ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA – DOD

AQSETIN2022015 – Solução de gestão e análise de vulnerabilidades de ativos

1. INTRODUÇÃO

Este documento tem como finalidade formalizar o início do processo de planejamento da contratação de **Solução de gestão e análise de vulnerabilidades de ativos,** vincular as necessidades da contratação desejada aos objetivos estratégicos e às necessidades corporativas da instituição, garantindo alinhamento ao Plano Estratégico Institucional e ao Painel de Contribuição da TI, indicar a fonte de recursos para a contratação e indicar os integrantes da Equipe de Planejamento da Contratação.

2. IDENTIFICAÇÃO DA ÁREA REQUISITANTE DA SOLUÇÃO

Unidade/setor/departamento: Serviço de Segurança da Informação do Tribunal de Justiça do Estado do Ceará.

Data: Agosto/2022.

Nome da Aquisição: Solução de gestão e análise de vulnerabilidades de ativos.

Responsável pela Demanda: Adarildo de Brito Figueiredo

Matrícula: 8025

E-mail do Responsável: adarildo@tjce.jus.br

Telefone: 3207-7794

Fonte de Recursos: Fundo Especial de Reaparelhamento e Modernização do Poder Judiciário do Estado do Ceará – FERMOJU

3. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante Requisitante			
Nome	Adarildo de Brito Figueiredo	**Matrícula**	8025
E-mail	adarildo@tjce.jus.br	**Telefone**	(85) 3207-7794
Integrante Técnico			
Nome	Heldir Sampaio Silva	**Matrícula**	9630
E-mail	heldir.sampaio@tjce.jus.br	**Telefone**	(85) 3207-7944/7756/6850
Integrante Administrativo			
Nome	Fabio de Carvalho Leite	**Matrícula**	9594
E-mail	fabio.leite@tjce.jus.br	**Telefone**	(85) 3207-7872

4. ALINHAMENTO ESTRATÉGICO

ID	Objetivo Estratégico Institucional	ID	Objetivos de Contribuição da Setin
01	Fortalecer a inteligência de dados e a segurança da informação	01	Proporcionar segurança, disponibilidade e confiabilidade às informações dos sistemas, plataformas e ferramentas institucionais

5. MOTIVAÇÃO/JUSTIFICATIVA

5.1. Situação Atual

A infraestrutura tecnológica do Poder Judiciário do Estado do Ceará é composta por ativos de rede; servidores, estações de trabalho e notebooks; servidores em Cloud; contêineres e aplicações Web e API;

• Estações de trabalho, smartphones, tablets e notebooks distribuídos para os usuários (servidores e magistrados) que utilizam os serviços providos pela Secretaria de Tecnologia da Informação – SETIN - TJCE;

• Os switches e roteadores compõem a infraestrutura lógica (tráfego de dados e acesso à internet) provendo o compartilhamento de recursos, conectando todos os dispositivos, inclusive computadores, impressoras e servidores. Tais dispositivos proporcionam o compartilhamento de informações sensíveis às atividades executadas pelo Judiciário Cearense. Portanto, torna-se impossível a concepção de uma rede lógica, sem a utilização dos mesmos.

• Assim como um switch, o roteador conecta vários dispositivos para criar uma rede. Além disso, um roteador conecta vários switches e suas respectivas redes para formar uma rede ainda maior. Essas redes podem estar em um único local ou em vários.

• Os servidores, alocados no Centro de Documentação e Informática – CDI – Prédio Anexo ao Palácio da Justiça, comportam quase todos os serviços e sistemas disponibilizados para o público externo e interno deste Tribunal;

É composta também, pela infraestrutura contida nas tabelass abaixo:

HOSTS DIFERENTES
Imagens de computadores
Imagens de notebooks
Switchs
Firewalls pequenos
Access Points - AP’s
Controladoras dos AP’s
Servidores físicos
Servidores diferentes – Windows 1
Servidores diferentes – Windows 2
Servidores diferentes – Windows 3
Servidores diferentes – Linux 1
Servidores diferentes – Linux 2
Servidores diferentes – Linux 3
Servidores diferentes – Linux 4
Servidores diferentes – Linux 5
Impressoras Multifuncionais
Balanceador de Carga – Netscaler
Firewall de grande porte – NGFW
Fitotecas – Tape Library
Switches de Núcleo
Servidores de Armazenamento – Storage
Relógio de Ponto
Controle de Acesso

Conteiners
Pje
IP3
MinIO
Pje Midias
Portal SAJ
SAJ CAS
SAJ PG
SAJ SG
DJE - SAJ

SAJ CPOPG
SAJ AT
Openshift
AUTDOC - API
AUTDOC - Autenticação
PAJ
SAV
SCP - Sistema de Certidão de Precatórios
Aplicação de Referência (Ruby On Rails)
DJe - Administração
Dje - Consulta Pública
FATJ
FERIAS SERVIDOR
Gestão a Vista
INDICA
Manager ProTJ
Minha ESMEC
Novo SAA
Novo SCONC
SADJUS
SAE
SASR
SBIM
SCGV
SCI
SCN
SCT
SDTS
SEI
SGM
SIM TJ
SISNUGEP
SISPORT - Sistema de Controle de Portaria
SSAS-Sistema de Solicitação de Auxílio Saúde
TJCE Mobile Notifications API
Redmine

TJCE Mobile API
Discovery
Gateway
Keycloak
Redis
Rabbitmq
Awx
codex
codex pje pg
codex pje sg
pje binários
registry portal esaj
Vault portal esaj
Aplicaçoes Java

Sites / Dominios
Total Geral (Origem Netscale - Disponibilizado na Internet)
Externos - Principais
Sites de aplicação judicial:
Malote Digital
Encurtador de link
tjcev2
Consulta processo (SCPU
E-saj
Pje
Sites administrativos:
Sites de ADMRH (portal)
Themis
Portal Adm (Ead)
Spes
SSAS
Espaço do Servidor
Webmail
Catinet (Versão externa)
CatiWeb (Versão externa)
Sasr

Processo Administrativo – CPA
VDC
Sites de aplicativos / sistemas
Sites de informações gerais

5.2. Descrição da Oportunidade ou do Problema

As funcionalidades dos equipamentos citados podem vir a sofrer degradação, tendo em vista o risco de invasão por parte de terceiros mal-intencionados, seja por meio de acesso a sites, por meio de aplicativos, ou e-mails que contém em seus anexos *malwares (software intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores)* que podem comprometer a segurança de dados dos usuários que os utilizam.

O trabalho de manter a segurança de tais ativos, incluindo os de rede e de segurança, seguros vai além da utilização de antivírus nos computadores. Softwares desatualizados em estações de trabalho, notebooks e servidores, podem vir a criar alvos fáceis para exploradores de vulnerabilidades.

O intuito deste planejamento é abordar os principais tipos de vulnerabilidades – softwares maliciosos e ataques – demonstrando assim a importância e necessidade da aquisição de uma solução de análise de vulnerabilidade.

O intuito da utilização desse tipo de software é automatizar e facilitar a descoberta de vulnerabilidades em todos os ativos que estejam vinculados à rede do TJCE, para correção, antes que as mesmas sejam exploradas por atacantes e, neste contexto, é de grande importância seu adequado funcionamento.

5.3. Motivação da Demanda

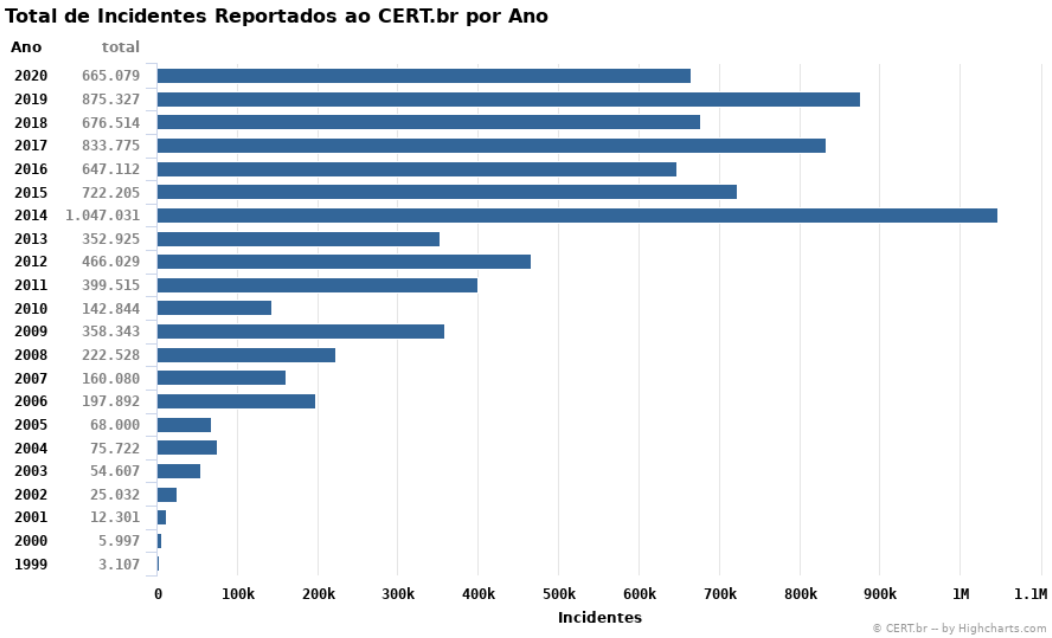
Vulnerabilidade é um conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Já segundo o CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT.BR, uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

As vulnerabilidades são originadas de falhas na maioria das vezes não intencionais. Estas falhas podem ser:

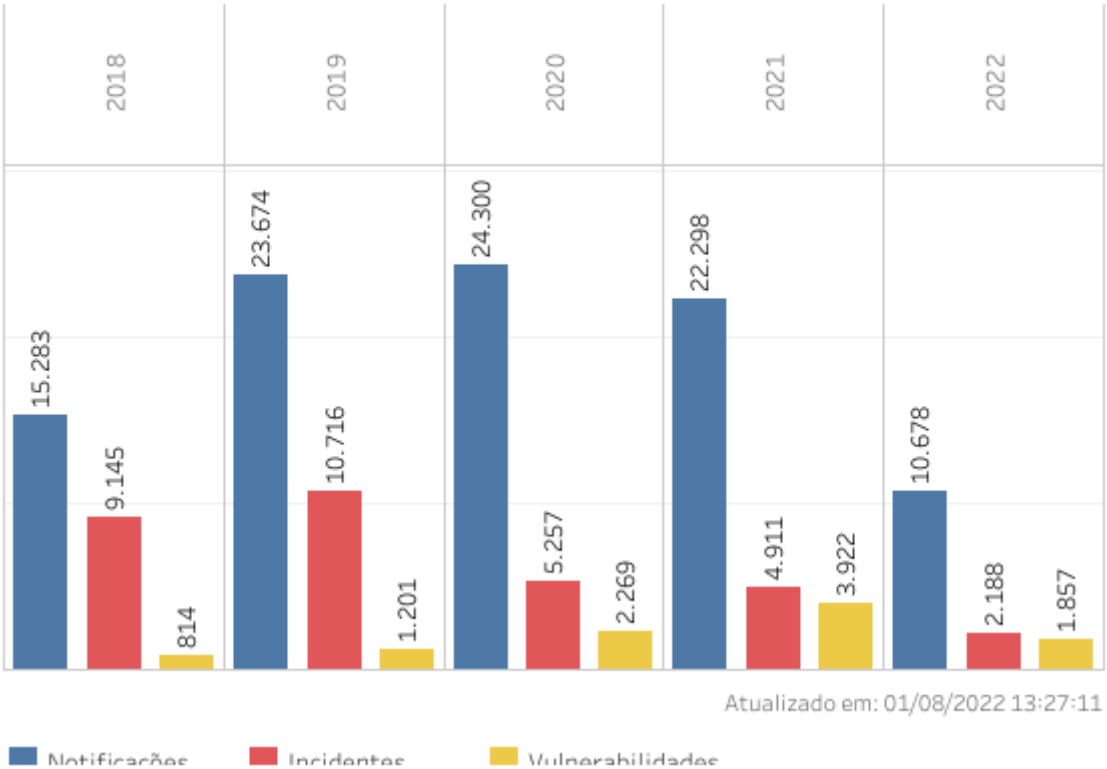
- **Físicas:** Acesso a ativos por pessoas não autorizadas, devido à falta de controle de acesso. Por exemplo, uma empresa terceirizada de limpeza desligar um switch por engano.
- **Hardware:** Falhas no Hardware que ocasionam indisponibilidade no sistema ou perda dados. Outro item desta falha é a inclusão de um hardware malicioso como um Keylogger.
- **Naturais:** Desastres naturais comprometendo a segurança dos dados armazenados.

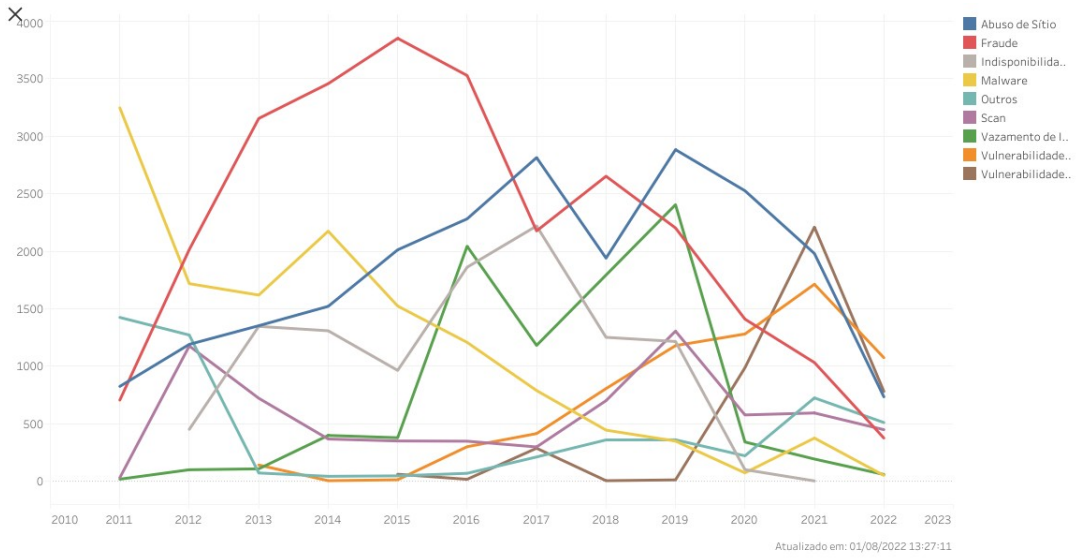
- **Humanas:** Operador de sistema utilizar erroneamente uma função, prejudicando o funcionamento do mesmo ou ocasionando perda de informações.
- **Software:** Falhas de programação, abrindo brechas a serem exploradas.



As estatísticas de incidentes do CERT.BR reportados de janeiro a junho de 2020, citadas na imagem acima, demonstram que 58,81% de incidentes são do tipo de ataque Scan, onde o atacante faz uma varredura de portas abertas em uma rede para identificar os serviços disponibilizados e suas possíveis vulnerabilidades.

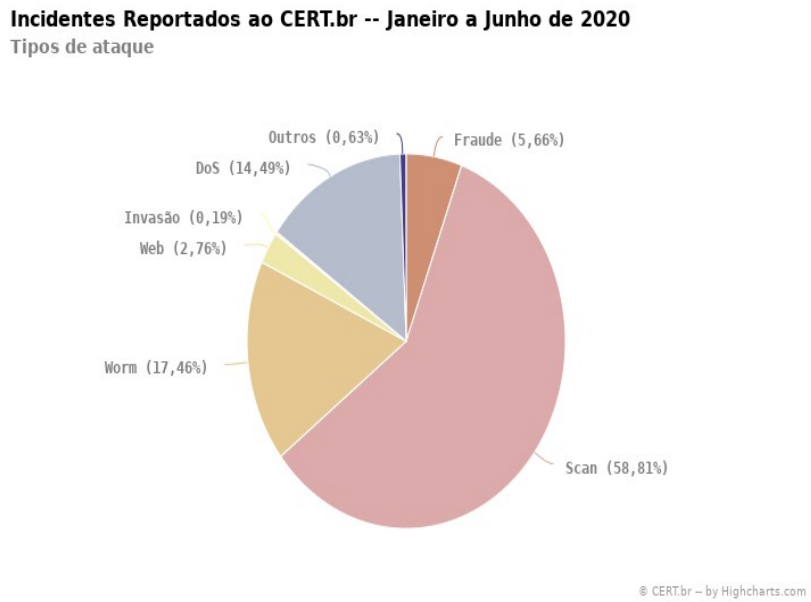
Corroborando com as estatísticas apresentadas acima, podemos citar ainda os índices apurados pelo CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, cujas imagens abaixo indicam as ocorrências acerca de vulnerabilidades:





Muitas vulnerabilidades são exploradas ou criadas a partir de softwares desenvolvidos para este fim conhecidos como Malware. Proveniente do inglês *malicious software* o Malware é um programa que produz efeitos danosos e indesejados.

Os principais tipos de Malware encontrados hoje são:



- **Vírus:** Programa capaz de se autoexecutar e infectar outros arquivos com seu próprio código.
- **Worm:** Programa malicioso que se propaga sem a necessidade de infectar outros arquivos, diferentemente do vírus, sua propagação é feita sem intervenção humana utilizando vulnerabilidades em uma rede.
- **Bot e botnet:** Bot é um programa que permite ser controlado remotamente para executar vários comandos maliciosos, como, por exemplo, ataque de negação de serviço a um site. Uma botnet é uma rede com vários bots no qual sua ação maliciosa é amplificada.
- **Spyware:** Os Spywares coletam informações pessoais ou empresariais e as enviam para terceiros. O Keylogger é um tipo de Spyware que captura as teclas digitadas pelo usuário, geralmente utilizado para roubar senhas.
- **Backdoor:** O Backdoor ou Porta do fundo é uma vulnerabilidade que abre uma brecha para o atacante obter acesso indevido.
- **Cavalo de tróia:** Também conhecido como Trojan o Cavalo de Tróia é um programa malicioso que se disfarça por um programa bem-intencionado. O usuário executa, sem saber, um código malicioso pensando que está executando apenas um programa legítimo. Eles geralmente são disseminados por e-mails e redes sociais se passando por cartões, álbum de fotos, jogos e etc.
- **Rootkit:** Conjunto de programas utilizado por um atacante para ocultar sua invasão e facilitar um futuro ataque. Os Rootkits podem ser utilizados em outros malwares para dificultar a detecção destes.

A efetivação de um ataque é o êxito na exploração de uma ou mais vulnerabilidades. As motivações para realizar um ataque segundo o Cert.br, podem ser financeiras, por prestígio,

demonstração de poder, por ideologia ou comerciais.

Com novas tecnologias novos ataques surgem, mas os principais ataques conhecidos atualmente são:

DoS e DDoS: Negação de Serviço do inglês Denial of Service, sigla DoS, ocorre quando um site (ou serviço) fica indisponível por receber uma grande quantidade de tráfego, não podendo atender as requisições legítimas. Os ataques DDoS (Distributed Denial of Service) são vários ataques DoS feitos de maneira distribuída dificultando assim o bloqueio da origem os ataques. Geralmente estes ataques provêm de computadores infectados com Bots participantes de uma rede Botnet.

Buffer Overflow: ou Estouro de Buffer ocorre quando um espaço de memória com tamanho fixo recebe um dado maior que seu tamanho, ocorrendo assim um vazamento dados na memória sobrescrevendo a memória adjacente.

Spam: são e-mails não solicitados que são enviados em massa gerando tráfego desnecessário nas redes. Geralmente os Spams têm como intuito a divulgação de produtos, mas também são responsáveis por muitos golpes de Internet por disseminarem Malwares.

Phishing Scam: E-mails falsos que se passam por mensagens de instituições confiáveis, como bancos e órgãos governamentais. Seu intuito é induzir o usuário a instalar um programa malicioso ou visitar uma página falsa (cópia de uma verdadeira) para obter dados pessoais, como por exemplo, senhas e números de cartão de crédito. Segundo o Cert.br 87,05% das fraudes de janeiro a dezembro de 2019 eram de páginas falsas, conforme apresentado na imagem acima.

Tipos de incidentes de segurança da informação:

- **DNS Poisoning:** Envenenamento de DNS é um ataque que forja um endereço falso no servidor de DNS. Assim, o atacante pode capturar senhas e números de cartões de crédito utilizando páginas clones do site original.
- **Ataque de Força Bruta:** Programa que utiliza várias combinações de usuário e senha para conseguir acesso indevido a sistemas ou para descriptografar chaves e arquivos. Além do risco de acesso indevido, o Ataque de Força Bruta gera uma carga excessiva no alvo por ter responder e processar a várias tentativas de logins. Esta técnica é muito utilizada em servidores de SSH mal configurados.
- **Packet Sniffing:** Packet Sniffing ou Farejamento de Pacotes é um método utilizado para capturar pacotes destinados a outras máquinas da mesma rede com objetivo de obter dados pessoais. Ativos de rede que utilizam broadcast de pacotes, como Hub, facilitam o farejamento dos pacotes. Em redes segmentadas por Switches o Packet Sniffing é possível com a utilização de outra técnica conhecida como Man-in-theMiddle (MiTM). Com MiTM o atacante forja a passagem dos pacotes da rede pela sua interface através do envenenamento da tabela ARP dos outros computadores.

- **Varreduras em Redes – Scan:** Técnica onde o atacante descobre máquinas ativas e serviços disponíveis na rede. Em uma rede 192.1 68.0.0/24, por exemplo, o atacante envia ping para todos endereços possíveis para descobrir quais estão ativos. Com os endereços das máquinas ativas é feita uma nova varredura em cada máquina para descobrir suas portas abertas e seus respectivos serviços. Com isso o atacante pode explorar as vulnerabilidades destes serviços e prejudicar o computador alvo. Por exemplo, sabendo que o alvo possui a porta TCP 23 aberta, o atacante irá explorar vulnerabilidades de software ou configuração do serviço para obter acesso ao sistema.
- **SQL Injection:** O ataque de Injeção de SQL consiste em inserir códigos SQL em um software vulnerável para obter ou danificar informações do Banco de dados.
- **CSS – Cross Site Scripting:** XSS ou CSS o Cross Site Scripting é um ataque a um site vulnerável que aceita a inserção de códigos Javascript. Através do CSS o atacante pode inserir uma página externa para capturar logins e senhas.

5.4. Resultados Pretendidos

- **Maior controle de segurança da informação e proteção de dados no âmbito do TJCE**: através da redução de *malwares*, sistemas desatualizados, dentre outros problemas;
- **Aumento dos esforços de correção e testes de eficácia:** as análises de vulnerabilidades de rede permitem não só a identificação de problemas de rede, mas também ajuda na sua priorização e no desenvolvimento de uma estratégia para lidar com aqueles mais críticos;
- **Melhoria na gestão de mudanças e no gerenciamento de patches**: faz parte da gestão de vulnerabilidades centralizar e gerar todos os feedbacks sobre os problemas, as suas correções e as próximas ações;
- **Fortalecimento da atuação das equipes que gerem soluções críticas**: A identificação e o tratamento das vulnerabilidades auxiliarão a SETIN na execução de suas responsabilidades de análise e respostas às notificações e atividades relacionadas a incidentes de segurança em redes de computadores além da redução desses incidentes;
- **Apoio nas auditorias de Segurança da Informação e Comunicações**: a obtenção de relatórios detalhados permitirá a devida diligência durante as auditorias;
- **Atualização da Política de Segurança da Informação e Comunicações**: O gerenciamento de vulnerabilidades possibilitará aplicar melhorias na segurança da informação e na revisão da Política de Segurança da Informação e Comunicações – POSIC e suas normas complementares.
- **Auxílio nos requisitos regulamentares**: A identificação e o tratamento das vulnerabilidades contribuirá para que o TJCE se mantenha em conformidade com:
    - Resoluções, Normativos e Portarias editados pelo Conselho Nacional de Justiça - CNJ;

◦ Os princípios e controles de segurança definidos nos padrões ABNT NBR ISO/IEC 27001, 27002, 27005, 27011 e 27014;

◦ A Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

◦ Os frameworks de processos de governança e boas práticas como o ITIL e COBIT.

Não obstantes os aspectos técnicos citados anteriormente, que por sua venham a impingir a Administração a ponderar acerca da implantação da referida solução, é oportuno citar que o CNJ, Órgão cuja competência é o de o controlar da atuação administrativa e financeira do Poder Judiciário (Regimento Interno Nº 67 de 03/03/2009), vinculando assim as diretrizes do TJCE quanto às soluções de TI, editou a Portaria Nº 162 de 10/06/2021,*Aprova protocolos e Manuais criados pela Resolução CNJ nº. 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário(ENSEC-PJ)., cujos enunciados e ANEXOS instruem*:

Protocolo – Prevenção de Incidentes Cibernéticos do Poder Judiciário – PPINC-PJ

> *4.1 A gestão de incidentes de segurança cibernética é realizada por meio de processo definido e constituída formalmente, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.*
>
> *5.3 Caberá a cada órgão do Poder Judiciário avaliar o adequado posicionamento da ETIR (Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética) em seu organograma institucional, considerando-se seu desenho organizacional e suas peculiaridades.*

Para a efetivação da implantação, atualização e acompanhamento da política de segurança, almejada pela solução em questão, faz-se necessária a inclusão de treinamentos e consultoria, tendo em vista o atendimento do requisito de independência do conhecimento.

ANEXO IV DA PORTARIA No 162, DE 10 DE JUNHO DE 2021

Manual de Referência – Proteção de Infraestruturas Críticas de TIC

Checklist para utilização dos Controles Mínimos Recomendados

Gerenciamento Contínuo de Vulnerabilidade		
3.1	Utilizar uma ferramenta atualizada e compatível com o SCAP para efetuar varreduras automatizadas em todos os ativos conectados à rede com frequência semanal ou inferior. para identificar todas as vulnerabilidades potenciais nos sistemas da organização.	Detectar
3.2	Realizar varreduras por vulnerabilidades com contas autenticadas em agentes executados localmente em cada sistema, ou varreduras por *scanners* remotos que sejam configurados com privilégios elevados nos sistemas que estejam sendo testados.	Detectar

3.3	Utilizar uma conta dedicada para as varreduras por vulnerabilidades autenticadas, que não deve ser utilizada para quaisquer outras atividades administrativas e que deve ser vinculada a equipamentos específicos, em endereços IP específicos.	Detectar
3.4	Implantar ferramentas de atualização automatizada de *software*, de forma a garantir que os sistemas operacionais sejam executados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	Proteger
3.5	Implantar ferramentas de atualização automatizada de *software* de forma a garantir que os *softwares* de terceiros em todos os equipamentos sejam utilizados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	Proteger
3.6	Utilizar um processo de classificação de riscos para priorizar a remediação de vulnerabilidades descobertas.	Responder

5.5. Ciclo de Vida da Demanda

Define-se que o tempo de utilização da solução proposta deverá acompanhar parâmetros legais, vide o determinado pela Lei nº 8.666/93:

> *Art. 57. A duração dos contratos regidos por esta Lei ficará adstrita à vigência dos respectivos créditos orçamentários, exceto quanto aos relativos:*
> *(...)*
> *II – à prestação de serviços a serem executados de forma contínua, que poderão ter a sua duração prorrogada por iguais e sucessivos períodos com vistas à obtenção de preços e condições mais vantajosas para a administração, limitada a sessenta meses.*

Bem como deverá se balizar por preceitos mercadológicos para o fornecimento e manutenibilidade da mesma.

5.6. Clientes que farão uso da solução (objeto da demanda) ou serão beneficiados

A equipe técnica alocada na SETIN deverá gerir a solução contratada, por conseguinte, todo o Poder Judiciário Cearense, através dos seus usuários, serão beneficiários da mesma.

5.7.Expectativa de entrega da solução

Estima-se que a referida Solução de Tecnologia da Informação deva estar disponível em março de 2023.

6. METAS DO PLANEJAMENTO ESTRATÉGICO A SEREM ALCANÇADAS

A contratação de **Solução de gestão e análise de vulnerabilidades de ativos**, está alinhada e presente no mapa do Planejamento Estratégico do TJCE 2030 com os objetivos de:

- **FORTALECER A INTELIGÊNCIA DE DADOS E A SEGURANÇA DA INFORMAÇÃO.**

- **ANEXO II – INDICADORES E METAS DESDOBRAMENTO DA ESTRATÉGIA – SETIN**
  - **Indicador 1: Índice de Serviços Críticos com Gestão de Risco**
    - **Fortalecer a inteligência de dados e a segurança da informação**
  - **Indicador 2: Índice de conformidade com as políticas de segurança de TIC**
    - **Fortalecer a inteligência de dados e a segurança da informação**

ENCAMINHAMENTO

Em conformidade com o **art. 12°, § 7° da Resolução N° 182, de 17 de outubro de 2013 do Conselho Nacional de Justiça**, encaminha-se ao Secretário de Tecnologia da Informação para:

1. Decidir motivadamente sobre o prosseguimento da contratação;

2. Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e

3. Instituir a Equipe de Planejamento da Contratação conforme exposto no art. 2º, inciso XIII da Resolução N° 182 do CNJ.

Adarildo de Brito Figueiredo – 8025 **Área Requisitante da Solução**	Cristiano Henrique Lima de Carvalho – 5198 Área de Tecnologia da Informação

Fortaleza, (16 de agosto de 2022.)

APROVAÇÃO

I. Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante.

II. Designo como Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da Contratação o(a) servidor(a) indicado(a) no item 3 deste Documento para esta função.

III. Instituo como Equipe de Planejamento desta contratação a indicada no item 3 deste Documento.

Cristiano Henrique Lima de Carvalho – 5198
Autoridade Competente da Área Administrativa, em substituição.

Fortaleza, 19 de agosto de 2022

CIÊNCIA DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Por este instrumento declaro ter ciência das competências do INTEGRANTE DEMANDANTE/ REQUISITANTE definidas no art. 3º da Resolução nº 182/2013, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Adarildo de Brito Figueiredo – 8025
Integrante Demandante/Requisitante da Solução

Fortaleza, 26 de agosto de 2022.

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas no art. 4º da Resolução nº 182/2013, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Heldir Sampaio Silva – 9630
Integrante Técnico da Solução

Fortaleza, 26 de agosto de 2022.

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas no art. 5º da Resolução nº 182/2013, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Fábio de Carvalho Leite – 9594
Integrante Administrativo da Solução

Fortaleza, 26 de agosto de 2022.