (quarenta e cinco) dias corridos contados a partir da emissão de Ordem de Serviço – OS;

4.10 DESCRIÇÃO DETALHADA PARA DIVULGAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

4.10.1 Esta etapa tem como objetivo a divulgação por meio de palestras, treinamento e cursos para os servidores e prestadores de serviço do TJCE, em todos os níveis hierárquicos, dos conceitos de Segurança da Informação e das Políticas de Segurança elaboradas para o TJCE.

4.10.2 A capacitação realizada pela CONTRATADA enfocará públicos diferentes, levando-se em consideração os 04 (quatro) seguintes tipos de usuários do TJCE: COLABORADORES (servidores e prestadores de serviço em geral), CORPO TÉCNICO DE TI, COMITÊ DE SEGURANÇA DA INFORMAÇÃO E ALTA ADMINISTRAÇÃO. As informações ofertadas a cada público, por ocasião das atividades de treinamentos/palestras/workshops, deverá passar por PRÉVIA AVALIAÇÃO DO TJCE e enfocar linguagem pertinente ao público-alvo das atividades.

4.10.3 Deverá ser montado um Plano de Divulgação e Treinamento, conforme os públicos acima indicados, sobre os conceitos gerais de Segurança da Informação e de ações que serão realizadas por esta etapa.

4.10.3.1 A divulgação deverá levar em consideração o emprego de recursos visuais para colocação nas áreas internas do TJCE, como folders, cartazes, papel de parede desktop, material na Intranet;

4.10.3.2 O plano deverá contemplar a montagem da Semana da Segurança da Informação e a estratégia de conteúdo a ser passado para conhecimento dos servidores e prestadores de serviço do TJCE;

4.10.3.3 Também, o plano deverá considerar um Seminário de Segurança da Informação para os Colaboradores do Departamento de Informática, visando capacitar tais colaboradores nas práticas de segurança da informação do TJCE;

4.10.3.4 Deverá ser incluído no plano os demais treinamentos que serão empregados ao Corpo Técnico, ao Comitê de Segurança da Informação e à alta Administração;

4.10.4 Os Instrutores das palestras e dos treinamentos deverão ser profissionais certificados e capacitados OFICIALMENTE por instituições reconhecidas pelo MEC e/ou por instituições reconhecidas pelo mercado nacional e/ou internacional no quesito Segurança da Informação e com conhecimento dos serviços do TJCE;

4.10.5 A Contratante resguardar-se-á do direito de acompanhar e avaliar a capacitação, com instrumento próprio, e caso a Contratada não atinja os requisitos mínimos da Contratante, a Contratada deverá reestruturar a capacitação para atingir estes objetivos, sem nenhum custo adicional à Contratante;

4.10.6 Deverá ser realizada a Semana da Segurança da Informação com palestras para o público de servidores e prestadores de serviço em geral do TJCE em Auditório:

4.10.6.1 Cada palestra deverá ter duração mínima de 1hr (uma hora), sendo no período da manhã

e/ou no período da tarde, visando facilitar a presença de todos;

4.10.6.2 Prever, em seu planejamento, um total de 10 (dez) palestras para o período da Semana da Segurança da Informação;

4.10.6.3 O conteúdo da palestra deverá contemplar no mínimo:

Item	Palestra
1	Política de segurança da informação do TJCE, com base em conhecimento técnico da CONTRATADA bem como em normas de segurança da informação do TJCE JÁ REVISADAS PELA CONTRATADA. Conteúdo programático: Gestão de segurança da Informação; Classificação segura da informação; Áreas de segurança e prevenção de acessos não autorizados; Proteção contra software malicioso; Correio eletrônico do TJCE; Utilização da Internet; Tratamento de incidentes de segurança da informação; Troca de informações e softwares do TJCE entre os agentes internos e externos do Tribunal; Responsabilidades dos usuários; Acesso seguro aos sistemas operacionais.
2	Manuseio seguro de informações, com base em conhecimento técnico da CONTRATADA bem como em conteúdo programático abaixo. Conteúdo programático mínimo: Ameaças; Backup (cópia de segurança); Ciclo de Segurança; Medidas de Segurança; Riscos; Vulnerabilidades; Códigos maliciosos; Requisitos legais; Incidentes de segurança; Ambiente de trabalho; Antivírus; Controle de acesso; Direitos de privacidade; Direitos de propriedade intelectual; Estação de trabalho: Mesa limpa e tela limpa; Senha seguras; Identificação e autenticação; Golpes virtuais e fraude eletrônica; Segurança em computadores pessoais; Uso de crachá; Vídeos de segurança da informação. A empresa contratada poderá inserir, além dos temas acima observados, outros temas pertinentes e atuais à época das palestras para complementar/completar este tópico.

4.10.6.4 As turmas das palestras não deverão ser limitadas na quantidade de ouvintes, respeitando-se apenas a capacidade máxima suportada pelas instalações físicas do local de realização;

4.10.6.5 A Empresa deverá preparar e fornecer a versão eletrônica do material nos formatos *CAD e PDF* para divulgação interna no TJCE, como folders, cartazes, papel de parede desktop, conteúdo de Intranet. Caberá ao TJCE a impressão e distribuição de qualquer material no formato físico.

4.10.6.6 A Empresa deverá preparar e fornecer material didático informativo a ser distribuído aos participantes das palestras;

4.10.6.7 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o desenvolvimento das palestras, assim como também controlar e registrar as presenças.

4.10.6.8 A empresa deverá produzir e fornecer Certificado de participação das palestras para cada um dos participantes da Semana da Segurança da Informação;

4.10.7 Ao Corpo Técnico de TI, colaboradores do Departamento de Informática em geral, deverá ser realizado um Seminário de Segurança da Informação contemplando um conjunto de palestras de conteúdo específico e diferenciado para capacitação desse público:

4.10.7.1 O Seminário deverá ocorrer em, pelo menos, 03 (três) dias com palestras na manhã e/ou à tarde, em Auditório, envolvendo os seguintes tópicos:

4.10.7.1.1 Política de Segurança da Informação e Comunicações (PSIC) do TJCE;

4.10.7.1.2 Gestão de riscos em Segurança da Informação;

4.10.7.1.3 Tratamento e resposta a incidentes de Segurança da Informação;

4.10.7.1.4 Guia de desenvolvimento seguro de aplicações;

4.10.7.1.5 Modelo de gestão de Segurança da Informação;

4.10.7.1.6 Plano de recuperação de desastres em ambiente computacional;

4.10.7.1.7 Plano Diretor de Segurança da Informação;

4.10.7.1.8 Normativos Federais/Estaduais;

4.10.7.1.8.1 Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário;

4.10.7.1.8.2 Decreto no 3.505, de 13 de junho de 2000;

4.10.7.1.9 Normativos ABNT;

4.10.7.1.9.1 ABNT NBR ISO Guia 73:2005; ABNT NBR ISO/IEC 15408, Nível 2 e 3; ABNT NBR ISO/IEC 27005:2008; ABNT NBR ISO/IEC 27001:2006; ABNT NBR ISO/IEC

27002:2005; ABNT NBR 15999:2007, Parte 2: Requisitos - ABNT NBR 15999-2:2008 e ABNT NBR ISO 22301:2013;

4.10.7.1.10 Lei de Acesso à Informação, Lei nº 12.527, de 18 de novembro de 2011;

4.10.7.2 As turmas das palestras deverão ser formatadas para atender a um público de no mínimo 50 (cinquenta) participantes;

4.10.7.3 Nos intervalos entre as palestras deverá ser realizado coffee-break;

4.10.7.4 A Empresa deverá preparar e fornecer material para divulgação interna no TJCE, como folders, cartazes, papel de parede desktop, conteúdo de Intranet;

4.10.7.5 A Empresa deverá preparar e fornecer material didático com conteúdo do Seminário aos participantes;

4.10.7.6 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o desenvolvimento das palestras, assim como também controlar, registrar as presenças e apresentar ao TJCE o resultado do comparecimento dos colaboradores da SETIN para avaliação do Tribunal;

4.10.7.7 A empresa deverá produzir e fornecer Certificado de participação das palestras para cada um dos Técnicos participantes do Seminário;

4.10.7.8 A Empresa deverá produzir e fornecer questionários aos participantes dos eventos com a finalidade de se verificar a didática e qualidade das informações repassadas aos alunos. Estes formulários serão, após devido recolhimento e parametrização pela Contratada, entregues ao TJCE, onde este (TJCE) irá verificar a qualidade do serviço realizado. Caso, comprovadamente (com base nas respostas dos referidos questionários), a empresa não consiga repassar os conhecimentos propostos, esta deverá realizar, por suas custas, novo treinamento. Para aceitação e recebimento do treinamento pelo Tribunal, a Contratada deverá demonstrar índice de satisfação da turma treinada na casa de 70%, obtida por meio do computo total (resultado) das perguntas realizadas;

4.10.8 Ao Corpo Técnico de TI deverão ser realizados treinamentos específicos sobre normativos da ABNT assim como boas práticas em segurança da informação.

4.10.8.1 Os treinamentos estão relacionados na tabela a seguir e o seu conteúdo programático.

Item	Treinamento	Quantidade Técnicos	Carga Horária Mínima
1	Gestão de continuidade de negócios, com base em conhecimento técnico da CONTRATADA bem como nas normas ABNT NBR 15999-1:2007, ABNT NBR 15999-2:2008 e ABNT NBR ISO 22301:2013	10	16
2	Sistemas de gestão de segurança da informação, com base em conhecimento técnico da CONTRATADA bem como nas normas ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005.	10	16
3	Gestão de riscos em TI, com base em conhecimento técnico da CONTRATADA bem como na norma ABNT NBR ISO/IEC 27005:2008 e ABNT NBR ISO/IEC Guia 73:2005	10	16
4	Diretrizes para gestão da segurança da informação, com base em conhecimento técnico da CONTRATADA bem como nas normas ABNT NBR ISO/IEC 27002:2005, ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27011:2009.	10	16

4.10.8.2 Os horários para início e fim dos treinamentos serão conforme disponibilidade do Corpo Técnico do DEINF, em períodos matutinos, vespertinos ou noturnos - 4hrs/dia;

4.10.8.3 Nos intervalos dos cursos deverá ser realizado coffee-break;

4.10.8.4 Empresa deverá preparar e fornecer material didático com conteúdo dos cursos aos participantes;

4.10.8.5 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o desenvolvimento dos cursos, assim como também controlar e registrar as presenças;

4.10.8.6 A Empresa deverá produzir e fornecer questionários aos participantes dos eventos com a finalidade de se verificar a didática e qualidade das informações repassadas aos alunos. Estes formulários serão, após devido recolhimento e parametrização pela Contratada, entregues ao TJCE, onde este verificará a qualidade do serviço realizado. Caso, comprovadamente (com base nas respostas dos referidos questionários), a empresa não consiga repassar os conhecimentos propostos, esta deverá realizar, por suas custas, novo treinamento. Para aceitação e recebimento do treinamento pelo Tribunal, a Contratada deverá demonstrar índice de satisfação da turma

treinada na casa de 70%, obtida por meio do computo total (resultado) das perguntas realizadas;

4.10.8.7 A Empresa deverá produzir e fornecer Certificado de participação dos cursos para cada um dos Técnicos participantes.

4.10.9 Para os integrantes do Comitê de Segurança da Informação do TJCE, deverão ser realizados treinamentos específicos sobre normativos da ABNT assim como de práticas de segurança da informação.

4.10.9.1 Os treinamentos estão relacionados na tabela a seguir e o conteúdo programático está descrito abaixo.

Item	Treinamento	Carga Horária Máxima
1	Sistemas de gestão de segurança da informação, com base em conhecimento técnico da CONTRATADA bem como nas normas ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005.	08

4.10.9.2 Os horários para início e fim dos treinamentos serão conforme disponibilidade dos responsáveis do TJCE, em períodos matutinos, vespertinos ou noturnos – 4hrs/dia;

4.10.9.3 Nos intervalos dos cursos deverá ser realizado coffee-break;

4.10.9.4 A Empresa deverá preparar e fornecer material didático com conteúdo dos cursos aos participantes;

4.10.9.5 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o desenvolvimento dos cursos, assim como também controlar e registrar as presenças;

4.10.9.6 A Empresa deverá produzir e fornecer questionários aos participantes do evento com a finalidade de se verificar a didática e qualidade das informações repassadas aos alunos. Estes formulários serão, após devido recolhimento e parametrização pela Contratada, entregues ao TJCE, onde este verificará a qualidade do serviço realizado. Caso, comprovadamente (com base nas respostas dos referidos questionários), a empresa não consiga repassar os conhecimentos propostos, esta deverá realizar, por suas custas, novo treinamento. Para aceitação e recebimento do treinamento pelo Tribunal, a Contratada deverá demonstrar índice de satisfação da turma treinada na casa de 70%, obtida por meio do computo total (resultado) das perguntas realizadas;

4.10.9.7 A Empresa deverá produzir e fornecer Certificado de participação dos cursos para cada um dos Técnicos participantes.

4.10.10 Para a alta Administração e demais Autoridades indicadas, deverá ser realizado Workshop sobre Política de Segurança desenvolvida para o Tribunal assim como de boas práticas de segurança da informação.

Item	Treinamento	Carga Horária Máxima
1	Workshop sobre Política de Segurança desenvolvida para o Tribunal assim como de boas práticas de segurança da informação.	04

4.10.10.1 Os horários para início e fim do Workshop será conforme disponibilidade dos responsáveis do TJCE, em períodos matutinos, vespertinos ou noturnos, em períodos de expediente alternados ou contínuos;

4.10.10.2 O Instrutor do Workshop deverá ser profissional capacitado OFICIALMENTE por instituições reconhecidas pelo MEC e/ou por instituições reconhecidas pelo mercado nacional e/ou internacional no quesito Segurança da Informação e com a seguinte qualificação:

4.10.10.2.1 Prova do Registro na Ordem dos Advogados do Brasil – OAB;

4.10.10.2.2 Experiência acadêmica na área de Direito Eletrônico comprovada através de Certificados fornecidos pela instituição de ensino promotora do curso no qual foram ministradas as aulas;

4.10.10.2.3 Deverá possuir publicações na área de direito eletrônico. A comprovação de publicações deverá ser efetuada mediante a apresentação de exemplar integral (original ou cópia de boa qualidade) em que conste claramente o nome do profissional e o ISBN. Não serão aceitas publicações em mídia eletrônica;

4.10.10.2.4 Apresentação de atestado de capacidade técnica, fornecida por Pessoa Jurídica de Direito público, em nome do profissional, comprovando que prestou serviço de característica técnicas semelhantes ao objeto licitado fazendo uso de cópia de propriedade da proponente da norma ABNT NBR ISO IEC 17799:2005;

4.10.10.3 A Empresa deverá preparar e fornecer material didático com conteúdo dos cursos aos participantes;

4.10.10.4 A Empresa deverá providenciar todos os recursos audiovisuais necessários para o

desenvolvimento dos cursos, assim como também controlar e registrar as presenças;

4.10.10.5 Empresa deverá produzir e fornecer questionários aos participantes do evento com a finalidade de se verificar a didática e qualidade das informações repassadas aos alunos. Estes formulários serão, após devido recolhimento e parametrização pela Contratada, entregues ao TJCE, onde este verificará a qualidade do serviço realizado. Caso, comprovadamente (com base nas respostas dos referidos questionários), a empresa não consiga repassar os conhecimentos propostos, esta deverá realizar, por suas custas, novo treinamento. Para aceitação e recebimento do treinamento pelo Tribunal, a Contratada deverá demonstrar índice de satisfação da turma treinada na casa de 70%, obtida por meio do computo total (resultado) das perguntas realizadas;

4.10.10.6 A Empresa deverá produzir e fornecer Certificado de participação dos cursos para cada um dos Responsáveis do TJCE participantes.

4.10.11 Descrição do conteúdo programático dos treinamentos técnicos:

4.10.11.1 Gestão de continuidade de negócios:

4.10.11.1.1 Interpretação da Norma ABNT 15999:2007, Parte 2: Requisitos - ABNT NBR 15999-2:2008 e ABNT NBR ISO 22301:2013, contemplando no mínimo: visão geral da gestão de continuidade de negócios (GCN); A política de gestão de continuidade de negócios; Gestão do programa de GCN; Entendendo a organização; Determinando a estratégia de continuidade de negócios; Desenvolvendo e implementando uma resposta de GCN; Testando, mantendo e analisando criticamente os preparativos de GCN; Incluindo a GCN na cultura da organização; Planejamento do SGCN; Implementação e operação do SGCN; Monitoração e análise crítica do SGCN;- Manutenção e melhoria do SGCN;

4.10.11.2 Sistemas de gestão de segurança da informação:

4.10.11.2.1 Interpretação da Norma ABNT NBR ISO/IEC 27001:2006, contemplando no mínimo: Visão Geral das normas NBR ISO/IEC 27001 e NBR ISO/IEC 17799; Conceitos: informação, segurança da informação, ativos, confidencialidade, integridade, disponibilidade, vulnerabilidades, ameaças, impactos, probabilidade; Conceitos: riscos de segurança, processos de avaliação e tratamento do risco, sistema de gestão, sistema de gestão de segurança da informação; Interpretação das cláusulas: 0, 1, 2, 3 da NBR ISO/IEC 27001:2006; Interpretação das cláusulas: 4 /4.1, 4.2/ 4.2.1, 4.2.2, da NBR ISO/IEC 27001:2006; Interpretação das cláusulas: 4.2.3, 4.2.4, 4.3/ 4.3.1, 4.3.2, 4.3.3 da NBR ISO/IEC 27001:2006; Interpretação das cláusulas: 5, 6, 7 e 8 da NBR ISO/IEC 27001:2006; Visão Geral do Anexo A - objetivos de controle; Anexo A - Controles detalhados do A5 ao A9; Anexo A - Controles detalhados do A10 ao A12;

4.10.11.2.2 Interpretação da Norma ABNT NBR ISO/IEC 27002:2005, contemplando no mínimo: Visão geral das normas NBR ISO/IEC 27002 e NBR ISO/IEC 27001, apresentação do processo de exame do EXIN; Informação, objetivos do negócio e requisitos de qualidade - Formas, sistemas, valor da informação, disponibilidade, integridade e confidencialidade, análise da informação, gestão da informação; Conceitos de riscos e ameaças para segurança da informação - Tipos de ameaças, danos e riscos, medidas para redução de risco, guia para implementação de medidas de segurança; Ativos da informação e incidentes de segurança - O que são estes ativos e como gerenciá-los, sua classificação, papéis; Medidas físicas - Segurança física, anéis de proteção, alarmes, proteção contra incêndio; Medidas técnicas - Gerenciamento do acesso lógico, requisitos de segurança para sistemas de informação, criptografia, segurança de arquivos do sistema, vazamento de informação; Medidas organizacionais - Política de segurança, pessoal, gestão de continuidade do negócio, gestão das comunicações e processos de operação; Legislação e regulamentações - Observação de regulamentações, adequação, propriedade intelectual, proteção de documentos do negócio, de dados e confidencialidade de dados pessoais, prevenção contra abuso das instalações, cumprimento de política e padrões de segurança, medidas de monitoramento, auditorias, proteção de deficiências;

4.10.11.3 Gestão de riscos de segurança da informação:

4.10.11.3.1 Interpretação da Norma ABNT NBR ISO/IEC 27005:2008, contemplando no mínimo: Visão geral do processo de Gestão de Riscos de Segurança da Informação; Termos e definições; Conceitos relacionados com Gestão de Riscos de Segurança da Informação; Apresentação da organização da Norma; Análise/Avaliação de riscos de segurança da informação; Tratamento do risco de segurança da informação; Comunicação do risco de segurança da informação; Monitoramento e análise crítica de riscos de segurança da informação; Ferramentas para Gestão de Riscos;

4.10.11.4 Diretrizes para gestão da segurança da informação para organizações de telecomunicações:

4.10.11.4.1 Interpretação da Norma ABNT NBR 27011:2009, contemplando no mínimo: Termos e Definições Relacionados com Segurança da Informação; Segurança de Telecomunicações e

Legislação Especifica; Política de Segurança da Informação; Organizando a Segurança da Informação; Gestão de Ativos; Segurança em Recursos Humanos; Segurança Física e do Ambiente; Gerenciamento das Operações e Comunicações; Controle de Acesso; Aquisição, Desenvolvimento, e Manutenção de Sistemas de Informação; Gestão de Incidentes de Segurança da Informação; Gestão de Continuidade de Negócios; Conformidade; Conjunto de Controles Extendidos para Telecomunicações; Diretrizes Adicionais de Implementação;

4.10.12 A reprodução de todo o material de divulgação e de todo o material didático necessário à execução dos cursos e das palestras será de responsabilidade da Contratada;

4.10.13 As dependências físicas (Auditório, Salas) realização para os cursos e palestras serão de responsabilidade do TJCE.

4.10.14 Os cursos e palestras deverão ser teóricos, sem a necessidade de utilização de equipamentos de informática pelos Participantes.

4.10.15 PRODUTOS ESPERADOS:

4.10.16 Plano de Divulgação e Treinamento;

4.10.17 As palestras da Semana da Segurança da Informação para os servidores e prestadores de serviço em geral do TJCE, acompanhado de todo o material de divulgação e didático;

4.10.18 As palestras do Seminário de Segurança da Informação para o Corpo Técnico de TI da SETIN, acompanhado de todo o material de divulgação, didático e certificados;

4.10.19 Os treinamentos do Corpo Técnico de TI, acompanhado de todo o material de divulgação, didático e certificados;

4.10.20 Os treinamentos para os integrantes do Comitê de Segurança da Informação do TJCE, acompanhado de todo o material de divulgação, didático e certificados;

4.10.21 O Workshop da alta Administração do TJCE e demais Autoridades indicadas, acompanhado de todo o material de divulgação, didático e certificados;

4.10.22 ATIVIDADES DE APOIO:

4.10.22.1 PLANO DE TRABALHO com o detalhamento do escopo da divulgação e cronograma de execução;

4.10.22.2 RELATÓRIOS DE ACOMPANHAMENTO do plano de trabalho;

4.10.22.3 APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada para a equipe do TJCE;

4.10.23 PRAZO DE ENTREGA:

4.10.23.1 O serviço deverá ser executado em até 60 (sessenta) dias corridos contados a partir da emissão de Ordem de Serviço – OS para o "Plano de Divulgação e Treinamento";

4.10.23.2 O prazo de entrega de cada capacitação e ou treinamento será definido na Ordem de Serviço – OS competente de acordo com disponibilidade das Equipes do TJCE;

Cláusula Quinta – Da Prestação dos Serviços

Os serviços a serem executados obedecerão às seguintes condições e peculiaridades:

5.1 Do Local:

5.1.1 TJCE: na Av. General Afonso Albuquerque Lima, S/N. - Cambeba CEP: 60822-325, Fortaleza-CE, na Secretaria de Tecnológica da Informação – SETIN.

5.2 Dos Prazos:

5.2.1 O fornecimento deverá ser executado a partir de notificação para fornecimento a ser emitida pelo TJCE posterior à assinatura do contrato;

5.2.2 Em até 15 (quinze) dias corridos a partir da data de emissão da notificação para fornecimento pelo TJCE, a empresa Contratada deverá efetuar inicialização de projeto;

5.2.3 Efetuada a inicialização do projeto, com o competente aceite de abertura do projeto, todos os serviços contemplados pelo Objeto deverão estar disponíveis para demanda do TJCE via emissão de Ordem de Serviços – OS;

5.2.4 O prazo para execução de cada serviço contemplado no Objeto é de acordo com a definição de "prazo de entrega" de cada subitem de serviço constante da "Descrição detalhada dos serviços";

5.3 Forma de Fornecimento:

5.3.1 Todo o fornecimento deverá estar de acordo com os critérios estabelecidos nos itens do Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014;

5.3.2 A Contratada deverá implementar rigorosa gerência de projeto, com observância às regras a seguir além de adotar a Metodologia de Gerenciamento de Projetos – MGP da SETIN;

5.3.3 Para a inicialização do projeto, a empresa Contratada deverá executar:

5.3.3.1 Atividades que serão realizadas nesta fase

5.3.3.2 Abertura do projeto: deverá ser elaborado e apresentado Termo de Abertura do Projeto;

5.3.3.3 Apresentação do escopo do serviço: deverá ser elaborado e apresentado Declaração de Escopo do Projeto;

5.3.3.4 Pré-planejamento do projeto: deverá ser elaborado e apresentado Plano de Gerenciamento do Projeto;

5.3.3.5 A Contratada deverá apresentar Cronograma de Execução, constando atividades, subatividades e marcos, contemplando todas as ações previstas para a execução dos serviços, datas de entrega de documentação, datas das reuniões de ponto de controle, dentre qualquer outro evento que se julgar relevante e necessário;

5.3.3.6 Em até 07 (sete) dias consecutivos após emissão da ordem de fornecimento, a Contratada deverá agendar reunião ("kick-off meeting") junto aos responsáveis técnicos da Contratante, objetivando dar início ao acompanhamento da execução do Contrato;

5.3.3.7 Na reunião de "kick-off", a Contratada deverá apresentar sua equipe de trabalho, composta, no mínimo, por 01 (um) Gerente de Projeto e Equipe de Técnicos Especialistas;

5.3.3.8 Para apoio ao Gerente de Projeto, deverão ser alocados todos os técnicos necessários para a execução dos serviços;

5.3.3.9 Caberá ao Gerente de Projeto coordenar e orientar todo o processo de planejamento e execução dos serviços do Contrato, respeitando os prazos estabelecidos, atestando a qualidade dos produtos entregues e serviços executados;

5.3.3.10 Deverá ser elaborada e apresentada Lista de Contatos do Projeto;

5.3.3.11 Definição das regras para execução do serviço;

5.3.3.12 Definição das responsabilidades de cada um dos envolvidos;

5.3.4 A contar da 1ª reunião do projeto, deverão ser executadas reuniões periódicas de controle do projeto ("Status do Projeto") entre as equipes técnicas envolvidas, onde o Gerente de Projeto posicionará os responsáveis do CONTRATANTE sobre o andamento do projeto e apresentando os documentos pertinentes;

5.3.5 As reuniões de status poderão ser realizadas semanalmente, quinzenalmente ou conforme a demanda, a critério da CONTRATANTE;

5.3.6 O Gerente será responsável pela elaboração e entrega de relatórios de progresso e ou situação do projeto ("Relatório de Acompanhamento"), onde deverão ser descritas as atividades pertinentes ao período, além de destacar as pendências e solicitações de mudança do projeto, dentre outros tópicos;

5.3.7 Os relatórios de progresso e ou situação do projeto deverão ser fornecidos por período, semanalmente, quinzenalmente ou conforme a demanda, a critério da CONTRATANTE;

5.3.8 Todas as reuniões do projeto deverão ser registradas em "Ata", a qual será de inteira responsabilidade do Gerente;

5.3.9 As atas deverão ser entregues em no máximo 48 (quarenta e oito) horas após a realização da reunião para verificação e revisão por parte do TJCE, para posterior emissão de aceite por ambas as partes;

5.3.10 Após a apresentação e aprovação dos documentos relacionados ao plano de projeto, a equipe do projeto dará início às demais Fases do cronograma;

5.3.11 Produtos da fase para entrega ao TJCE:

5.3.11.1 Documentação inicial do projeto, incluindo termo de abertura, declaração de escopo, plano de gerenciamento, cronograma de trabalho, matriz de responsabilidade e lista de contatos dos participantes;

5.3.11.2 Documentos de acompanhamento do projeto, incluindo relatórios de situação e atas de reunião;

5.3.11.3 Termo de Aceitação;

5.4 O TJCE oficializará a demanda dos serviços por meio da emissão de uma "Ordem de Serviço – OS", conforme:

5.4.1 A execução será sempre precedida da emissão pelo TJCE da competente "Ordem de Serviço – OS", contendo no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço e produtos esperados;

5.4.2 A "Ordem de Serviço – OS" será emitida, assinada e autorizada pelo Fiscal do Contrato;

5.4.3 Toda "Ordem de Serviço – OS" deverá ser assinada pelo Gerente do Projeto / Preposto,

representante da CONTRATADA perante o TJCE, declarando a concordância da CONTRATADA em executar as atividades descritas na “Ordem de Serviço – OS”, de acordo com as especificações estabelecidas pelo TJCE;

5.4.4 Os serviços deverão estar sempre de acordo com as especificações constantes nas “Ordens de Serviços – OS”;

5.4.5 O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução – quando a “Ordem de Serviço – OS” é emitida pelo TJCE, durante a execução – com o acompanhamento e supervisão de responsáveis do TJCE, e ao término da execução – com o fornecimento de “Relatório de Serviços” pela Contratada e atesto dos mesmos por responsáveis do TJCE;

5.4.6 Todos os serviços prestados pela Contratada deverão ser necessariamente documentados (passo-a-passo), registrados e entregues ao TJCE pela mesma, em cópias impressas e gravadas em meio magnético, complementarmente ao “Relatório de Serviços”;

5.4.7 A partir da emissão da “Ordem de Serviço – OS”, a Contratada terá até 07 (sete) dias corridos para iniciar a sua execução, ressalvados os casos em que comprovadamente seja necessário um agendamento dos trabalhos;

5.5 Do Recebimento

5.5.1 O objeto será dado como recebido de acordo com os artigos 73 a 76 da Lei 8.666/93, conforme abaixo informado:

5.5.1.1 Provisoriamente, em até 5 (cinco) dias, a partir da entrega do serviço ou fornecimento do produto, para efeito de posterior verificação de sua conformidade;

5.5.1.2 Definitivamente, em até 10 (dez) dias úteis, a partir do recebimento provisório e após minuciosa verificação e avaliação dos serviços executados;

5.5.2 Para aceite do recebimento e posterior encaminhamento ao pagamento, deverão ser apresentados os seguintes documentos:

5.5.2.1 Ordem de Serviços emitida e assinada, Relatório de Serviços e demais Documentos Técnicos pertinentes e comprobatórios de execução do serviço;

5.5.3 Independentemente da aceitação no recebimento, a Contratada deverá garantir a qualidade do serviço executado pelo prazo estabelecido nas especificações e nas condições constantes do Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014, obrigando-se a corrigir aquele que apresentar inconsistência no prazo estabelecido pelo TJCE.

5.5.4 O pagamento será efetuado com apresentação da(s) respectiva(s) Nota(s) Fiscal(is) / Fatura(s), uma vez que tenham sido cumpridos, no que couber, todos os critérios estabelecidos neste Contrato, acompanhado dos documentos de aceite de cada tipo de serviço e conforme eventos a seguir relacionados:

5.5.4.1 Dos serviços: na conclusão ou encerramento de cada ciclo de atendimento ou da OS;

5.5.5 Os Fiscais do Contrato verificarão a conformidade dos serviços e/ou da entrega e da documentação requerida e, no caso de estarem conformes, atestará a Nota Fiscal e encaminhará para pagamento. No caso de não estarem conformes, as devolverá, com as ressalvas devidas, no prazo de até 10 (dez) dias da apresentação, para a Contratada providenciar a sua conformidade e novo encaminhamento para o TJCE.

5.5.6 No caso dos serviços e/ou entregas em não conformidade, a contagem dos prazos aqui estabelecidos será reiniciada a contar da data do saneamento das ressalvas pela Contratada, devidamente certificadas pelo Fiscal do Contrato.

5.5.7 O TJCE rejeitará, no todo ou em parte, os serviços e fornecimentos executados em desacordo com o disposto no Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014. Se, após o recebimento provisório, constatar-se que os serviços e fornecimentos foram executados em desacordo com o especificado, com defeito ou incompleto, os responsáveis do TJCE notificarão, por escrito, à Contratada, interrompendo-se os prazos de recebimento e ficando suspenso o pagamento até que seja sanada a situação.

5.5.8 Em caso de produto entregue em desconformidade com o especificado, será determinado um prazo, pelo TJCE, para que a Contratada faça a correção, sendo emitido pelo TJCE “Termo de Recusa do Serviço”. Este prazo iniciar-se-á a partir da data da emissão do mencionado termo de recusa. A Contratada ficará obrigada a substituir, às suas expensas, o item do objeto que for recusado.

5.5.9 Os valores da(s) NF(s) / Fatura(s) deverão ser os mesmos consignados na Nota de Empenho, sem o que não será liberado o respectivo pagamento. Em caso de divergência, será estabelecido prazo para a Contratada fazer a substituição desta(s) NF(s) / Fatura(s).

5.5.10 São critérios de mensuração dos serviços prestados para controle dos fornecimentos e dos pagamentos:

Item	Métrica	Indicador	Valor

Serviços técnicos	Unidade	Serviço Especificado na OS	100% executado
Transferência de conhecimento	Participantes	Conhecimento atualizado	100% prestado

Cláusula Sexta – Dos Preços e Condições de Pagamento

A CONTRATANTE pagará à CONTRATADA, pelos serviços prestados, o valor global de R$_____ (_____), referente aos serviços descritos no Anexo_____ deste Contrato.

Parágrafo Primeiro – O fornecimento do software poderá ser faturado após a solicitação de pagamento por parte da CONTRATADA e entrega/aceite dos documentos comprobatórios (entregáveis) dos mesmos. A aceitação será formalizada, pela CONTRATANTE, através da emissão do Termo de Recebimento Definitivo (TRD) ou documento similar;

Parágrafo Segundo – Os serviços poderão ser faturados após a solicitação de pagamento por parte da CONTRATADA e entrega/aceite dos documentos comprobatórios (entregáveis) dos mesmos. A aceitação será formalizada, pela CONTRATANTE, através da emissão do Termo de Recebimento Definitivo (TRD) ou documento similar;

Parágrafo Terceiro – As notas fiscais deverão ser emitidas em nome do Fundo de Especial de Reaparelhamento e Modernização do Judiciário – FERMOJU, CNPJ nº. 41.655.846/0001-47;

Parágrafo Quarto – O pagamento referente ao fornecimento e aos serviços serão realizados através de depósito bancário nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias corridos contados do recebimento do documento fiscal previamente assinado pelas unidades responsáveis pelo contrato;

Parágrafo Quinto – O Tribunal de Justiça reserva-se o direito de recusar o pagamento, no ato da ATESTAÇÃO, caso o objeto não esteja em conformidade com as condições deste instrumento;

Parágrafo Sexto – Nenhum pagamento será efetuado à CONTRATADA na pendência de qualquer uma das situações abaixo especificadas, sem que isso gere direito a alteração de preços ou compensação financeira: Apresentação da Certidão Negativa de Débito da Previdência Social – CND; Apresentação de Certidão Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida Ativa da União; Apresentação de Certidão Negativa de Débitos junto aos Governos Estadual e Municipal; Apresentação de Certificado de Regularidade do FGTS – CRF; Certidão Negativa de Débitos Trabalhistas.

Parágrafo Sétimo – Nenhum pagamento será efetuado à CONTRATADA antes de paga à multa que por ventura lhe tenha sido aplicada;

Parágrafo Oitavo – Caso existam penalidades a serem aplicadas a CONTRATADA será notificada, conforme especificado no item **MECANISMOS FORMAIS DE COMUNICAÇÃO** do Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014, sendo o prazo do atesto da respectiva ORDEM DE SERVIÇO interrompido até a entrega das justificativas pela CONTRATADA;

Cláusula Sétima – Dos Reajustes e dos Recursos Orçamentários

Os preços oferecidos serão fixos e irreajustáveis.

Parágrafo Único – As despesas decorrentes da execução deste Contrato correrão por conta do Fundo Especial de Reaparelhamento e Modernização do Judiciário – FERMOJU, tendo como Fonte dos Recursos – Recursos Diretamente Arrecadados, na seguinte dotação orçamentária:

04200001.02.061.500.21360.01.33903900.70.1.20

Cláusula Oitava – Da Vigência

O prazo de vigência deste contrato é de 24 (vinte e quatro) meses contados a partir da sua assinatura, permitindo efetuar o acompanhamento da execução do Plano Diretor de Segurança da Informação – PDSI no ciclo de sua operação de 04 (quatro) anos.

Cláusula Nona – Da Garantia Contratual

Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive pagamento de multas eventualmente aplicadas, a licitante prestará garantia no percentual de 5% (cinco por cento) do valor total do contrato, podendo a CONTRATADA optar por qualquer das modalidades previstas no art. 56 da Lei 8.666/93, a saber:

e) Caução em dinheiro ou títulos da dívida pública, cuja exigibilidade não seja contestada pelo TJCE;

f) Quando se tratar de caução em dinheiro, deverá ser recolhido na Secretaria de Finanças do

TJCE;

g) Seguro garantia;

h) Fiança bancária.

Parágrafo Primeiro - Em se tratando de fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil;

Parágrafo Segundo - Se o valor da garantia for utilizado em pagamento de qualquer obrigação, a CONTRATADA deverá re-integralizar o seu valor, no prazo não superior a 10 (dez) dias corridos, contados da data em que for notificada;

Parágrafo Terceiro - A não apresentação da garantia até a assinatura contratual significará recusa à assinatura do contrato, ensejando aplicação das sanções previstas;

Parágrafo Quarto – No caso de rescisão do contrato, a garantia se presta a cobrir prejuízos comprovados;

Parágrafo Quinto - A garantia ofertada deverá cobrir multas aplicadas, bem como obrigações trabalhistas e previdenciárias, não deverá ser proporcional ao tempo de vigência do contrato, garantindo sua totalidade durante todo o período de vigência. Não será aceita cláusula que preveja a realização do contrato por terceiros, bem como cláusula que preveja a subrogação da seguradora nos créditos da segurada. Deve, também, ser concedido pela seguradora, prazo mínimo de 30(trinta) dias para comunicação pelo TJCE das falhas cometidas pela segurada.

Cláusula Décima – Da Forma de Acompanhamento do Contrato

O acompanhamento e a fiscalização da execução do Contrato serão realizados por servidores do TJCE e designados como Fiscais do Contrato, os quais obedecerão às disposições de normas e resoluções internas do Tribunal, assim como o artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010.

Parágrafo Primeiro – Conforme alínea "a" do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, caberá à fiscalização providenciar elaboração do Plano de Inserção da contratada.

Parágrafo Segundo – Conforme alínea "b" do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, deverá ser realizada reunião inicial com participação dos Fiscais do Contrato, do Representante Legal da Contratada (apresentando o Preposto da mesma) e demais intervenientes identificados.

Parágrafo Terceiro – Conforme item 2 da alínea "b" do inciso I do artigo 25 da INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, entrega, por parte da Contratada, a pauta da reunião mencionada acima contemplará a entrega do Termo de Compromisso e do Termo de Ciência.

Parágrafo Quarto – É importante informar que o Termo de Referência – Anexo 01 do Edital de Pregão Eletrônico nº 03/2014 é fruto da sequência de trabalhos da etapa de Planejamento da Contratação conforme a INSTRUÇÃO NORMATIVA Nº 4 da SLTI/MPOG, de 12 de novembro de 2010, a qual dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional.

Parágrafo Quinto – Conforme a instrução normativa acima, os documentos de planejamento (Análise de Viabilidade, Plano de Sustentação, Análise de Riscos e Estratégia de Contratação) foram devidamente elaborados e se encontram aprovados.

Cláusula Décima Primeira – Da Metodologia de Avaliação da Qualidade

Todo o trabalho realizado pela CONTRATADA estará sujeito à avaliação técnica, sendo homologado quando estiver de acordo com o padrão de qualidade exigido pelo Órgão e de acordo com os prazos definidos;

Parágrafo Único - A documentação técnica gerada deverá seguir o padrão definido pelo TJCE ou pelo CONTRATANTE, sendo devidamente verificada por responsável técnico e atestada pelo Fiscal do Contrato.

Cláusula Décima Segunda – Das Sanções Administrativas

Pela inexecução total ou parcial do objeto definido neste Contrato, o TJCE poderá, garantida a prévia defesa, aplicar à Contratada, as sanções a seguir, de acordo com o grau do prejuízo causado pelo descumprimento das respectivas obrigações:

a) Advertência escrita quando se tratar de infração leve, a juízo da fiscalização, no caso de descumprimento das obrigações e responsabilidades assumidas no contrato ou ainda no caso

de outras ocorrências que possam acarretar prejuízos ao TJCE desde que não caiba a aplicação de sanção mais grave;

b) 0,3% (três décimos por cento) por dia sobre o valor dos serviços entregues com atraso, até o percentual de 9% (nove por cento) e mais 1% (um por cento) caso ultrapasse os 30 dias de atraso. Decorridos mais de 30 (trinta) dias de atraso o TJCE poderá decidir pela rescisão, em razão da inexecução total;

c) 1% (um por cento) por dia sobre o valor da garantia contratual, pela não apresentação/atualização, até o percentual de 10% (dez por cento) no prazo estabelecido neste instrumento, da garantia de execução contratual;

d) 0,5% (meio por cento) por evento sobre o valor global atualizado do contrato, pela não manutenção das condições de habilitação e qualificação exigidas no instrumento convocatório;

e) 10 % (dez por cento) sobre o valor do contrato, nas hipóteses de rescisão contratual por inexecução total do contrato;

f) Suspensão temporária de participar em licitação e impedimento de contratar com a Administração, pelo prazo não superior a 5 (cinco) anos;

g) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos que determinaram sua punição ou até que seja promovida a sua reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

Cláusula Décima Terceira – Da Rescisão

Constituem motivo para rescisão contratual:
a) O não cumprimento de cláusulas contratuais, especificações ou prazos;
b) O cumprimento irregular de cláusulas contratuais, especificações e prazos;
c) A lentidão do seu cumprimento, levando o Tribunal a comprovar a impossibilidade da execução do serviço, nos prazos estipulados;
d) O atraso injustificado no início dos serviços;
e) A paralisação dos serviços, sem justa causa e prévia comunicação ao Tribunal;
f) Não será permitida a subcontratação total ou parcial de qualquer item, a associação da CONTRATADA com outrem, a cessão ou transferência total ou parcial das obrigações contraídas, bem como a fusão, cisão ou incorporação da CONTRATADA, que afetem a boa execução do Contrato, sem prévio conhecimento e expressa autorização do Tribunal;
g) O desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a execução do Contrato, assim como as de seus superiores;
h) O cometimento reiterado de faltas na execução do Contrato, anotadas pelo Tribunal;
i) A decretação de falência ou a instauração de insolvência civil da CONTRATADA;
j) A dissolução da CONTRATADA;
k) A alteração social ou a modificação da finalidade ou da estrutura da CONTRATADA que prejudique a execução do Contrato;
l) Razões de interesse público, justificadas e determinadas, de alta relevância e amplo conhecimento, pela máxima autoridade do Tribunal, e exaradas no Processo Administrativo a que se refere este Contrato;
m) A não liberação, por parte do Tribunal, de área ou local para execução dos serviços, nos prazos contratuais;
n) A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do Contrato;
o) O descumprimento do disposto no Inciso V, do Artigo 27, da Lei 8.666/93, sem prejuízo das sanções cabíveis;
p) A rescisão do Contrato poderá ser determinada por ato unilateral e escrita do TJCE;
q) Este Contrato poderá ser rescindido por acordo entre as partes, mediante aviso prévio e escrito, desde que haja conveniência para o Tribunal, conforme previsto no Artigo 79, Inciso II da Lei 8666/93.
r) Poderá o Tribunal rescindir imediatamente este Contrato, sem qualquer ônus, no caso de persistência no inadimplemento de obrigações pela CONTRATADA, e pelas quais já tenha a mesma, sido notificada para providenciar as devidas regularizações.
s) O Contrato poderá ser rescindido a qualquer tempo, sem ônus de qualquer espécie, a exclusivo critério do Tribunal, desde que devidamente notificado, devendo este notificar a CONTRATADA de sua intenção rescisória, com antecedência mínima de 30 (trinta) dias corridos.

Cláusula Décima Quarta – Da Propriedade, Sigilo e Restrições

A contratada cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do art. 111, da Lei Federal N.º 8.666/93, combinado com o art. 4.º, da Lei Federal N.º 9.609/98, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência dos serviços contratados, entendendo-se por resultados quaisquer estudos, relatórios, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presenta contratação, em papel ou em mídia eletrônica;

Parágrafo Primeiro – Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a CONTRATADA, zelar por si, por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados;

Parágrafo Segundo – A obrigação assumida de Confidencialidade permanecerá válida durante o período de vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA, previstas no CONTRATO e na legislação pertinente;

Parágrafo Terceiro - Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados, a qualquer título, da equipe executante do Objeto deste Contrato, a assinatura do ANEXO 09 - TERMO DE COMPROMISSO, bem como a assinatura do ANEXO 08 – TERMO DE CIÊNCIA do Edital de Pregão Eletrônico nº 03/2014 onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.

Cláusula Décima Quinta – Da Legislação

Este contrato rege-se pela Lei nº 10.520/2002 e Lei nº 8.666/93, alterada pelas Leis nº 9.648/1998, nº 9.854/1999, legislação correlata, medidas provisórias, bem como pelos preceitos de Direito Público, regulamentos, instruções normativas e ordens de fornecimento, emanados de órgãos públicos, aplicando-se-lhes, supletivamente, nos casos omissos, os princípios gerais dos contratos e demais disposições de Direito Privado.

Cláusula Décima Sexta – Do Foro

Fica eleito o foro de Fortaleza (CE) para dirimir quaisquer dúvidas oriundas do presente Contrato, caso não possam ser resolvidas por via administrativa, com renúncia de qualquer outro por mais privilegiado que seja.

E, por estarem justos e acertados, firmam o presente em 02(duas) vias de igual teor e forma, nas presenças da(s) testemunha(s) que também o assinam, para que produza seus jurídicos e legais efeitos, devendo seu extrato ser publicado no Diário da Justiça.

Fortaleza, xx de xxxxxxxx de 2014.

_____

CONTRATANTE

_____

CONTRATANTE

_____

EMPRESA – CONTRATADA (ASSINATURA/CARIMBO)

Testemunhas: _____

_____