Syslog de outras plataformas.

4.2.12.3 Os agentes de coleta devem ser capazes de identificar e separar "relay logs" (servidores Syslog que recebem e repassam logs de várias outras fontes) de forma independente, garantindo uma correlação adequada.

4.2.12.4 A solução deve permitir o monitoramento e envio de alertas relativos a agentes que não estejam funcionando corretamente ou estejam inoperantes.

4.2.12.5 A solução deve operar usando agentes, com exceção dos dispositivos que geram logs usando o protocolo padrão Syslog.

4.2.13. A solução deve disponibilizar o uso da ferramenta *User Behavior Analytics* (UBA) em computadores de usuários determinados pelo TJCE, sem custo adicional e com regras pré-definidas e modificáveis.

4.2.14. Os coletores e logs devem fazer a compactação e criptografia dos dados antes do envio dos mesmos à nuvem do SIEM.

4.2.15. Quando coletando logs que estão hospedados na nuvem, a coleta deve ocorrer diretamente da nuvem da aplicação para a nuvem do SIEM, sem permitir que os logs passem pela infraestrutura do TJCE. Isso é válido desde que a solução em nuvem permita a coleta por meio de integrações via API. Qualquer questionamento de serviços em nuvem usados pelo TJCE poderão ser esclarecidos na Vistoria Técnica.

4.2.16. A solução deverá segregar logicamente os logs do TJCE dos demais logs de outras contratantes que utilizem a solução de SIEM SaaS na infraestrutura da CONTRATADA.

4.2.17. A solução deve ser monitorada para garantir disponibilidade e infraestrutura em tempo integral, 24 horas por dia, 7 dias por semana, durante todo o ano.

4.2.18. Se a solução consistir em módulos, eles devem ser fornecidos por um único fabricante para garantir suporte completo em relação a funcionalidades, integrações e compatibilidade de 100% com a solução. Como um dos requisitos da ferramenta SIEM para a assinatura do TRD de implantação, a CONTRATADA

deverá apresentar documentação fornecida pelo fabricante para comprovar a cobertura de garantia do fabricante relacionada com a funcionalidade da ferramenta SIEM.

4.2.19. A solução deve armazenar os logs por pelo menos 6 meses online, conforme diretrizes da PORTARIA No 162, DE 10 DE JUNHO DE 2021 do CNJ.

4.2.20. O armazenamento dos logs deve ser efetuado no território brasileiro pela CONTRATADA. Os logs não poderão trafegar por território fora do Brasil.

4.2.21. A coleta, normalização e correlacionamento dos eventos dos dispositivos monitorados devem ocorrer em tempo próximo ao real.

4.2.22. A fim de aprimorar a operação e a compreensão dos eventos, é obrigatório normalizá-los e categorizá-los em um único padrão que será utilizado pela solução.

4.2.23. A solução deve possibilitar a criação de metadados personalizados, permitindo a extração de dados existentes na linha de log (raw). Isso pode ser realizado por meio de recursos como expressões regulares ou interfaces gráficas dedicadas para essa finalidade.

4.2.24. Propriedades customizadas poderão ser utilizadas em regras de correlação online e histórica.

4.2.25. A solução deve possibilitar a agregação de eventos similares.

4.2.26. A solução deve atribuir uma métrica de prioridade tanto para os eventos quanto para os alertas/incidentes.

4.2.27. A solução deve ser capaz de gerar alertas/incidentes com base em regras predefinidas anteriormente.

4.2.28. A solução deve ter a capacidade de armazenar os eventos, incluindo aqueles normalizados, de forma compactada.

4.2.29. A solução deve possibilitar a análise de eventos com base em contexto, como usuários, localização geográfica e qualquer outro metadado presente nos eventos.

4.2.30. A solução deve fornecer painéis gráficos ou integração com painéis gráficos existentes no TJCE (dashboards), que apresentam indicadores de segurança, aplicações e monitoramento do SIEM.

4.2.31. Os painéis gráficos (dashboards) devem ser personalizáveis por usuário, permitindo a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução na interface web.

4.2.32. O Dashboard integrado deve:

4.2.32.1 Fornecer um painel que apresente uma visão consolidada das métricas de segurança dos ativos monitorados.

4.2.32.2 Permitir a personalização do painel, incluindo a adição de relatórios e métricas.

4.2.32.3 Realizar a análise dos eventos de segurança da informação em quase tempo real.

4.2.32.4 Assegurar a funcionalidade de análise por meio do drill-down, possibilitando a exploração detalhada a partir de um gráfico de visão geral, com a capacidade de descer aos diferentes níveis de análise conforme necessário.

4.2.32.5 Permitir o acesso da equipe do TJCE em qualquer momento.

4.2.33. Ter a capacidade de enviar e-mails ou mensagens via SMS contendo notificações sobre incidentes ou alertas.

4.2.34. A solução deve oferecer, no mínimo, os seguintes métodos de coleta de eventos: Syslog (UDP, TCP), Syslog com criptografia TLS, JDBC, SNMP (v1, v2 e v3), Registro de Eventos do Microsoft, Cliente MQ Series, Arquivos de Log em formato de texto, Kafka, Checkpoint OPSEC/LEA, CISCO NSEL e Protocolo Juniper NSM.

4.2.35. A solução deve ser capaz de encaminhar os logs e fluxos, em seu formato nativo, para outros sistemas de segurança da informação ou servidores Linux/Windows em tempo real.

4.2.36. A solução deve ser capaz de encaminhar eventos já normalizados para outros sistemas de correlação em tempo real.

4.2.37. A solução deve oferecer a capacidade de configurar a ofuscação de qualquer parte dos dados recebidos após a normalização. A configuração da ofuscação de dados

deve ser realizada por meio de chaves de criptografia.

4.2.38. A solução deve ser capaz de automatizar a resposta a incidentes, executando scripts como ação personalizada dentro das regras de correlação.

4.2.39. A solução deve permitir a personalização e customização de diversos modelos de e-mail que serão enviados como resposta aos incidentes identificados.

4.2.40. A solução deve ser capaz de processar logs no formato JSON, identificando e criando automaticamente os campos comuns do log como metadados para aquele tipo de log.

4.2.41. A solução deve permitir a criação de metadados com nomes personalizados, à escolha do administrador, e possibilitar a referência desses metadados em pesquisas e regras de correlação.

4.2.42. A solução deve permitir a personalização/definição de metadados para extrair dados de uma linha de log (raw), usando recursos como expressões regulares, JSON, LEEF e CEF, a partir de dados RAW previamente armazenados na solução de correlação, possibilitando o uso desses dados em pesquisas de eventos.

4.3. Características do coletor de logs do SIEM

4.3.1. A solução deverá oferecer a possibilidade da utilização de quantos coletores de eventos forem necessários de acordo com sua arquitetura de preferência (network appliance ou virtualização), desde que não gere impacto no desempenho (processamento, uso de memória, uso de armazenamento) nos ativos do TJCE.

4.3.2. Os coletores deverão comunicar-se com o SIEM da CONTRATADA através de VPN com tráfego criptografado.

4.3.3. Deverá possibilitar a compressão/compactação e criptografia dos dados para o envio dos logs à nuvem.

4.3.4. Deverá realizar a filtragem e seleção dos eventos a serem inseridos na solução ou mantidos na base de dados da solução, conforme períodos definidos previamente.

4.3.5. Deverá possibilitar a criação e modificação de políticas de retenção.

4.3.6. Deverá realizar a normalização e categorização dos eventos em um padrão único, que será utilizado pela solução.

4.3.7. Deverá oferecer suporte nativo para o reconhecimento e coleta de pelo menos 250 tipos distintos de fontes de dados.

4.3.8. Deverá processar eventos em formato comprimido (zip, gz, tar.gz) sem exigir descompressão manual.

4.3.9. Deverá realizar a agregação de eventos, exibindo a contagem de ocorrências quando o mesmo evento acontecer dentro de um período curto.

4.3.10. A possibilidade de efetuar a agregação de eventos deve ser configurável, permitindo escolher entre realizar ou não essa operação.

4.3.11. Deverá preservar o evento bruto (raw), juntamente com seus metadados para fins de armazenamento e consultas futuras.

4.3.12. Deverá ter a capacidade de agregar informações de localização geográfica dos endereços IP envolvidos no evento, a fim de utilizá-las na correlação.

4.3.13. Um único componente da solução deve ter a capacidade de coletar, processar e normalizar tanto os eventos de segurança quanto os eventos de negócio (não relacionados à segurança).

4.3.14. Os eventos de segurança e de negócios devem ser normalizados para um único padrão de eventos.

4.3.15. A solução deve oferecer suporte à integração de dispositivos ou logs que não são nativamente suportados.

4.3.16. A integração de logs ou dispositivos deve ser feita através da interface web, utilizando expressões regulares, JSON e recursos similares, sem definir de maneira obrigatória a utilização de linguagens de programação ou scripts, como Java, C, TCL/TK, PowerShell, Shell Scripts, entre outros.

4.3.17. A integração mencionada deve ser compatível com as seguintes formas de coleta de eventos:

4.3.17.1 Check Point OPSEC/LEA.

4.3.17.2 Kafka.

4.3.17.3 Arquivos de Log em Formato de texto.

4.3.17.4 Syslog (UDP, TCP).

4.3.17.5 Microsoft Event Log.

4.3.17.6 Juniper NSM Protocol.

4.3.17.7 SNMP (v1, v2 e v3).

4.3.17.8 CISCO NSEL.

4.3.17.9 Syslog criptografado com TLS.

4.3.17.10 PAN-OS XML

4.3.17.11 Common Event Format (CEF)

4.3.17.12 Outros formatos de logs presente nos ativos de rede do TJCE (switches, access point, etc).

4.3.18. A solução precisa ter suporte incorporado para, no mínimo, as seguintes fontes de logs:

4.3.18.1 Windows.

4.3.18.2 Linux.

4.3.18.3 IBM/AIX.

4.3.18.4 HP-UX, Solaris.

4.3.18.5 Oracle Database.

4.3.18.6 IBM/DB2.

4.3.18.7 PostgreSQL.

4.3.18.8 MS SQL Server.

4.3.18.9 Firewalls (Checkpoint, Cisco/ASA, Juniper, Fortinet, Hillstone, Huawei, Palo Alto e SonicWall).

4.3.18.10 Network IPS/IDS (Sourcefire, IBM/ISS, HP Tipping Point, Snort e McAfee).

4.3.18.11 Outras fontes de logs de tecnologias presentes na infraestrutura do TJCE.

4.3.19. A solução deve oferecer a capacidade de criar automaticamente data sources com base na detecção do tipo de fonte de log, a partir das opções nativamente suportadas e enviadas via Syslog.

4.3.20. A solução deve ter a capacidade de criar automaticamente data sources com base

na detecção do tipo de fonte de log, incluindo tipos de logs personalizados na solução, quando enviados via Syslog.

4.3.21. A solução deve ter suporte para IP overlap, ou seja, categorizar os eventos de forma que seja possível gerenciar eventos provenientes de fontes de log que estão em redes distintas, mas possuem o mesmo endereço IP.

4.4. Recursos de correlação de logs do SIEM.

4.4.1. Considera-se tempo de processamento "quase real" no receptor, ao processamento instantâneo da informação mais o atraso de tráfego de dados entre o emissor e o receptor.

4.4.2. A solução deve realizar a correlação de eventos provenientes das fontes de logs e flows, resultando na geração de incidentes de segurança.

4.4.3. A solução deve efetuar a correlação dos eventos em tempo quase real.

4.4.4. A solução deve efetuar a correlação dos flows em tempo quase real.

4.4.5. A solução deve oferecer a capacidade de criar regras inexistentes e editar as existentes.

4.4.6. A solução deve permitir a correlação de qualquer informação presente no evento, inclusive dados financeiros ou outras informações que não estejam relacionadas a endereçamento IP, portas, etc.

4.4.7. Oferecer um mínimo de 150 regras incorporadas, permitindo a criação ilimitada de novas regras ou personalização das regras incorporadas:

4.4.7.1 Ataques de força bruta com e sem sucesso.

4.4.7.2 Detecção de anomalias de comportamento baseado em estatísticas (Statistical Behavioral Analysis).

4.4.7.3 Infecção de equipamentos por vírus.

4.4.7.4 Comprometimento ou invasão de ativos da rede.

4.4.7.5 Anomalias de Logon: excessivas falhas de logon, logons fora do expediente, logons a partir de endereços IP não usuais.

4.4.7.6 Realização de ações suspeitas por parte de usuários privilegiados.

4.4.7.7 Detecção de padrões em logs observados e não observados.

4.4.7.8 Autenticações concorrentes de múltiplas regiões ou cidades com as mesmas credenciais (roubo de identidade).

4.4.7.9 Bloqueio de contas e password scans.

4.4.7.10 Ataques comuns em aplicações WEB, como XSS e SQL injection.

4.4.7.11 Ataques de negação de serviço (DoS e DDoS).

4.4.7.12 Identificação em tempo real e de maneira automatizada da origem dos eventos de segurança, identificando cidades, estados e países e não somente os endereços IP de origem.

4.4.7.13 Botnets, worms, DDoS e outros zero-day malwares, através do cruzamento dos logs de DNS, DHCP, web proxy e tráfego de rede.

4.4.8. As regras podem variar desde a detecção simples de thresholds até o uso de operadores lógicos comuns para correlacionar eventos distintos, possibilitando:

4.4.8.1 Permitir a utilização de thresholds estáticos ou dinâmicos.

4.4.8.2 Facilitar a execução de scripts automáticos em casos de incidentes.

4.4.8.3 Permitir a configuração de políticas de notificação com base na severidade do incidente, hora do dia e serviço.

4.4.8.4 Integrar a solução com a monitoração de capacidade e desempenho dos ativos gerenciados via SNMP.

4.4.9. A capacidade de autodetecção deve incluir:

4.4.9.1 Oferecer recursos mínimos de busca de eventos, incluindo: busca em tempo real utilizando palavras-chave semelhantes ao Google e consultas estruturadas semelhantes ao SQL, assim como ter a capacidade de converter os resultados da busca em relatórios ou widgets de painel.

4.4.10. A solução deve incluir regras de correlação específicas para regulamentações e conformidades aplicáveis ao TJCE, com suporte mínimo para PCI, ISO 27001 e GDPR ou LGPD.

4.4.11. A solução deve possuir um repositório que ofereça novas regras de correlação especializadas em segurança para atualização e expansão da capacidade de detecção de incidentes, sem custos adicionais.

4.4.12. A solução deve permitir a criação de regras que identifiquem mudanças de comportamento, como surtos ou ausência de eventos/tráfego, quando comparados a períodos semelhantes (por exemplo, mesmo período do dia, mesmo dia da semana).

4.4.13. A solução deve permitir a criação de regras que identifiquem desvios em qualquer metadado, em relação aos limites preestabelecidos.

4.4.14. A solução deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que ocorrem ao longo do tempo e não foram previstos ou observados anteriormente.

4.4.15. A solução deve integrar-se com ferramentas externas como Nslookup, Whois e Nmap.

4.4.16. A solução deve permitir o correlacionamento de eventos e alertas com dados existentes em listas de observação (watchlist), permitindo também a criação e edição automatizada e manual de listas.

4.4.17. A solução deve ser capaz de correlacionar eventos e fluxos de rede, como NetFlow, J-Flow, S-Flow e IPFIX, sem a necessidade de ferramentas de terceiros ou componentes adicionais ao licenciamento da solução.

4.4.18. A solução deve ser capaz de correlacionar eventos provenientes de múltiplas fontes, tipos ou localizações.

4.4.19. A solução deve ter a capacidade de priorizar os eventos e incidentes com base em critérios que incluem, pelo menos, severidade e criticidade/relevância do evento ou incidente. Deve ser possível utilizar uma combinação desses critérios para determinar a prioridade.

4.4.20. Os incidentes devem ser agrupados, no mínimo, de acordo com:

4.4.20.1 Endereço de origem.

4.4.20.2 Endereço de destino.

4.4.20.3 Categoria.

4.4.21. A solução deve ter, no mínimo, os seguintes tipos de correlação:

4.4.21.1 Extrapolação de um limite (threshold).

4.4.21.2 Correlação por anomalia e padrão de comportamento.

4.4.21.3 Correlação por regras.

4.4.22. Como resultado das regras, a solução deve ter a capacidade de realizar ações automáticas, no mínimo:

4.4.22.1 Enviar e-mail.

4.4.22.2 Enviar mensagem para o usuário conectado no console.

4.4.22.3 Criar um incidente no sistema de workflow interno.

4.4.22.4 Enviar traps SNMP e popular listas (watchlist).

4.4.23. A solução deve possuir a capacidade de se integrar com os principais sistemas de inteligência de ameaças de riscos globais e das soluções de segurança da informação presente no TJCE, tais como: PAN-DB, Tenable.io Threat Intelligenc, Kaspersky Threat Intelligence, HP ThreatLink (DVLabs), Symantec DeepSight, Verisign iDefense, IBM X-Force, etc.

4.4.24. A solução deve oferecer a flexibilidade de utilizar qualquer metadado dos eventos em regras de correlação.

4.4.25. A solução deve permitir testar as regras de correlação em eventos passados, com um período de tempo e escopo claramente definidos.

4.4.26. A correlação histórica deve fornecer a opção de escolher o período a ser analisado, com suporte mínimo para correlação de 1 dia, 7 dias e 30 dias.

4.4.27. As regras de correlação histórica devem processar logs e flows, gerando alertas quando os eventos/flows analisados corresponderem às especificações definidas na regra.

4.4.28. Uma regra de correlação deve ter a capacidade de correlacionar eventos de tipos e origens distintos, verificando situações como a sequência de eventos diferentes, a contagem de eventos e a ausência de um evento após a ocorrência de outro.

4.5. Recursos da console de administração e operação do SIEM.

4.5.1. A console de administração e operação deve ser configurada e operada pela CONTRATADA.

4.5.2. A console de consulta deve incluir a capacidade de classificar os eventos em geral

em três grupos distintos:

4.5.2.1 Eventos de auditoria (logins, logouts, erros de autenticação, etc.).

4.5.2.2 Eventos de Segurança (ataques, comprometimento, roubo de dados, fraudes, etc.).

4.5.2.3 Eventos de Operação (erros, eventos críticos de ativos e rede, etc.).

4.5.3. A console deve contar com as seguintes especificações:

4.5.3.1 Ter uma interface web única, via HTTPS, para administração, gerenciamento e operação do sistema como um todo, garantindo a confidencialidade dos dados.

4.5.3.2 Ter acesso controlado e autenticado por usuário.

4.5.3.3 Ter capacidade de integração com bases Microsoft Active Directory, LDAP, TACACS e RADIUS para autenticação de usuários.

4.5.3.4 Permitir a integração com Single Sign-On que suporte o protocolo SAML 2.0.

4.5.3.5 Garantir acesso aos dados e funcionalidades específicas por perfis de usuário.

4.5.3.6 O controle de acesso deve ser configurado na interface web, com capacidade para limitar os recursos da solução de acordo com os perfis de usuários definidos pelo administrador.

4.5.3.7 O controle de acesso deve ser configurado para permitir o acesso por perfil às funções de Administração, Incidentes, Configuração de Regras, atividades de Redes e Logs.

4.5.3.8 Permitir a visualização de eventos, flows de rede e incidentes de segurança em tempo quase real.

4.5.3.9 Permitir a pesquisa nos eventos históricos com base em metadados, oferecendo a capacidade de drill-down, ou seja, refinamento da pesquisa a partir da seleção de elementos no resultado para realizar uma nova pesquisa.

4.5.3.10 Disponibilizar a visualização dos eventos relacionados a um alerta e/ou

incidente de segurança identificado pelas regras de correlação da solução.

4.5.3.11 A solução deve permitir a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução.

4.5.3.12 Ter a capacidade de criar novos painéis gráficos (dashboards) e modificar os existentes.

4.5.3.13 Ter a capacidade de visualizar eventos de mais de um tipo de dispositivo na mesma visualização (exemplo: Firewall, Proxy e antivírus na mesma visualização).

4.5.3.14 Ter a capacidade de criar listas (watchlist) e alterar as existentes, permitindo a inserção dos dados de forma manual, por linha de comando e automática por meio das regras de correlação.

4.5.3.15 Permitir a remoção de dados das listas (watchlist) de forma manual, automática por meio das regras de correlação e por expiração do tempo de vida da informação.

4.5.3.16 Possuir a capacidade de gerenciar e configurar centralmente todas as partes distribuídas da solução.

4.5.3.17 Possuir a capacidade de atualizar os componentes da solução por meio da console central de administração.

4.5.3.18 Ter a capacidade de restaurar informações de cópia de segurança do banco de dados, configurações e dados que foram arquivados previamente pela solução.

4.5.3.19 Permitir a criação de novos tipos de eventos na ferramenta, a fim de integrar logs não suportados nativamente.

4.5.3.20 Permitir a associação manual de eventos já normalizados, mas ainda não categorizados/associados, às categorias, classificações ou tipos de eventos já existentes ou definidos pelo usuário.

4.5.3.21 Para análise dos eventos e flows de rede, é necessário ter suporte a

filtros de eventos, incluindo filtros simples, pesquisa de expressões e buscas avançadas diretamente na base de dados.

4.5.3.22 Deve oferecer APIs do tipo webservices, seguindo o padrão "RESTful API", para permitir o acesso externo à solução, possibilitando a busca de informações de eventos e flows, assim como a manipulação de incidentes.

4.5.3.23 Deve suportar o controle de acesso à solução com base em informações externas, validando atributos do usuário ou grupo a que ele pertence. Essa validação de autorização deve ser suportada em diretórios LDAP ou Windows Active Directory.

4.5.3.24 Deve fornecer uma API para a criação de fontes de logs (data sources) por meio de uma interface ReST, com o objetivo de automatização.

4.5.4. Os relatórios devem contar com as seguintes especificações:

4.5.4.1 Deve permitir a geração de relatórios, em quase tempo real, que englobem diversas informações em um único documento, como dados de segurança e rede.

4.5.4.2 Fornecer a funcionalidade de geração de relatórios de conformidade, abrangendo, pelo menos, SOX, PCI e ISO.

4.5.4.3 Deve ser permitido agendar a execução de relatórios em qualquer horário ou período, com a opção de enviar os resultados por e-mail.

4.5.4.4 Deve permitir a criação de relatórios relacionados a incidentes, logs, flows de rede e vulnerabilidades.

4.5.4.5 Deve organizar os relatórios em grupos temáticos, permitindo a criação de novos agrupamentos de relatórios pelos usuários.

4.5.4.6 Deve possibilitar a personalização de novos relatórios com base em dados de Logs, Flows de rede, Vulnerabilidades e Incidentes.

4.5.4.7 Deve gerar relatórios de eventos, alertas/incidentes em níveis técnico e gerencial, que podem ser exportados nos formatos PDF, HTML, XLS, CSV, XML e RTF/DOC.

4.5.4.8 Os usuários devem ter acesso apenas aos seus próprios relatórios ou aos relatórios disponibilizados por outros usuários. Os administradores devem ter acesso a todos os relatórios.

4.5.4.9 Deve ser possível definir perfis de usuários com permissões/restrições para editar os modelos de relatórios.

4.5.4.10 Deve ser possível gerar relatórios com base em dados que contenham endereços IPv6.

4.5.4.11 A funcionalidade de backup deve preservar os dados dos relatórios.

4.5.4.12 Deve permitir a geração de relatórios que incluam os eventos associados a um incidente detectado por regras de correlação.

4.5.4.13 Permitir classificar eventos de segurança: ataques, reconhecimento, malware, atividades suspeitas de rede ou usuários, etc.

4.5.4.14 Contar com a opção de incluir os TOP endereços lógicos de origem das ameaças, TOP países e cidades de origem das ameaças e dos alertas de segurança.

4.5.5. A CONTRATADA deverá garantir que terá acesso ao suporte do fabricante da tecnologia SIEM durante a vigência do contrato. Para isso, a CONTRATADA deverá apresentar um acordo de suporte direto com o fabricante, assegurando que terá acesso a especialistas qualificados para resolver dúvidas, consultas ou problemas de configuração relacionados à ferramenta SIEM.

4.6. Dimensionamento do SIEM.

4.6.1. Considerando os elementos listados na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE as seguintes ferramentas consultadas:

4.6.1.1 Planilha de cálculo de EPS da IBM baseada no preenchimento na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE, com estimativa final de demanda na faixa de 10.100 a 11.300 EPS.

Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE

Item	Tipo de equipamento	Qde.
1	Sistemas Núcleo de Alto Volume	2
2	Sistemas Núcleo de Médio Volume	3
3	Infraestrutura de Segurança Típica	2
4	Soluções de Autenticação	7
5	Soluções de Serviços de Rede	39
6	Soluções IaaS/PaaS	0
7	Soluções Núcleo SaaS	1
8	Soluções Anti-Malware	1
9	Soluções de Criptografia	1
10	Registros de Servidores Web/Email	264
11	Soluções de Gerenciamento de Inventário	1
12	Soluções de HIPS e Decepção	1
13	Soluções de Borda SaaS	0
14	Registros de Servidores	42
15	Registros de Estações de Trabalho/Hosts	9050
16	Sistemas de Rede	1275

4.6.1.2 Calculadora de EPS: https://teskalabs.com/products/logman.io/eps-calculator/ com demanda de 5.873 EPS, conforme mostrado abaixo:

TeskaLabs SIEM and Log Management EPS Calculator

Sizing your Log Management and SIEM solution right is important and not an easy task. The solution is to make an analysis of your infrastructure as it directly impacts your Log Management / SIEM and the storage required to operate it efficiently. The two key numbers are Events per Second (EPS) and Gigabytes per Day (GB/day) indicating the volume of data processed in your IT infrastructure.

The calculation is based on the number of types of devices (nodes) in your IT infrastructure, which includes servers, routers, switches, firewalls and other network devices and applications.

Events Per Second (EPS) define the number of events or processes that take place in a given time on any IT appliance in your IT infrastructure.

Log Sources	Count	EPS	Daily volume
Windows desktops	905(	45.25	18.1 GB
Windows Servers	7	28	1.7 GB
Linux Servers	10	30	716.8 MB
Application Firewalls	1	30	716.8 MB
Network Firewalls	2	320	6.0 GB
Network Routers	2	2	41.0 MB

Network Switches	625	1250	12.5 GB
Network Flows	0	0	0.0 GB
Network Wireless LAN	650	3250	39.0 GB
Network Load Balancers	1	5	61.4 MB
Network IPS/IDS	1	100	2.4 GB
Network VPN	2	4	102.4 MB
Network Web Proxy	1	20	1.0 GB
Other Network Devices	0	0	0.0 GB
Hypervisor (Microsoft Hyper-V, VMware ESXi etc)	31	465	37.5 GB
WebServers	251	251	555.2 MB
Database	42	42	74.4 MB
Mail Servers	13	26	57.5 MB
Antivirus, DLP, EDR, etc.	1	5	11.1 MB
Other applications	0	0	0.0 GB
Custom		0	0 GB
	Total	5873	120.5 GB

4.6.1.3 Calculadora de EPS: https://siemsizingcalculator.logpoint.com/ com demanda de 6.226,53 EPS, conforme mostrado abaixo:

LOGPOINT Contact About Us

Infrastructure

Device Type	Quantity	EPS	GB/day
Windows Servers - HIGH EPS (Event Log)	7	49.00	4.73
Windows Servers - MED EPS (Event Log)	1	3.00	0.29
Windows Servers - LOW EPS (Event Log)	0	0.00	0.00
Linux Servers	10	30.00	0.72
Unix Servers	0	0.00	0.00
Network Wireless LAN	650	3250.00	39.23
Hypervisor (ESXi, Hyper-V etc)	31	465.00	37.42
Web Servers	251	251.00	5.05
Email Servers	0	0.00	0.00

Security

Device Type	Quantity	EPS	GB/day
Network Firewalls (Layer 7 Internal)	1	240.00	9.66
Network Firewalls (Layer 7 - DMZ)	0	0.00	0.00
Network Firewalls (Internal)	2	480.00	9.66
Network Firewalls (DMZ)	2	100.00	2.01
Network IPS/IDS	1	100.00	2.41
Antivirus	0	0.00	0.00
Data Loss Protection (DLP)	0	0.00	0.00
Others	0	0.00	0.00

Network

Device Type	Quantity	EPS	GB/day
VPN Server	1	2.00	0.05
Network Routers	2	2.00	0.04
Switches	625	1250.00	10.06

Endpoints

Device Type	Quantity	EPS	GB/day
Laptops	0	0.00	0.00
Desktops	9050	4.53	0.44

4.6.1.4 Calculadora de EPS: https://positka.in/siem-sizing-calculator com demanda de 8.304 EPS, conforme mostrado abaixo:

SIEM Sizing Calculator – Calculate your infrastructure EPS

Design an efficient plan for sizing SIEM as per your infrastructure with our ha calculator. The calculation is based on the volume of data ingested to the SIE devices in your IT infrastructure.

Data Source	Number of Devices (endpoints)	In monitoring scope? (Yes / No)	Estimated EPS per day
Network and security			
User Authentication / SSO / PAM / IAM	1	Yes	10
Active Directories, Domain Controlers	7	Yes	70
Switches (syslog)	625	Yes	1250
Routers (syslog)	2	Yes	2
Wireless Access Points	650	Yes	3250
Firewalls	2	Yes	400
DDoS Protection	0	Yes	0
VPNs	1	Yes	5
Proxy Systems	1	Yes	20
Vulnerability Scanners	1	Yes	5

IDS / IPS	1	Yes	15
Threat Intelligence Feeds	0	Yes	0
Data Loss/Leakage Prevention (DLP)	0	Yes	0
EDR (Endpoint Detection & Response)	0	Yes	0
WAF (Web Application Firewall)	1	Yes	30
Network Load Balancers	1	Yes	5

Infrastructure and applications			
Windows Servers (physical and virtual)	7	Yes	105
Unix Servers (physical and virtual)	10	Yes	30
Virtual Infrastructure Servers (Hypervisor)	31	Yes	465
Web Servers	251	Yes	2510
Application Servers	13	Yes	65
Database Instances	42	Yes	42
Storage Arrays	0	Yes	0

Cloud			
Cloud Services - Azure	0	Yes	0
Cloud Services - AWS	0	Yes	0
Cloud Services - Google	0	Yes	0
SaaS	1	Yes	25
Totals	1648		8304

4.6.2. A variação de EPS de ferramentas SIEM de múltiplos fabricantes, em uma mesma infraestrutura de redes, pode ser influenciada por vários fatores, incluindo o desempenho e eficiência da ferramenta, a capacidade de processamento do hardware subjacente e a otimização das configurações da ferramenta para o ambiente específico. Cada fabricante de SIEM pode ter implementações e abordagens diferentes para a coleta, processamento e análise de eventos de segurança. Essas diferenças podem impactar diretamente a capacidade do SIEM de lidar com um grande volume de eventos por segundo.

4.6.3. Os cálculos mostrados no item 4.6.1 são dados sobredimensionados porque na implantação podem haver ferramentas que diminuam a demanda de EPS (exemplo: EDR ou XDR) e nem todos os ativos podem ser considerados necessários para monitoramento. Sendo assim, a quantidade demandada de EPS é incerta (relatada pelos próprios fabricantes) até ser evidenciado na implantação da solução SIEM. Para não existir risco de contratar uma quantidade maior de EPS do que a mínima possível implantada, e conforme orientação de fornecedores, serão demandados inicial e aproximadamente 30% da maior estimativa de EPS levantada (item 4.6.1.1). Ou seja, a CONTRATADA deve fornecer o serviço de solução SIEM com funcionamento de 3.000 EPS por 36 meses a partir do TRD de implantação.

4.6.4. Como estratégia de complementação de EPS, a CONTRATADA deve oferecer a possibilidade de fornecer até 10 pacotes adicionais, usados sob demanda, de 500 EPS, 1.000 EPS ou 2.000 EPS cada um (ver serviços 4, 5 e 6 da Tabela 1. Serviços gerenciados e inter-relacionados necessários de segurança da informação). Os pacotes adicionais podem ser demandados de forma gradual e seu quantitativo poderá variar em virtude da flutuação natural do tamanho da rede durante a execução contratual. Portanto, os quantitativos de pacotes de EPS contratados representam meramente uma estimativa de utilização de serviço. Não haverá obrigação do TJCE na utilização do quantitativo parcial ou total dos pacotes de extra que são apresentados nos serviços 4, 5 e 6 da Tabela 1. Serviços gerenciados e inter-relacionados necessários de segurança da informação. Somente serão

devidos e pagos os pacotes adicionais efetivamente prestados e demandados através das respectivas Ordens de Serviço. A quantidade de pacotes adicionais demandados pode ser redimensionado em qualquer momento para quantidades maiores ou anualmente em quantidade menor (dentro da duração do contrato) e em função da mudança de monitoramento demandado pelo TJCE.

4.7. Serviço de monitoramento e correlação de eventos de segurança da informação

4.7.1. As atividades do Serviço de monitoramento e correlação de eventos de segurança da informação serão medidas por Níveis Mínimos de Serviço.

4.7.2. Os profissionais alocados no serviço de monitoramento e correlação de eventos (Analista SIEM) serão integrantes das operações no SOC conforme perfil descrito no item 4.8.

4.7.3. A CONTRATADA deverá disponibilizar, nas instalações do TJCE (Fortaleza/CE), o acesso de leitura a console das tecnologias que suportam os serviços de Gestão de Vulnerabilidades e de Coleta, Análise e Correlação de Logs (SIEM).

4.7.4. Monitoramento 24x7x365 da infraestrutura de TI, utilizando a ferramenta SIEM como sua tecnologia base, conforme apresentado na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE e futuras expansões ou modificações.

4.7.5. A CONTRATADA deverá adotar uma abordagem preventiva e reativa, identificando eventos suspeitos, classificando os incidentes de cibersegurança e fornecendo ao TJCE um relatório para cada evento identificado.

4.7.6. A CONTRATADA terá a responsabilidade de identificar e classificar os eventos de segurança utilizando a ferramenta de SIEM. O Blue Team, com apoio do serviço de monitoramento e o Red Team, será responsável por tratar o evento no serviço/host indicado no relatório fornecido pela CONTRATADA.

4.7.7. O serviço de SIEM deverá oferecer ao TJCE as seguintes facilidades:

4.7.7.1 Monitoração de correlação de eventos.

4.7.7.2 Gestão de incidentes.

4.7.7.3 Criação de novas regras de correlação e casos de uso e detecção.

4.7.7.4 Inteligência de ameaças e conformidade.

4.7.8. Triagem de incidentes identificados pelo serviço de monitoramento.

4.7.8.1 É necessário realizar uma triagem inicial nos chamados abertos pela monitoração de segurança, identificando e agrupando os potenciais incidentes que possuam características semelhantes, como ataques direcionados ao mesmo servidor, ataques originados do mesmo IP ou múltiplas falhas de login, por exemplo.

4.7.8.2 Após a etapa de triagem inicial, os chamados devem ser avaliados para determinar se são resultantes de falsos positivos/negativos, além disso, serão realizados testes para verificar a veracidade do incidente detectado.

4.7.9. Problemas identificados pelo serviço de monitoramento.

4.7.9.1 A equipe da CONTRATADA deve abrir chamados de problema em seu próprio sistema e no sistema do TJCE, relacionados ao serviço de monitoração, a fim de identificar a causa raiz. O Blue Team, com o suporte do serviço de monitoramento e o Red Team, deve solucionar o(s) problema(s) identificado(s) ao atender as demandas de incidentes.

4.7.9.2 Os chamados devem ser atendidos pelo Blue Team, com o apoio do serviço de monitoramento.

4.7.10. Incidentes de segurança identificados pelo serviço de monitoramento.

4.7.10.1 O Blue Team, com o suporte do serviço de monitoramento e o Red Team, será responsável por lidar com todo tipo de incidente e executar os procedimentos de resposta (item 2.3.13) para que seja implementada a respectiva solução.

4.7.10.2 O TJCE deve ser notificado sobre os incidentes por meio do sistema de chamados, e-mail e/ou telefone, conforme acordado previamente com o TJCE, de acordo com as necessidades de comunicação interna e/ou externa.

4.7.10.3 A CONTRATADA deve fornecer informações sobre os incidentes ao TJCE, por meio da abertura de chamados na ferramenta de ITSM do

TJCE.

4.7.11. Ocorrência de Incidentes no serviço de monitoramento.

4.7.11.1 Em caso de detecção de algum incidente de segurança, a CONTRATADA deve contatar imediatamente o TJCE por telefone, e-mail e abertura de chamado na ferramenta de ITSM do TJCE. Isso é necessário para que sejam tomadas as medidas corretivas e legais adequadas, tanto pela equipe da CONTRATADA quanto, se necessário, com a colaboração da equipe do TJCE, seguindo o procedimento estabelecido para resposta a incidentes (item 2.3.13).

4.7.11.2 O serviço de monitoramento deve comunicar imediatamente ao TJCE sobre acessos indevidos, instalação de códigos maliciosos ou qualquer outra ação que represente um risco para a segurança do ambiente do TJCE. Isso deve ser feito mesmo se essas tentativas não forem bem-sucedidas, mas houver persistência por parte do agente mal-intencionado.

4.7.11.3 O serviço de monitoramento deve fornecer todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que os incidentes de segurança relatados possam ser investigados pelo Blue Team, com o suporte do serviço de monitoramento e do Red Team.

4.7.12. Resposta a incidentes no serviço de monitoramento.

4.7.12.1 A CONTRATADA deve incluir as informações necessárias, como origem do ataque, tipo de ataque, data e hora, logs, causa do incidente de segurança e o procedimento de resposta ao incidente na ferramenta de ITSM do TJCE, a fim de possibilitar a implementação das medidas corretivas necessárias pelo Blue Team, com o suporte do serviço de monitoramento e do Red Team.

4.7.12.2 Os incidentes de segurança devem estar relacionados a eventos de segurança das soluções monitoradas e podem incluir, mas não se limitar

a, acessos indevidos, instalações de códigos maliciosos, indisponibilidade de serviços devido a ataques de negação de serviço (DoS e DDoS), ataques por força bruta ou qualquer outra ação que possa comprometer a confidencialidade, disponibilidade ou integridade das informações do TJCE.

4.7.13. Software e Hardware necessários para a solução SIEM no serviço de monitoramento.

4.7.13.1 A CONTRATADA é responsável por fornecer os softwares e hardwares necessários para implantar os serviços gerenciados de monitoramento e correlação de eventos de segurança da informação, durante o prazo do contrato e sem custos adicionais para o TJCE.

4.7.14. Configuração do *Security Information and Event Management* (SIEM).

4.7.14.1 A CONTRATADA deverá ativar o serviço que será utilizado como ferramenta, durante a vigência do contrato e antes do TRD de implantação, para prestação do Serviço de Coleta, Análise e Correlação de Logs, através de uma solução SIEM.

4.7.14.2 A CONTRATADA deve realizar a implementação das configurações, regras e políticas apropriadas para o ambiente do TJCE, levando em consideração as necessidades específicas do ambiente.

4.7.14.3 O TJCE, com o suporte da CONTRATADA, será responsável por realizar as configurações nos equipamentos de rede (switches, roteadores, servidores, etc.), servidores Linux/Windows e equipamentos de segurança da informação do TJCE para enviar os logs para a solução de SIEM. Adicionalmente, as configurações na solução de SIEM são de responsabilidade da CONTRATADA.

4.7.14.4 As configurações, regras de correlação, alertas e outras configurações do SIEM serão implementadas pela CONTRATADA e de propriedade intelectual e responsabilidade exclusiva do TJCE. Portanto, essas configurações não devem ser extraídas, copiadas, manipuladas ou

removidas sem o consentimento expresso do TJCE.

4.7.14.5 A Solução de SIEM deve abrir automaticamente chamados na ferramenta de ITSM do TJCE sempre que detectar um possível incidente de disponibilidade ou segurança.

4.7.14.6 Toda a mão de obra especializada necessária para a instalação e configuração da solução de SIEM deve ser fornecida pela CONTRATADA.

4.7.14.7 A CONTRATADA é responsável por executar todas as operações de monitoramento, gerenciamento e administração da solução de SIEM, conforme determinação do TJCE, abrangendo, mas não se limitando a:

4.7.14.7.1. Coleta de logs.

4.7.14.7.2. Criação de regras de correlação, não havendo limite mínimo para qualquer ativo e obrigatoriamente tratando todos os ativos monitorados.

4.7.14.7.3. Realização de configurações do SIEM (agentes, regras de incidentes, regras de correlação, etc).

4.7.14.7.4. Interação com o fabricante da solução.

4.7.14.7.5. Backup e restore.

4.7.14.7.6. Resolução de problemas.

4.7.14.7.7. Suporte.

4.7.14.7.8. Instalação de serviços relativos ao escopo contratado.

4.7.14.7.9. Atualização, de acordo com as recomendações do fabricante.

4.7.14.7.10. Outras operações citadas nos itens 4.3, 4.4 e 4.5.

4.7.14.8 Durante a fase de implantação, a CONTRATADA deve apresentar um conjunto de regras pré-definidas para ativação. Essas regras só serão implementadas após a aprovação do TJCE.

4.7.14.9 CONTRATADA será responsável por documentar as regras aprovadas pelo TJCE. A documentação de regras aprovadas (novas ou atualizadas)

deve seguir os processos de gerenciamento de mudanças do TJCE.

4.7.14.10 O TJCE tem permissão para solicitar alterações nas regras de correlação de eventos, de forma a ajustá-las às suas necessidades.

4.7.14.11 A CONTRATADA deverá prestar todos os serviços relativos ao SIEM (implantação, configuração, manutenção, análise de logs, detecção/resposta a incidentes, backup e restore, etc), conforme requisitos de funcionamento do SIEM apresentados nos itens 4.1 até 4.6.

4.7.14.12 A operação da console de administração e operação deverá ser de responsabilidade exclusiva da CONTRATADA, conforme especificações técnicas dos itens 4.1 até 4.6.

4.7.14.13 É de responsabilidade da CONTRATADA realizar a integração do SIEM de forma a possibilitar o recebimento de alertas e a abertura automática de incidentes na ferramenta de ITSM do TJCE.

4.8. Perfil dos profissionais do Analista de Segurança Sênior - SIEM.

4.8.1. Devem possuir graduação em cursos de tecnologia da informação e contar com experiência comprovada (CTPS, contrato de Pessoa Jurídica), no cargo a ser executado, de no mínimo 12 meses.

4.8.2. Deve contar com a certificação relacionada e emitida pelo fabricante da ferramenta SIEM usada no serviço de monitoramento e correlação de eventos.

4.8.3. Deve contar com proficiência de inglês intermediário para poder estabelecer comunicação com a comunidade técnica do fabricante da ferramenta SIEM, com o objetivo de obter informações que ajudem na implantação, execução, configuração e manutenção da ferramenta SIEM.

4.8.4. Deve contar com especialização em segurança da informação, comprovada através de certificado de conclusão oudiploma emitido por instituição de ensino superior reconhecida pelo Ministério da Educação ou com, pelo menos, uma das seguintes certificações: CompTIA Security+; EXIN Information Security Foundation; EXIN Ethical Hacking Foundation; GIAC Security Essentials (GSEC).

5. NÍVEIS MÍNIMOS DE SERVIÇO

5.1. Os Níveis Mínimos de Serviço (NMS) são parâmetros claros e mensuráveis que têm como objetivo avaliar e verificar vários aspectos dos serviços contratados, incluindo qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança. Esses critérios são estabelecidos de forma objetiva para garantir a excelência na prestação dos serviços.

5.2. Os serviços serão avaliados por meio de indicadores e NMS estabelecidos em fórmulas de cálculo específicas.

5.3. A responsabilidade de cumprir os NMSs é da CONTRATADA. A avaliação será realizada pela equipe de fiscalização do TJCE mensalmente, levando em consideração as metas exigidas dos serviços, conforme descrito na Tabela 4. Indicadores de Nível de Serviço. Para os casos de haver mais de uma ocorrência, as glosas por inadimplemento (pontos) serão cumulativas.

5.4. A empresa contratada é responsável por manter os padrões de qualidade estabelecidos para a prestação dos serviços, conforme Tabela 4. Indicadores de Nível de Serviço e Tabela 5. Glosas por descrição de referências para todos os serviços contratados.

5.5. A CONTRATADA terá uma redução de 2% (dois por cento) sobre o valor da fatura referente ao mês de ocorrência, a cada 15 pontos, ou um valor proporcional de redução de 2% a cada 15 pontos de glosa. Exemplo: para uma glosa de 10 pontos, a redução será de 1,33% como resultado da conta proporcional (10/15)*2%.

5.6. A meta exigida estabelece o valor exato (=), o limite máximo (<=) ou o limite mínimo (>=) que a CONTRATADA deve alcançar para cada um dos indicadores.

5.7. A meta exigida do cálculo com base no mês calendário será aplicado ao menor valor instantâneo entre os indicadores relativos aos horários de expediente regular ou horários de plantão contínuo. Por exemplo, um incidente que tenha sido inicializado no horário de plantão contínuo faltando 5 minutos para que comece o horário de expediente regular, passará a ter a menor meta entre ambos horários (após os 5 minutos) até a sua solução. Da mesma forma, um incidente que tenha sido inicializado no horário de expediente regular faltando 5 minutos para que comece o horário de plantão contínuo, passará a ter a menor meta (após os 5 minutos) entre ambos horários até a sua solução.

5.8. A CONTRATADA será responsável apenas pelos índices relacionados às solicitações de serviços e incidentes atribuídos a ela. Ela não poderá ser responsabilizada por chamados pendentes de fornecedores/prestadores de serviços externos ou encaminhados a outras equipes do TJCE, nem por situações dependentes de terceiros, que, portanto, não serão consideradas para fins de cálculo.

5.9. Requisições de serviço e incidentes reabertos referem-se a solicitações de serviço ou incidentes que foram considerados resolvidos, mas ainda estão pendentes de solução.

Tabela 4. Indicadores de Nível de Serviço

Serviço da Tabela 1	Nº	Indicadores de Nível de Serviço	Cálculo com base no mês calendário	Meta Exigida	Glosa
1, 2 e 3	1	Atividades rotineiras mensais definidas nos itens 2, 3 e 4, e programadas de acordo com o Plano de Trabalho ou por Requisição de Serviço.	Tempo = (Horas investidas nas atividades programadas) – ([Horas acordadas na OS]*1,25)	<=0 minutos	60 pontos
1 e 3	2	Índice de disponibilidade dos serviços de monitoramento e correlação de eventos (SIEM).	100 * [(Total de tempo com disponibilidade no mês – com exceção de indisponibilidade de energia ou link de conexão) / (Total de tempo no mês)] %	>= 99,7%	5 pontos (+2 pontos a cada hora excedente)
	3	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de indisponibilidade e em horário de expediente regular.	Tempo = (Hora do diagnóstico) – (Hora do início da indisponibilidade)	<= 60 minutos	30 pontos (+5 pontos a cada 10 minutos excedentes)
	4	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de indisponibilidade e em horário de plantão contínuo.	Tempo = (Hora do diagnóstico) – (Hora do início da indisponibilidade)	<= 180 minutos	30 pontos (+5 pontos a cada 20 minutos excedentes)
	5	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de degradação de desempenho e em horário de expediente regular.	Tempo = (Hora do diagnóstico) - (Hora do início da degradação de desempenho)	<= 120 minutos	15 pontos (+5 pontos a cada 10 minutos excedentes)
	6	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de degradação de desempenho e em horário de plantão contínuo.	Tempo = (Hora do diagnóstico) - (Hora do início da degradação de desempenho)	<= 240 minutos	15 pontos (+5 pontos a cada 10 minutos excedentes)
	7	Tempo máximo de não acompanhamento	Tempo = (Hora da solicitação de	<= 15	10 pontos

		a incidentes críticos de disponibilidade que estão sendo solucionados por outras equipes e em horário de expediente regular.	acompanhamento) – (Hora de resposta da solicitação)	minutos	(+5 pontos a cada 10 minutos excedentes)
	8	Tempo máximo de não acompanhamento a incidentes críticos de disponibilidade que estão sendo solucionados por outras equipes e em horário de plantão contínuo.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 45 minutos	10 pontos (+5 pontos a cada 10 minutos excedentes)
	9	Tempo máximo de não acompanhamento a incidentes de degradação de desempenho que estão sendo solucionados por outras equipes e em horário de expediente regular.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 30 minutos	5 pontos (+2 pontos a cada 10 minutos excedentes)
	10	Tempo máximo de não acompanhamento a incidentes de degradação de desempenho que estão sendo solucionados por outras equipes e em horário de plantão contínuo.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 90 minutos	5 pontos (+2 pontos a cada 10 minutos excedentes)
	11	Tempo máximo para requisição de mudança para aplicação de patches e hotfixes de segurança ou indicação de solução de contorno para tratamento de grave vulnerabilidade ou ameaça emergente.	Tempo = (Hora de conclusão do planejamento da requisição de mudança) – (Hora de disponibilização dos patches e hotfixes ou divulgação de grave vulnerabilidade ou ameaça emergente)	<= 72 horas	5 pontos (+2 pontos a cada hora excedente)
	12	Tempo máximo para abertura de chamados de suporte com terceiros. Somente aplicável a partir do horário de expediente regular.	Tempo = (Hora de abertura do chamado) – (Hora da triagem)	<= 30 minutos	5 pontos (+2 pontos a cada 5 minutos excedente)
1	13	Tempo máximo para resolução de requisições de serviços relacionados aos Produtos de UTM, NGFW, EDR, WAF, Gestor de vulnerabilidades. Somente aplicável a partir do horário de expediente regular.	Tempo = (Hora de resolução da solicitação) – (Hora da solicitação)	<= 180 minutos	10 pontos (+3 pontos a cada 10 minutos excedentes)
	14	Tempo máximo para resolução de requisições de serviços relacionados a outros ativos de segurança da informação.	Tempo = (Hora de resolução da solicitação) – (Hora da solicitação)	<= 30 horas	10 pontos (+3 pontos a cada hora excedente)
	15	Tempo máximo para triagem de incidentes de segurança e em horário de expediente regular.	Tempo = (Hora da triagem) – (Hora de entrada do evento de segurança)	<= 15 minutos	3 pontos (+1 ponto a cada 5 minutos excedentes)
	16	Tempo máximo para triagem de incidentes de segurança e em horário de plantão contínuo.	Tempo = (Hora da triagem) – (Hora de entrada do evento de segurança)	<= 120 minutos	3 pontos (+1 ponto a cada 5 minutos excedentes)
	17	Tempo máximo para resposta de	Tempo = (Hora do início da resposta) –	<= 60	10 pontos

		incidentes de segurança de gravidade alta e em horário de expediente regular.	(Hora da triagem)	minutos	(+3 pontos a cada 5 minutos excedentes)
	18	Tempo máximo para resposta de incidentes de segurança de gravidade alta e em horário de plantão contínuo.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 480 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	19	Tempo máximo para resposta de incidentes de segurança de gravidade média e em horário de expediente regular.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 150 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	20	Tempo máximo para resposta de incidentes de segurança de gravidade média e em horário de plantão contínuo.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 420 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	21	Tempo máximo para resposta de incidentes de segurança de gravidade baixa e em horário de expediente regular.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 210 minutos	5 pontos (+2 pontos a cada hora excedente)
	22	Tempo máximo para resposta de incidentes de segurança de gravidade baixa e em horário de plantão contínuo.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 420 minutos	5 pontos (+2 pontos a cada hora excedente)
	23	Tempo máximo para comunicação de incidentes a central de serviços da CONTRATADA e à equipe de segurança do TJCE. Somente aplicável a partir do horário de expediente regular.	Tempo = (Hora da comunicação) – (Hora da triagem)	<= 15 minutos	5 pontos (+2 pontos a cada 5 minutos excedentes)
2	24	Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço.	Tempo = (Horas investidas na Requisição de Serviço) – ([Horas acordadas na OS]*1,25)	<=0 minutos	15 pontos

Tabela 5. Glosas por descrição de referências para todos os serviços contratados

Nº	Descrição	Referência	Glosa
1	Não implementar a coleta de logs (via coletores), sua integração com a ferramenta SIEM e a retenção de logs após o período de carência de glossa.	Por ocorrência e por dia	15 pontos
2	Deixar de disponibilizar presencialmente no TJCE o Red Team, conforme descrito no item 1.3.1.	Por ocorrência e por dia	15 pontos
3	Deixar de fornecer os documentos comprobatórios de qualificação de qualquer profissional.	Por ocorrência e por dia	15 pontos
4	Deixar de documentar atividades rotineiras ou de requisição de serviço na ferramenta de ITSM.	Por ocorrência	5 pontos

5	Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, mesmo em situações de substituição temporária.	Por profissional e por dia	15 pontos
6	Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais	Por ocorrência	50 pontos
7	Suspender, colocar como pendente, pausar ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços solicitados.	Por ocorrência	5 pontos
8	Realizar mudanças de configuração nas soluções de segurança sem autorização da unidade responsável.	Por regra incluída, alterada ou excluída	10 pontos
9	Fraudar, manipular ou descaracterizar indicadores, metas de níveis de serviço e de desempenho por quaisquer subterfúgios.	Por ocorrência	100 pontos
10	Deixar de cumprir qualquer outra obrigação estabelecida no contrato e não prevista nesta tabela, de forma reincidente, após formalmente notificada pelo CONTRATANTE.	Por ocorrência	10 pontos
11	Perder dados ou informações corporativas por erros na operação devidamente comprovados.	Por ocorrência	180 pontos
12	Causar qualquer dano aos equipamentos do TJCE por motivo de imperícia na execução das atividades contratuais.	Por ocorrência	50 pontos
13	Recusar-se a executar serviço relacionado ao objeto do contrato, determinado pela fiscalização, por serviço.	Por ocorrência	10 pontos
14	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares, etc.) ou utilizar equipamento particular, salvo em situação excepcional e devidamente autorizado pelo TJCE.	Por ocorrência	10 pontos
15	Incluir, excluir ou alterar regras nos dispositivos de segurança sem autorização do gestor de TI, ou contrariando as políticas de segurança do CONTRATANTE.	Por ocorrência	20 pontos
16	Não respeitar o cronograma apresentado em uma proposta de execução de atividades quando se tratar de uma Requisição Planejada ou Rotineira.	Por ocorrência	10 pontos
17	Interromper unilateralmente a prestação de serviços sem que haja evento de força maior que o justifique, sem prejuízo de outras sanções legais e das cabíveis penais previstas no art. 156, da Lei n. 14.133/2021.	Por ocorrência	60 pontos
18	Deixar de apresentar relatórios, levantamentos ou inventários no prazo determinado em comum acordo.	Por ocorrência	15 pontos
19	Deixar de comunicar o contratante da substituição de profissionais responsáveis pela execução das atividades.	Por ocorrência	30 pontos
20	Deixar de atuar tempestivamente no caso de incidentes graves.	Por ocorrência	60 pontos
21	Deixar de cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato.	Por ocorrência	10 pontos
22	Deixar de cumprir ou implementar as rotinas em conformidade com os processos de trabalho do TJCE e da Diretoria de Tecnologia da Informação	Por ocorrência	10 pontos
23	Deixar de apresentar mensalmente propostas de melhorias no ambiente	Por ocorrência	5 pontos
24	Deixar de notificar sobre ocorrências recorrentes.	Por ocorrência	5 pontos

ANEXO II DO CONTRATO

TERMO DE CIÊNCIA

Anexo II – Termo de Ciência – TCI

AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação

Versão 1.0

Estado do Ceará
Poder Judiciário
Tribunal de Justiça

Histórico de Revisões

Data	Versão	Descrição	Responsável

Sumário

Termo de Ciência – TCI

AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação

Finalidade

Este documento tem como finalidade obter comprometimento formal dos empregados da contratada diretamente envolvidos nos projeto sobre o conhecimento da declaração e manutenção de sigilo e das normas de segurança vigentes na instituição

1 Equipe de Planejamento da Contratação

Contrato Nº:			
Objeto:			
Gestor do Contrato:		**Matricula:**	
Contratante órgão:			
Contratada		**CNJP**	
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.

2 Ciência/ Aprovação

Local e data,

Contratada	Funcionários

Nome Matricula	Nome Matricula
Nome Matricula	Nome Matricula

ANEXO III DO CONTRATO

TERMO DE COMPROMISSO

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

Anexo III – Termo de Compromisso – TC

AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação

O TRIBUNAL DE JUSTIÇA DO CEARÁ, sediado na Av. General Afonso Albuquerque Lima, S/N. – Cambeba CEP: 60822-325 – Fone: (85) 3207-7000, CNPJ n.° 09.444.530/0001-01, 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:

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 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 dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e

transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO 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 ideias, 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;

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

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.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem 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 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 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.

Cláusula Sexta – 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.

Cláusula Sétima – 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.

Cláusula Oitava – 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 equidade, 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 para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – 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.

DE ACORDO

CONTRATANTE	**CONTRATADA**
_____ *<Nome>* Matrícula: *<Matr.>*	_____ *<Nome>* *<Qualificação>*
Testemunhas	
Testemunha 1	**Testemunha 2**
_____ *<Nome>* *<Qualificação>*	_____ *<Nome>* *<Qualificação>*

_____, _____ de _____ de 20____

ANEXO IV DO CONTRATO
PROPOSTA DA CONTRATADA

(Inserir proposta ajustada ao valor homologado)

ANEXO V DO TERMO DE CONTRATO

POLÍTICA DO BANCO INTERAMERICANO DE DESENVOLVIMENTO SOBRE PRÁTICAS PROIBIDAS

Política do Banco Interamericano de Desenvolvimento sobre Práticas Proibidas

Práticas Proibidas

1.1 O Banco requer que todos os Mutuários (incluindo beneficiários de doações), Agências Executoras ou Agências Contratantes, bem como todas as empresas, entidades ou pessoas físicas que estejam apresentando propostas ou participando de atividades financiadas pelo Banco, incluindo, *interalia*, solicitantes, concorrentes, fornecedores de bens, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias (incluindo seus respectivos funcionários, empregados e agentes, quer com atribuições expressas ou implícitas), observem os mais altos padrões éticos, e denunciem ao Banco[1] todos os atos suspeitos de constituir uma Prática Proibida da qual tenha conhecimento, ou seja, informado, durante o processo de seleção e negociação ou na execução de um contrato. As Práticas Proibidas compreendem atos de: (a) práticas corruptas; (b) práticas fraudulentas; (c) práticas coercitivas; (d) práticas colusivas (e) práticas obstrutivas. O Banco estabeleceu mecanismos para denúncia de suspeitas de Práticas Proibidas. Qualquer denúncia deverá ser apresentada ao Escritório de Integridade Institucional (EII) do Banco para que se realize a devida investigação. O Banco também estabeleceu procedimentos de sanção para a resolução de casos. Além disso, o Banco celebrou acordos com outras instituições financeiras internacionais (IFI) visando ao reconhecimento recíproco às sanções aplicadas pelos respectivos órgãos de sanção.

(a) Para fins de cumprimento dessa política, o Banco define os termos indicados a seguir:

(i) uma *prática corrupta* consiste em oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer coisa de valor para influenciar as ações de outra parte;

(ii) uma *prática fraudulenta* é qualquer ato ou omissão, incluindo uma declaração falsa que engane ou tente enganar uma parte para obter benefício financeiro ou de outra natureza ou para evitar uma obrigação;

(iii) uma *prática coercitiva* consiste em prejudicar ou causar dano ou na ameaça de prejudicar ou de causar dano, direta ou indiretamente, a qualquer parte ou propriedade da parte para influenciar indevidamente as ações de uma parte;

(iv) uma prática colusiva é um acordo entre duas ou mais partes efetuadas com o intuito de alcançar um propósito impróprio, incluindo influenciar impropriamente as ações de outra parte; e

(v) uma prática obstrutiva consiste em:

(aa) destruir, falsificar, alterar ou ocultar deliberadamente uma evidência significativa para a investigação ou prestar declarações falsas aos investigadores com o fim de obstruir materialmente uma investigação do Grupo do Banco sobre denúncias de uma prática corrupta, fraudulenta, coercitiva ou colusiva; e/ou ameaçar, assediar ou intimidar qualquer parte para impedir a divulgação de seu conhecimento de assuntos que são importantes para a investigação ou a continuação da investigação,

(bb) ameaçar, assediar ou intimidar qualquer parte para impedir a divulgação de seu conhecimento de assuntos que são importantes para a investigação do Grupo BID ou a continuação da investigação; ou

(cc) todo ato que vise a impedir materialmente o exercício de inspeção do Grupo BID e dos direitos de auditoria previstos no parágrafo 1.1(f) a seguir; e

(vi) A "apropriação indevida" consiste no uso de fundos ou recursos do Grupo BID para um propósito indevido ou para um propósito não autorizado, cometido de forma intencional ou por negligência grave.

(b) Se, em conformidade com os procedimentos de sanções do Banco, for determinado que em qualquer estágio da aquisição ou da execução de um contrato qualquer empresa, entidade ou pessoa física atuando como licitante ou participando de uma atividade financiada pelo Banco, incluindo, entre outros, solicitantes, licitantes, fornecedores, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços, concessionárias, Mutuários (incluindo os Beneficiários de doações), Agências Executoras ou Agências Contratantes (incluindo seus respectivos funcionários, empregados e agentes, quer sejam suas atribuições expressas ou implícitas), estiver envolvida em uma Prática Proibida em qualquer etapa da adjudicação ou execução de um contrato, o Banco poderá:

(i) não financiar nenhuma proposta de adjudicação de um contrato para obras, bens e serviços relacionados financiados pelo Banco;

(ii) suspender os desembolsos da operação se for determinado, em qualquer etapa, que um empregado, agente ou representante do Mutuário, do Órgão Executor ou da Agência Contratante estiver envolvido em uma Prática Proibida;

(iii) declarar uma aquisição viciada e cancelar e/ou declarar vencido antecipadamente o pagamento de parte de um empréstimo ou doação relacionada inequivocamente com um contrato, se houver evidências de que o representante do Mutuário ou Beneficiário de uma doação não tomou as medidas corretivas adequadas (incluindo, entre outras medidas, a notificação adequada ao Banco após tomar conhecimento da Prática Proibida) dentro de um período que o Banco considere razoável;

(iv) emitir advertência à empresa, entidade ou pessoa física com uma carta formal censurando sua conduta;

(v) declarar que uma empresa, entidade ou pessoa física é inelegível, permanentemente ou por um período determinado, para: (i) adjudicação de contratos ou participação em atividades financiadas pelo Banco; e (ii) designação[2] como subconsultor, subempreiteiro ou fornecedor de bens ou serviços por outra empresa elegível a qual tenha sido adjudicado um contrato para executar atividades financiadas pelo Banco;

(vi) encaminhar o assunto às autoridades competentes encarregadas de fazer cumprir a lei; e/ou;

(vii) impor outras sanções que julgar apropriadas às circunstâncias do caso, inclusive multas que representem para o Banco um reembolso dos custos referentes às investigações e ao processo. Essas sanções podem ser impostas adicionalmente ou em substituição às sanções acima referidas.

(c) O disposto nos parágrafos 1.1 (b) (i) e (ii) se aplicará também nos casos em que as partes tenham sido temporariamente declaradas inelegíveis para a adjudicação de novos contratos, na pendência da adoção de uma decisão definitiva em um processo de sanção ou qualquer outra resolução.

(d) A imposição de qualquer medida que seja tomada pelo Banco conforme as disposições anteriormente referidas será de caráter público.

(e) Além disso, qualquer empresa, entidade ou pessoa física atuando como licitante ou participando de uma atividade financiada pelo Banco, incluindo, entre outros, solicitantes, licitantes, fornecedores de bens, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços, concessionárias, Mutuários (incluindo os Beneficiários

de doações), Agências Executoras ou Agências Contratantes (incluindo seus respectivos funcionários, empregados e representantes, quer suas atribuições sejam expressas ou implícitas), poderá ser sujeita a sanções, em conformidade com o disposto nos acordos que o Banco tenha celebrado com outra instituição financeira internacional com respeito ao reconhecimento recíproco de decisões de inelegibilidade. Para fins do disposto neste parágrafo, o termo "sanção" refere-se a toda inelegibilidade permanente, imposição de condições para a participação em futuros contratos ou adoção pública de medidas em resposta a uma contravenção às regras vigentes de uma IFI aplicável à resolução de denúncias de Práticas Proibidas;

(f) O Banco exige que os solicitantes, concorrentes, fornecedores e seus agentes, empreiteiros, consultores, pessoal, subempreiteiros, prestadores de serviços e concessionárias permitam que o Banco revise quaisquer contas, registros e outros documentos relativos à apresentação de propostas e a execução do contrato e os submeta a uma auditoria por auditores designados pelo Banco. Solicitantes, concorrentes, fornecedores de bens e seus agentes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias deverão prestar plena assistência ao Banco em sua investigação. O Banco requer ainda que todos os solicitantes, concorrentes, fornecedores de bens e seus agentes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias: (i) mantenham todos os documentos e registros referentes às atividades financiadas pelo Banco por um período de sete (7) anos após a conclusão do trabalho contemplado no respectivo contrato; e (ii) forneçam qualquer documento necessário à investigação de denúncias de Práticas Proibidas e assegurem-se de que os empregados ou representantes dos solicitantes, concorrentes, fornecedores de bens e seus representantes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias que tenham conhecimento das atividades financiadas pelo Banco estejam disponíveis para responder às consultas relacionadas com a investigação provenientes de pessoal do Banco ou de qualquer investigador, agente, auditor ou consultor devidamente designado. Caso o solicitante, concorrente, fornecedor e seu agente, empreiteiro, consultor, pessoal, subempreiteiro, subconsultor, prestador de serviços ou concessionária se negue a cooperar ou descumpra o exigido pelo Banco, ou de qualquer outra forma crie obstáculos à investigação por parte do Banco, o Banco, a seu critério, poderá tomar medidas apropriadas contra o solicitante, concorrente, fornecedor e seu agente, empreiteiro, consultor, pessoal, subempreiteiro, subconsultor, prestador de serviços ou concessionária.

(g) Se um Mutuário fizer aquisições de bens, obras, serviços que forem ou não de consultoria diretamente de uma agência especializada, todas as disposições da Seção 8 relativas às sanções e Práticas Proibidas serão aplicadas integralmente aos solicitantes, concorrentes, fornecedores e seus representantes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias (incluindo seus respectivos funcionários, empregados e representantes, quer suas atribuições sejam expressas ou implícitas), ou qualquer outra entidade que tenha firmado contratos com essa agência especializada para fornecer tais bens, obras, serviços que forem ou não de consultoria, em conformidade com as atividades financiadas pelo Banco. O Banco se reserva o direito de obrigar o Mutuário a lançar mão de recursos tais como a suspensão ou a rescisão. As agências especializadas deverão consultar a lista de empresas ou pessoas físicas declaradas temporária ou permanentemente inelegíveis pelo Banco. Caso alguma agência especializada celebre um contrato ou uma ordem de compra com uma empresa ou uma pessoa física declarada temporária ou

permanentemente inelegível pelo Banco, o Banco não financiará os gastos correlatos e poderá tomar as demais medidas que considere convenientes.

1.2 Os Concorrentes ao apresentar uma proposta declaram e garantem que:

(i) leram e entenderam a proibição sobre atos de fraude e corrupção disposta pelo Banco e se obrigam a observar as normas pertinentes;
(ii) não incorreram em nenhuma Prática Proibida descrita neste documento;
(iii) não adulteraram nem ocultaram nenhum fato substancial durante os processos de seleção, negociação e execução do contrato;
(iv) nem eles nem os seus agentes, pessoal, subempreiteiros, subconsultores ou quaisquer de seus diretores, funcionários ou acionistas principais foram declarados inelegíveis pelo Banco ou outra Instituição Financeira Internacional (IFI) e sujeito às disposições dos acordos celebrados pelo Banco relativos ao reconhecimento mútuo de sanções à adjudicação de contratos financiados pelo Banco, nem foram declarados culpados de delitos vinculados a práticas proibidas;
(v) nenhum de seus diretores, funcionários ou acionistas principais tenha sido diretor, funcionário ou acionista principal de qualquer outra empresa ou entidade que tenha sido declarada inelegível pelo Banco ou outra Instituição Financeira Internacional (IFI) e sujeito às disposições dos acordos celebrados pelo Banco relativos ao reconhecimento mútuo de sanções à adjudicação de contratos financiados pelo Banco ou tenha sido declarado culpado de um delito envolvendo Práticas Proibidas;
(vi) declararam todas as comissões, honorários de representantes ou pagamentos para participar de atividades financiadas pelo Banco; e
(vii) reconhecem que o descumprimento de qualquer destas garantias constitui fundamento para a imposição pelo Banco de uma ou mais medidas descritas na Cláusula 1.1 (b).

ANEXO VI DO CONTRATO

PAÍSES ELEGÍVEIS

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ANEXO VI – Países Elegíveis

Elegibilidade para Provisão de Bens, Obras e Serviços em Contratos Financiados pelo Banco Interamericano de Desenvolvimento

Nota: *O termo "Banco" usado neste documento inclui o BID, o Fumin e outros fundos administrados por ele.*
Dependendo da fonte de financiamento, o usuário deve selecionar uma das seguintes opções do item 1. O financiamento pode vir do BID ou do Fundo Multilateral de Investimentos (Fumin); ocasionalmente, os contratos podem ser financiados por fundos especiais que restringem ainda mais os critérios de elegibilidade a um grupo de países membros. Quando a última opção for escolhida, os critérios de elegibilidade devem ser indicados aqui:
.....

1) Países Membros quando o financiamento provém do Banco Interamericano de Desenvolvimento.

a. ***Países Mutuários:***

i. *Argentina, Bahamas, Barbados, Belize, Bolívia, Brasil, Chile, Colômbia, Costa Rica, Equador, El Salvador, Guatemala, Guiana, Haiti, Honduras, Jamaica, México, Nicarágua, Panamá, Paraguai, Peru, República Dominicana, Suriname, Trinidad e Tobago, Uruguai e Venezuela.*

b. ***Países não Mutuários:***

i. *Alemanha, Áustria, Bélgica, Canadá, República Popular da China, República da Coréia, Croácia, Dinamarca, Eslovênia, Espanha, Estados Unidos, Finlândia, França, Israel, Itália, Japão, Noruega, Países Baixos, Portugal, Reino Unido, Suécia e Suíça.*

c) ***Territórios elegíveis:***

i. *Guadalupe, Guiana Francesa, Martinica, Reunião - como Estado da França*
ii. *Ilhas Virgens dos EUA, Porto Rico, Guam - como Território dos EUA*
iii. *Aruba - como um país integrante do Reino dos Países Baixos, assim como, Bonaire, Curaçao, Santa Marta, Saba, Santo Eustáquio - como Estados do Reino dos Países Baixos*
iv. *Hong Kong - Região Administrativa Especial da República Popular da China.*

---

1) Critérios para determinar a nacionalidade e origem dos bens e serviços

Estas disposições de políticas tornam necessário estabelecer critérios para determinar: a) a nacionalidade das firmas e indivíduos elegíveis para participar em contratos financiados pelo Banco; e b) o país de origem dos bens e serviços. Nessas determinações, serão utilizados os seguintes critérios:

A) Nacionalidade

a) **Um indivíduo é considerado nacional** de um país membro do Banco se satisfaz um dos seguintes requisitos:

i. é cidadão de um país membro; ou

ii. estabeleceu seu domicílio em um país membro como residente de boa fé e está legalmente autorizado para trabalhar nesse país.

b) **Uma firma é considerada nacional** de um país membro se satisfaz os dois seguintes requisitos:

i. está legalmente constituída ou estabelecida conforme as leis de um país membro do Banco; e

ii. mais de cinquenta por cento (50%) do capital da firma é de propriedade de indivíduos ou firmas de países membros do Banco.

Todos os membros de um consórcio e todos os subempreiteiros devem cumprir os requisitos acima estabelecidos.

B) Origem dos Bens

Os bens tem origem em um país membro do Banco se foram extraídos, desenvolvidos, cultivados, colhidos ou produzidos em um país membro do Banco. Considera-se que um bem é produzido quando, mediante manufatura, processamento ou montagem, o resultado é um artigo comercialmente reconhecido cujas características, funções ou utilidades básicas são substancialmente diferentes de suas partes ou componentes.

No caso de um bem que consiste de vários componentes individuais que devem ser interconectados (pelo fornecedor, comprador ou um terceiro) para que o bem possa ser utilizado, e sem importar a complexidade da interconexão, o Banco considera que este bem é elegível para financiamento se a montagem dos componentes for feita em um país membro, independente da origem dos componentes. Quando o bem é uma combinação de vários bens individuais que normalmente são empacotados e vendidos comercialmente como uma só unidade, o bem é considerado proveniente do país onde este foi empacotado e embarcado com destino ao comprador.

Para fins de determinação da origem dos bens identificados como “feito na União Europeia”, estes serão elegíveis sem necessidade de identificar o correspondente país específico da União Europeia.

A origem dos materiais, partes ou componentes dos bens ou a nacionalidade da empresa produtora, montadora, distribuidora ou vendedora dos bens não determina a origem dos mesmos.

C) Origem dos Serviços

O país de origem dos serviços é o mesmo do indivíduo ou empresa que presta os serviços conforme os critérios de nacionalidade acima estabelecidos. Este critério é aplicado aos serviços conexos ao fornecimento de bens (tais como transporte, seguro, instalação, montagem, etc.), aos serviços de construção e aos serviços de consultoria.

ANEXO VII DO CONTRATO

FICHA DE DADOS DO REPRESENTANTE LEGAL

Dados pessoais do(s) representante(s) e/ou procurador(es), devidamente habilitados, da futura CONTRATADA, indicado(s) para assinatura do Termo de Contrato:

NOME	:	_____
NACIONALIDADE	:	_____
ESTADO CIVIL	:	_____
PROFISSÃO	:	_____
RG	:	_____
CPF	:	_____
DOMICÍLIO	:	_____
CIDADE	:	_____
UF	:	_____
FONE	:	_____
FAX	:	_____
CELULAR	:	_____
E-MAIL	:	_____