PORTARIA PRE Nº 213, DE 16 DE SETEMBRO DE 2024

Institui Norma de Segurança Cibernética — NSC1 — Termos e Siglas de Segurança da Informação do Tribunal Regional Eleitoral de Minas Gerais.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS, no uso de suas atribuições conferidas pelo inciso XV do art. 22 da Resolução TRE-MG nº 1.277, de 29 de maio de 2024, o Regimento Interno, considerando o disposto no art. 4° da Resolução TRE-MG nº 1.240, de 6 de fevereiro de 2023, que determina que a "revisão e a atualização das normas complementares de Segurança da Informação ocorrerão sempre que necessário, por meio de portaria da Presidência do Tribunal.",

RESOLVE:

Art. 1° Fica instituída a Norma de Segurança Cibernética — NSC1 — Termos e Siglas de Segurança da Informação do Tribunal Regional Eleitoral de Minas Gerais.

Parágrafo único. A norma de segurança de que trata o *caput* estabelece os principais termos, siglas e definições utilizados em Segurança da Informação, os quais estão dispostos no Anexo desta Portaria.

Art. 2° Esta portaria integra a Política de Segurança da Informação do Tribunal Regional Eleitoral de Minas Gerais, regulamentada pela Resolução TRE-MG nº 1.240, de 6 de fevereiro de 2023.

Art. 3° Esta portaria aplica-se aos magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que utilizam os ativos de informação e de processamento na Justiça Eleitoral de Minas Gerais.

Art. 4° Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 5° Esta portaria entra em vigor na data de sua publicação.

Belo Horizonte, 16 de setembro de 2024.

Desembargador Ramom Tácio de Oliveira

ANEXO

TERMOS E SIGLAS DE SEGURANÇA DA INFORMAÇÃO

AD (*Microsoft Active Directory*)
Base de dados de identidades, autenticação e autorização utilizada internamente no TRE-MG.

AIN (Análise de Impacto no Negócio) ou BIA (*Business Impact Analysis*)
BIA (Business Impact Analysis) ou AIN (Análise de Impacto no Negócio) é um documento que registra a análise de uma disrupção na organização ao longo do tempo.

Ameaça
Situação em que um agente interno ou externo explora, de forma acidental ou proposital, uma vulnerabilidade, causando impactos negativos sobre um sistema ou recurso. Causa potencial de um incidente indesejado e que pode resultar em dano para um sistema ou organização.

Análise de riscos
A análise ou avaliação de risco é um processo sistemático que visa identificar, analisar e avaliar os riscos associados a determinadas atividades, situações ou processos, a fim de determinar a probabilidade e o impacto desses riscos e, assim, desenvolver estratégias para prevenir ou mitigá-los.

Análise de vulnerabilidade
Atividade que tem por objetivo buscar por fragilidades existentes nos ambientes, nos sistemas operacionais, nas aplicações e nas bibliotecas, componentes e infraestrutura por ela utilizados.

ANPD (Autoridade Nacional de Proteção de Dados Pessoais)
Agência Nacional de Proteção de Dados Pessoais é o órgão responsável por zelar pela proteção dos dados pessoais e por fiscalizar o cumprimento da LGPD no Brasil.

Antimalware
Programas informáticos desenvolvidos para prevenir, detectar e eliminar *malware* de computador.

Antispam
Serviço de detecção e análise que tem como objetivo bloquear o recebimento de *spam*.

API *(Application Programming Interface)*
É um conjunto de padrões, rotinas e instruções de programação que permite que softwares ou aplicativos diferentes se conectem.

Ataque de força-bruta
Tipo de ataque que busca alcançar seu objetivo (quebra de senha, tentativa de acesso indevido, etc.) por meio de um número expressivo de tentativas e combinações possíveis.

Atividades críticas
Conjunto de processos vinculados às atividades precípuas da Justiça Eleitoral, cuja interrupção pode ocasionar severos transtornos.

Atividades precípuas
Conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais,

inerentes às atividades específicas da Justiça Eleitoral, contemplando todos os ambientes existentes, no Tribunal Superior Eleitoral e nos Tribunais Regionais Eleitorais.

Ativo
Qualquer coisa que tenha valor para a organização, como exemplo, são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. É tudo aquilo que tem valor para o TRE□MG e que contribui para o alcance da sua missão institucional.

Ativo de informação
Todo dado ou informação gerado, adquirido, utilizado ou custodiado pela Justiça Eleitoral, assim como qualquer equipamento, *software* ou recurso utilizado para seu processamento ou armazenamento.

Ativo de TIC
Subconjunto de ativos que estão associados à tecnologia, à informação e à comunicação de dados e que são necessários à sustentação dos serviços de TIC.

Autenticação
Ato de comprovação da identificação por meio de um ou mais fatores (senha, biometria, certificado digital, *token*, *One-Time Password*, etc).

Autenticidade
Garantia de veracidade da fonte de informações, por meio da qual é possível confirmar a identidade das pessoas ou entidades que prestam a informação.

Autorização
Uma vez autorizado com sucesso, a credencial do usuário, programa ou dispositivo passa a ter acesso a recursos e informações previamente concedidos para ele e/ou seu perfil.

Avaliação de riscos
Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

Backbone
Infraestrutura central de interligação de equipamentos que compõem uma rede de comunicação de dados.

Back-end
É toda a parte da programação voltada ao funcionamento interno de um *software*, tudo aquilo que está por trás da interface de uma aplicação: seus sistemas, banco de dados, toda parte de segurança de dados, envio e recebimento de informações, armazenamento, etc. De maneira simplista, o *Front-end* é aquilo que você vê e com o quê você interage, ou seja, é a interface gráfica e o *Back-end* é o contrarregra por trás dessa interface, que trabalha do lado do servidor.

Backup
Cópias de segurança de informação.

***Backup* completo**
Modalidade de *backup* em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último *backup*.

***Backup* diferencial**
Modalidade de *backup* em que são salvaguardados apenas dados novos ou modificados desde o

último *backup* completo.

***Backup* incremental**
Modalidade de *backup* em que são salvaguardados apenas os dados novos ou modificados desde o último *backup* de qualquer modalidade efetuado.

Baseline
Uma baseline, ou linha de base, é um ponto de referência para monitorizar o desenvolvimento de tarefas relacionadas a um projeto. É composta por itens como escopo, cronograma e orçamento do projeto e é definida, na maioria das vezes, durante o planejamento. A partir da baseline, o gestor do projeto consegue controlar e acompanhar o que está acontecendo.

Buffer
É uma área de armazenamento de memória física usada para armazenar dados temporariamente enquanto está sendo movida de um lugar para outro.

Cache
É um dispositivo de acesso rápido, interno a um sistema, que serve de intermediário entre um operador de um processo e o dispositivo de armazenamento ao qual esse operador acessa. A principal vantagem na utilização de um cache consiste em evitar o acesso ao dispositivo de armazenamento - que pode ser demorado -, armazenando os dados em meios de acesso mais rápidos.

Central de Serviços ou *Service Desk*
Local de atendimento centralizado para esclarecimento de dúvidas, solicitação de serviços, tratamento de incidentes, e dos diversos tipos requisições de serviços de TIC disponíveis, através da abertura de chamados (ou *tickets*) pelos usuários.

Chave
É uma sequência de *bits* utilizada como parâmetro secreto no cifrador, necessária para realizar encriptação e/ou decriptação. A única maneira de descobrir uma chave deve ser por força-bruta: tentar todas as alternativas no espaço de chaves possíveis. O algoritmo utilizado pelo cifrador deve garantir que chaves longas implicam em um tempo impraticável para descobrir a chave por tentativa-e-erro.

Checksum
O *checksum*, ou soma de verificação em português, é uma técnica utilizada para verificar a integridade de dados durante a transmissão ou armazenamento. É um valor numérico calculado a partir de um conjunto de dados. O emissor calcula o valor do *checksum* e transmite o arquivo (ou pacote de dados) juntamente com o valor do *checksum*. O receptor recalcula o valor para o arquivo/pacote recebido e compara com o valor original enviado pelo emissor. Se os valores não forem iguais, significa que os dados foram alterados durante a transmissão ou armazenamento.

Cifrador
É um par de algoritmos que realizam a encriptação e a decriptação.

Cifrador assimétrico
É um cifrador que usa chaves diferentes, uma pública, uma privada, para encriptação e decriptação. Em geral mais lentos, mas com usos para assinatura e verificação de autenticidade. Exemplos: *Rivest-Shamir-Adleman* (RSA) e *Elliptic Curve Cryptography* (ECC).

Cifrador de bloco
Cifrador que opera sobre blocos de *bits* de tamanho fixo com uma transformação invariável que é especificada por uma chave simétrica.

Cifrador simétrico
É um cifrador que usa a mesma chave para encriptação e decriptação. É mais rápido, em geral. Exemplos: *Advanced Encryptation Standard* (AES) e *Data 16 Encryptation Standard* (DES).

Código Fonte
É um conjunto de instruções, escritas em uma linguagem de programação formal, que compõe um *software* escrito, ou seja, é a origem de um programa de computador.

Código malicioso
Programa ou *software* especificamente desenvolvido para executar ações danosas em um computador ou obter informações de forma ilícita.

Complexidade da senha
Diz respeito ao tamanho do conjunto de caracteres utilizado para definição da senha, o qual está diretamente relacionado ao número de combinações possíveis que podem ser geradas, dado um comprimento estabelecido. Uma senha de 3 (três) caracteres numéricos, por exemplo, permite criar 1000 (um mil) combinações. Mantendo-se o mesmo comprimento, mas usando-se as 26 (vinte e seis) letras minúsculas do nosso alfabeto, passamos para 17.576 (dezessete mil quinhentas e setenta e seis) combinações possíveis e, dessa forma, temos uma senha de maior complexidade. Outra forma de se aumentar a complexidade de senhas, para um determinado conjunto de caracteres, é aumentar o comprimento da senha.

Confidencialidade
Propriedade que assegura que a informação não esteja disponível - ou seja revelada - a indivíduos, entidades ou processos não autorizados.

Conta de acesso
Credencial utilizada para acessos a recursos e sistemas de informação. Esta terminologia pode ser usada de forma ampla para agrupar os diversos tipos de contas, como de usuário e de administrador.

Conta de administrador
Credencial com privilégio administrativo, concedida para uso pessoal e intransferível, utilizada para acesso à rede ou sistemas, sendo composta, no mínimo, por um identificador único (chamado de *login* ou simplesmente conta) e por uma senha. São contas que, de forma geral, têm poderes plenos para administração e configuração no ativo ao qual estão associadas.

Conta de serviço
Credencial utilizada para automação de processos informatizados, de uso não-pessoal, podendo ou não possuir privilégios administrativos.

Conta de usuário
Credencial sem privilégio administrativo, concedida para uso pessoal e intransferível, utilizada para acesso à rede ou sistemas, sendo composta, no mínimo, por um identificador único (chamado de *login* ou simplesmente conta) e por uma senha. Também conhecido como credenciais de acesso, é o conjunto de atributos (lógicos ou físicos) que identifica univocamente um usuário, previamente cadastrado, para concessão de acesso aos sistemas ou serviços de informação. Ex.: *login* e senha, certificado digital e senha, características biométricas etc.

Controle
Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.
NOTA: Controle é também usado como um sinônimo para proteção ou contramedida.

Controle de Acesso
Conjunto de requisitos associados a regras operacionais que estabelecem as condições para acessos físicos e lógicos no TRE-MG. De forma simplificada, foca em estabelecer quem pode acessar, quando pode acessar e o que pode ser feito durante o acesso, seja físico ou lógico, bem como requisitos complementares que possibilitam a gestão e o rastreio dos acessos.

Cookies
São pequenos arquivos de texto que os sítios criam e enviam para o navegador de um utilizador quando este visita o endereço. Armazenam informações sobre a visita do utilizador, como as suas preferências, o seu nome de utilizador e a sua senha, e ajudam a melhorar a sua experiência online.

Credenciais de acesso
Permissões concedidas por autoridade competente, que habilitam determinada pessoa, sistema ou organização ao acesso à informação ou ao recurso. A credencial pode ser física ou lógica para identificação de usuários.

Credencial padrão
Refere-se à credencial que vem por padrão embutida nos sistemas de informação e em grande parte dos ativos de TIC, como a conta Administrador do *Windows* ou o usuário *root* do *Linux*.

Criticidade
Grau de importância da informação para a continuidade das atividades precípuas da Justiça Eleitoral.

CSI
Comissão de Segurança da Informação. Tem por finalidade o planejamento, o controle e a avaliação da implantação de diretrizes e ações relacionadas à segurança da informação no Tribunal. Ver Portaria nº 329, de 9 de novembro de 2022, da Presidência.

CTIR GOV
Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

Datacenter
Ambiente composto pelos equipamentos centrais de processamento de dados (servidores e ativos de rede) que executam e armazenam a maioria dos sistemas e dados corporativos, compartilhando seus recursos para todos os usuários da organização (clientes internos e externos). Também conhecido como Centro de Processamento de Dados — CPD —, é o local onde estão concentrados os ativos de TIC responsáveis pelo processamento, armazenamento, transmissão e proteção, de forma centralizada, das informações de uma empresa ou organização.

DDL *(Data Definition Language)*
Linguagem de definição de dados (DDL na sigla em inglês) é uma linguagem de programação de computação usada para alterar ou modificar dados em um banco de dados. Em particular, DDL consiste em comandos que podem modificar estruturas, tabelas e outros formatos organizacionais.

Declaração de aplicabilidade
Declaração documentada que descreve os objetivos de controle e os controles que são pertinentes e aplicáveis ao SGSI da organização.
NOTA: Os objetivos de controle e os controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.

Decriptação
É o processo de converter texto cifrado em seu texto em claro original.

Denial of service
Negação de Serviço, causa interferência ou mal funcionamento de um sistema ou serviço.

DHCP *(Dynamic Host Configuration Protocol)*
Servidores/serviços que fornecem endereços IP e outras configurações de forma dinâmica para o ambiente de rede de computadores.

Diretório compartilhado ou área compartilhada
Espaço de armazenamento e compartilhamento de informações de um grupo de usuários específico na rede do Tribunal.

Diretório pessoal ou área privativa
Área reservada para armazenamento e compartilhamento de informações de um usuário interno, incluindo seu *e-mail*.

Diretriz
Descrição que orienta o que deve ser feito e como para se alcançarem os objetivos estabelecidos nas políticas.

Disponibilidade
Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

Disrupção
Incidente, previsto ou imprevisto, que causa um desvio não planejado e negativo da expectativa de entrega de produtos e serviços de acordo com os objetivos da organização.

DNS *(Domain Name System)*
Servidores/serviços que fazem localização e tradução de nomes de *hosts* e serviços de rede para números de endereços IP.

Elevation of privilege
Elevação de privilégio, para obter controle não autorizado sobre um sistema ou processo.

Encriptação
É o processo de converter texto em claro em texto cifrado.

Estação de trabalho
Conjunto de *hardware* e *software* fornecido ao usuário para que este possa executar suas atribuições.

ETIR (Equipe de Tratamento e Resposta a incidentes em Redes e Ambientes Computacionais)
A ETIR tem a finalidade de receber, analisar, classificar e tratar notificações e atividades relacionadas a incidentes de segurança em ambientes de computadores, responder às notificações e armazenar registros para a formação de séries históricas, como subsídio estatístico e para fins de auditoria.

Evento de segurança da informação
É uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Extranet
Porção da rede de computadores de uma empresa que faz uso da *internet* para partilhar com segurança parte do seu sistema de informação.

Fator de autenticação
Característica da informação utilizada para identificar e autorizar uma pessoa ou sistema perante outras pessoas ou sistemas. Essa característica recai, geralmente, em um de 3 (três) grupos principais: Algo que a pessoa conheça (uma senha, por exemplo), algo que a pessoa possua (geralmente um dispositivo externo como celular ou um *token* físico) ou algo que a pessoa é (inato ao nosso organismo, como digitais, íris, etc.). Outros fatores, como localização geográfica, podem ser definidos.

Firewall
É um dispositivo, podendo existir na forma de *software* ou *hardware,* que possui a função de filtrar o tráfego nocivo recebido e impedir que esses dados sejam propagados.

Framework
É uma estrutura de software abstrata que fornece um conjunto de funcionalidades genéricas. Ele pode ser usado para resolver problemas específicos e oferece uma arquitetura padrão para o desenvolvimento de aplicações.

Front-End
É toda a interface gráfica de um projeto. Em outras palavras, é a parte visual onde é desenvolvida a aplicação com que o usuário terá interação direta, seja em desenvolvimento de *software*, *sites*, aplicativos ou outros. De maneira simplista, o *Front-end* é aquilo que você vê e com o que você interage, ou seja, é a interface gráfica e o *Back-end* é o contrarregra por trás dessa interface, que trabalha do lado do servidor.

Gateway
Máquina que funciona como ponto de conexão entre duas redes.

Geolocalização
Recurso tecnológico que permite localizar qualquer objeto ou pessoa, por meio da sua posição geográfica, detectada automaticamente por um sistema de coordenadas.

Gestão de Ativos
É um conjunto coordenado de atividades voltadas para extrair valor dos ativos da empresa. Isso inclui o balanceamento de custos, oportunidades e riscos frente ao desempenho que se espera desses ativos para que sejam alcançados os objetivos da organização.

Gestão de riscos
Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.
NOTA: A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.

Gestão de Vulnerabilidades
A gestão de vulnerabilidades tem como objetivo prevenir a exploração de vulnerabilidades técnicas na rede corporativa, por meio da aplicação sistemática de ações de prevenção, identificação, classificação e tratamento.

Hacker
Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros. Dependendo dos objetivos da ação, podem ser chamados de *Cracker*, *Lammer* ou *BlackHat*.

Hardening
É o processo de mapear e reduzir as ameaças e vulnerabilidades em sistemas, aplicações, infraestruturas, redes, entre outros elementos tecnológicos.

Hardware
Equipamentos de forma geral, em particular equipamentos de tecnologia da informação.

***Hash* criptográfico**
É uma função matemática que mapeia uma entrada de tamanho arbitrário, em *bits*, para uma saída de tamanho fixo e que é utilizada para criptografia. A função também é de "mão única", no sentido de que é impossível invertê-la. A função deve ser determinística, de rápida computação e de alta entropia.

HTTP *(Hypertext Transfer Protocol)*
É um protocolo de comunicação utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da *World Wide Web*. Hipertexto é o texto estruturado que utiliza ligações lógicas entre nós contendo texto.

HTTPS *(Hypertext Transfer Protocol Secure)*
É uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais.

IaC *(Infrastructure as Code)*
Infraestrutura como código é o processo de gerenciamento e provisionamento de centros de processamentos dados usando arquivos de configuração ao invés de configurações físicas de *hardware* ou ferramentas de configuração interativas.

IAM (Identity and Access Management)
O Gerenciamento de Identidade e Acesso (*Identity and Access Management* - IAM) gerencia o ciclo de vida completo das identidades e direitos do usuário em todos os recursos da empresa, tanto em *data centers* quanto na nuvem. É um controle básico da segurança, pois autentica usuários e regula o acesso a sistemas, redes e dados.

IC (Item de configuração)
O termo item de configuração, ou IC, é qualquer componente que necessita ser configurado com o objetivo de se entregar um serviço de TI. Os ICs normalmente incluem serviços de TI, *hardware*, *software*, pessoas e documentações formais.

Identificação
Ato de informar uma credencial de um usuário para acesso a determinado recurso.

Incidente de segurança da informação
Um ou mais eventos em série de segurança da informação, indesejados ou inesperados, com grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Incidente de segurança da informação com dados pessoais
Qualquer incidente de segurança à proteção de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades de titulares de dados pessoais.

Incidente de segurança da informação grave
Incidente de segurança da informação de maior impacto para a organização, que prejudica de forma intensa a utilização dos serviços de TI ou expõe dados de forma indevida, devendo ser priorizado em relação aos demais incidentes.

Information disclosure
Este termo é frequentemente usado em avisos de vulnerabilidade para descrever uma consequência ou impacto técnico, para qualquer vulnerabilidade que tenha perda de confidencialidade. Divulgação de informação. Obter acesso à informação sem autorização.

Integridade
Propriedade que visa garantir que as informações sejam mantidas íntegras, sem modificações indevidas, acidentais ou propositais.

Internet
Rede mundial de computadores baseada em padrões abertos.

Intranet
Rede privada de computadores que segue os padrões da *internet*.

IP *(Internet Protocol)*
Internet Protocol ou Protocolo de *Internet*.

IPTV *(Internet Protocol Television)*
É um método de transmissão de sinais televisivos através de redes IP.

ITSM (*Information Technology Service Management)*
Ferramenta de *software* utilizada para gerenciamento dos serviços de TIC em uma Central de Serviços.

Janela de *backup*
Período de tempo durante o qual cópias de segurança podem ser executadas manualmente ou com agendamento.

JE (Justiça Eleitoral)
Justiça Eleitoral.

Loggin
Processo de estocagem de informações sobre eventos que ocorreram num *firewall* ou numa rede.

MFA *(Multi Factor Authentication)*
Autenticação baseada em mais de um fator. Historicamente, as concessões de acesso têm sido baseadas apenas no fator relativo ao que sabemos - senha, por exemplo - e, para melhorar a segurança, sistemas mais modernos passaram a requisitar mais de um fator de autenticação para identificar a pessoa ou sistema - senha e um certificado digital, por exemplo.

MTD (Maximum Tolerable Downtime)
MTD (Maximum Tolerable Downtime) ou PMI (Período Máximo de Interrupção Tolerável) é o tempo necessário para que os impactos adversos se tornem inaceitáveis, que pode surgir como resultado de não fornecer um produto/serviço ou realizar uma atividade.

Não-repúdio
Diz respeito à impossibilidade de negar a autoria de determinada ação.

Núcleo de segurança cibernética
Setor de segurança cibernética do TRE-MG, vinculado à Secretaria de Tecnologia da Informação.

OAuth2
É um protocolo de autorização que possibilita que aplicativos/aplicações obtenham acesso limitado a contas de usuários em um serviço HTTP sem a necessidade de enviar seu usuário e senha.

Open relay
Os servidores de correio eletrônico são classificados como *Open Relay* quando ele processa um *e-mail* onde o remetente e o destinatário não são usuários do servidor em questão.

OPR *(*Objetivo de Ponto de Recuperação*) ou RPO (Recovery Point Objective)*
É a posição (no tempo) na qual deverão estar disponíveis os dados das aplicações recuperadas após a ocorrência de uma disrupção.

OTR *(*Objetivo de Tempo de Recuperação*) ou RTO (Recovery Time Objective)*
É o período de tempo gasto pela organização para recuperar uma atividade ou processo crítico após sua interrupção.

PAM *(Privileged Access Management)*
O Gerenciamento de Acesso Privilegiado é formado por um conjunto de estratégias e tecnologias de segurança cibernética para exercer controle sobre o acesso privilegiado e permissões para usuários, contas, processos e sistemas em um ambiente tecnológico.

Patch
O termo vem do inglês e significa "remendo" ou "correção". Em computação, é um programa que atualiza ou corrige um software para melhorar a sua usabilidade ou desempenho. Podem ser usados para corrigir bugs, vulnerabilidades de segurança, incompatibilidades, ou para adicionar novos recursos.

PCN (Plano de Continuidade de Negócios)
O Plano de Continuidade de Negócios - PCN (do inglês *Business Continuity Plan* – BCP) é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual faz parte.

PCSETIC (Plano de Continuidade dos Serviços Essenciais de TIC)
O PCSETIC apresenta ações para prevenir e tratar eventos provenientes de desastres ou que impactem significativamente os Serviços Essenciais de TIC, através de um documento único e normatizado. É um plano de nível operacional que contém os detalhes para manter ou recuperar as atividades da organização frente a incidentes que causem uma disrupção.

Phishing
Técnica de fraude utilizada por criminosos para roubar senhas de banco e demais informações pessoais, usando-as posteriormente de maneira fraudulenta.

Plano de gerenciamento de backup e restauração de dados
Documento formal onde são definidos os responsáveis pela cópia dos dados, o que será armazenado, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da norma complementar da Política de Segurança da Informação para gerenciamento de *backup* e restauração de dados.

PMI (Período Máximo de Interrupção Tolerável) ou MTD (*Maximum Tolerable Downtime)*
É o tempo necessário para que os impactos adversos se tornem inaceitáveis, que pode surgir como resultado de não fornecer um produto/serviço ou realizar uma atividade.

PoC *(Proofs of Concept)*
É a evidência documentada de que um *software* pode ser bem-sucedido. Ao fazer uma PoC, é possível identificar erros técnicos que possam interferir no funcionamento e nos resultados esperados.

Política
Intenções e diretrizes globais formalmente expressas pela direção da Instituição.

Princípio de *Kerckhoffs*
Princípio que indica que a segurança deve ser estabelecida pela força da chave e não pelo segredo do método de criptografia.

Princípio do menor privilégio
Premissa de fornecer as permissões necessárias e suficientes para que um usuário possa realizar suas atividades, por um tempo limitado e com os direitosmínimosnecessários para as suas tarefas.

Privacy by default
O *software* deverá resguardar a exposição de dados pessoais salvaguardando a privacidade, sendo o mais restritivo possível tanto na exposição/visualização de dados pessoais quanto na coleta.

Privacy by design
O *Privacy by Design* é um *framework* que incorpora a proteção da privacidade no design de produtos ou serviços em todas as etapas do processo. É uma diretriz ética que garante que a privacidade seja integrada ao sistema durante todo o ciclo de desenvolvimento, incluindo permitir que o usuário tenha controle sobre seus dados.

Proxy
Servidor responsável por intermediar o acesso à *internet*, aplicando as regras de controle de acesso e mecanismos de proteção contra códigos maliciosos, previamente configurados. É responsável também por controlar a alocação de recursos de rede.

***Proxy* externo**
São servidores não administrados pelo TSE ou pelo Tribunal Regional Eleitoral, responsáveis por intermediar o acesso à *internet*, que não aplicam as regras de controle de acesso e mecanismos de proteção da mesma forma que os *proxies* administrados pelo TSE ou Tribunais Regionais Eleitorais.

PSI
Política de Segurança da Informação. Ver Resolução TRE-MG nº 1.240, de 6 de fevereiro de 2023.

RBAC *(Role Based Access Control)*
O controle de acesso baseado em função (*Role Based Access Control* - RBAC) é um método para controlar o que os usuários podem fazer nos sistemas de TI de uma empresa. O RBAC faz isso atribuindo uma ou mais "funções" a cada usuário e concedendo permissões diferentes a cada função.

RCJE (Rede Corporativa de Comunicação de Dados da Justiça Eleitoral)

Conjunto formado pelos segmentos da Rede Nacional, da Rede Regional do Tribunal Superior Eleitoral, dos Tribunais Regionais Eleitorais, dos cartórios eleitorais e de suas Redes Locais.

Recursos de processamento da informação
Qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.

Rede de computadores
Também conhecida por rede corporativa, é o conjunto de computadores, funcionalidades e outros dispositivos, de propriedade do Tribunal, que, ligados em uma rede de comunicação de dados, possibilitam a prestação de serviços de TI.

Repudiation
Repúdio, evitar responsabilidade por uma ação.

Resposta a incidentes
Ação tomada para proteger e restaurar as condições operacionais dos sistemas de informação e as informações neles armazenadas, quando ocorre um ataque ou intrusão.

REST *(Representational State Transfer)*
Protocolo para comunicação entre sistemas utilizando os métodos do protocolo HTTP.

Restauração
Processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de *backup*.

Retenção
Período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração.

Requisição AJAX
AJAX vem de *Asynchronous JavaScript And XML.* Com essa tecnologia podemos criar requisições assíncronas aos servidores seguindo basicamente o mesmo fluxo de uma requisição normal HTTP.

Requisição *POST*
É um dos métodos de requisição suportados pelo protocolo HTTP, projetado para solicitar que o servidor *web* aceite os dados anexados no corpo da mensagem de requisição para armazenamento.

RFID (Radio Frequency Identification)
É uma tecnologia pela qual os dados digitais codificados em etiquetas RFID e antenas são capturados por um leitor por meio de ondas de rádio.

Risco
Potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização.

Risco de segurança
Ameaça em potencial representada por falha ou vulnerabilidade em um ativo de TIC ou o uso indevido, intencional ou não intencional, de recursos da empresa, que possa gerar um impacto indesejado e muitas vezes crítico para a organização.

Risco residual
Risco remanescente após o tratamento de riscos.

Root
Refere-se ao usuário com o mais alto nível de privilégios em um sistema operacional. Quando você tem acesso root, você tem controle total sobre o sistema e pode modificar qualquer configuração, instalar ou desinstalar aplicativos e executar comandos privilegiados que normalmente não estão disponíveis para usuários regulares

Rotina de *backup*
Procedimento utilizado para se realizar um *backup*.

RPO (Recovery Point Objective)
RPO (*Recovery Point Objective*) ou OPR (Objetivo de Ponto de Recuperação) é a posição (no tempo) na qual deverão estar disponíveis os dados das aplicações recuperadas após a ocorrência de uma disrupção.

RTO (Recovery Time Objective) ou OTR (Objetivo de Tempo de Recuperação)
É o período de tempo gasto pela organização para recuperar uma atividade ou processo crítico após sua interrupção.

Sala-cofre
Ambiente modular estanque, testado e certificado, que protege o *data center* contra fogo, calor, umidade, gases corrosivos, fumaça, água, roubo, arrombamento, acesso indevido, sabotagem, impacto, pó, explosão, magnetismo e armas de fogo.

Salt
Em criptografia, sal (salt em inglês) é um dado aleatório que é usado como uma entrada adicional para uma função unidirecional que "quebra" os dados, uma senha ou frase-passe. Os sais são usados para proteger as senhas no armazenamento.

Salted hash
Fragmento adicionado ao conteúdo original do *hash* para que a saída mude mesmo que o conteúdo original seja o mesmo.

SAST (Static Application Security Testing)
Um conjunto de tecnologias desenvolvidas para analisar o código fonte, *byte code* e binários de aplicações buscando por indicativos de vulnerabilidades de segurança. Soluções SAST analisam a aplicação em um estado de não execução. Teste de invasão. Atividade que tem por objetivo explorar falhas e vulnerabilidades existentes na aplicação e nas bibliotecas, componentes e infraestrutura por ela utilizados, com vistas a obter acesso indevido.

Segurança cibernética
É um conjunto de ações sobre pessoas, tecnologias e processos contra os ataques cibernéticos. Por vezes nomeada como segurança digital ou segurança de TI, ela é uma ramificação na segurança da informação.

Segurança da informação
A segurança da informação — SI — está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade, autenticidade e legalidade. É um conceito mais abrangente e envolve a segurança física, segurança corporativa, segurança cibernética, entre outros.

Servidor de arquivos
Equipamento disponibilizado para acesso dos usuários da rede com o intuito de armazenar todos os documentos e mídias de cunho institucional.

SGSI (Sistema de Gestão da Segurança da Informação)
A parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.
NOTA: O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.

SIEM *(Security Information Event Management)*
Solução de *software* que faz a centralização de eventos de rede e de sistemas, com capacidade para busca e correlação entre esses eventos, possibilitando o monitoramento por parte das equipes de segurança e outros administradores de rede.

Sistema de Informação
Sistema formal adotado pela organização para coletar, processar, armazenar e disseminar dados informacionais. São exemplos de sistemas de informação o SEI, PJe, Freqweb, *Intranet*, Portal de Serviços, etc.

Sistemas administrativos
Conjunto de programas ou *software* de uso corporativo, não finalísticos e que são executados no ambiente produtivo de tecnologia da informação.

Sistemas eleitorais
Conjunto de programas ou *software* de uso corporativo que são executados no ambiente produtivo de tecnologia da informação, utilizados diretamente no processo eleitoral.

Sistemas judiciais
Conjunto de programas ou *software* de uso corporativo que são executados no ambiente produtivo de tecnologia da informação, utilizados nas atividades relacionadas à prestação jurisdicional.

***Site* ou sítio**
Primariamente, designa qualquer lugar ou local delimitado (sítio arquitetônico, sítio paisagístico, sítio histórico, entre outros), mas, quando referenciando um local numa rede de computadores (*website*), designa um sítio virtual, um conjunto de páginas virtualmente localizado em algum ponto da rede.

SOAP *(Simple Object Access Protocol)*
É um protocolo para troca de informações estruturadas em uma plataforma descentralizada e distribuída.

SOAR *(Security orchestration, automation and response)*
Possui as mesmas funções do SIEM, com capacidade adicional de abertura de chamados e automação da resposta ao incidente, como bloqueio de usuários e geração de regras de *firewall*.

***S*pyware**
Tipo de malware que monitoriza secretamente as atividades do seu computador e rouba informações pessoais sem o seu conhecimento.

Software
Conjunto de instruções e dados processado pelos computadores, também referenciado como programas, aplicativos ou sistemas.

***Softwares* de mensagens instantâneas**
São programas e serviços de comunicações *on-line* que possibilitem a troca de mensagens

textuais ou audiovisuais de forma imediata entre duas ou mais pessoas.

Spam
Prática de envio em massa de *e-mails* não solicitados.

Spoofing
É um tipo de ataque hacker em que uma pessoa se passa por outra ou por uma empresa legítima, no intuito de roubar dados, invadir sistemas e espalhar *malwares*.

SQL injection
É uma forma de ataque em sistemas, realizado via interface, no qual o usuário informa trechos de SQL em campos de texto (ou até mesmo em telas de *login* ou de pesquisa), alterando a consulta prevista pelo desenvolvedor, sendo que o atacante poderá receber privilégios especiais ou poderá manipular indevidamente o banco de dados.

Tampering
Adulteração, capacidade de alterar informação sem autorização.

Teletrabalho
Modalidade de trabalho realizado, em parte ou em sua totalidade, fora das dependências deste Tribunal, com a utilização de infraestrutura e recursos tecnológicos do usuário ou da instituição.

Terceira parte
Pessoa ou organismo reconhecido como independente das partes envolvidas, no que se refere a um dado assunto.

TIC
Tecnologia da Informação e Comunicação.

Ticket
Chamado aberto na Central de Serviços.

TLS (*Transport Layer Security)*
É um protocolo amplamente utilizado, criado para aumentar a privacidade e a segurança dos dados em comunicações pela *internet*.

Token
É um dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta *USB*. Existe também a variante para *smart cards* e *smartphones*, que é capaz de realizar as mesmas tarefas do *token*.

Tratamento do risco
Processo de seleção e implementação de medidas para modificar um risco.
NOTA: Em algumas normas o termo "controle" é usado como um sinônimo para "medida".

Unidade de armazenamento de *backup*
Dispositivo para armazenamento de dados em suporte digital com características específicas para retenção de cópia de segurança de dados digitais.

URL *(Uniform Resource Locator)*
"Localizador Uniforme de Recursos". Trata-se da indicação do endereço de umrecurso de informática disponível em uma rede, seja ela a internet□ou a□*intranet*□de uma organização.

Usuário

Quem utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral.

Usuário colaborador
Prestador de serviço terceirizado, estagiário ou qualquer outro colaborador da Justiça Eleitoral que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal.

Usuário externo
Servidor inativo, pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas no âmbito da Justiça Eleitoral.

Usuário interno
Autoridade ou servidor ativo do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo órgão.

Verificação em duas etapas
Também conhecido como autenticação de dois fatores ou duplo fator de autenticação (2FA), é um recurso de segurança disponível que fornece uma camada extra de autenticação de usuário, exigindo que os usuários forneçam informação extra para confirmar sua identificação.

VLAN *(Virtual Local Area Network)*
Recurso que permite a segmentação de uma rede física local em segmentos de redes lógicas virtuais com o objetivo de segregar tráfego e isolar ativos.

VPN *(Virtual Private Network)*
Rede Privada Virtual. É uma rede de comunicação privada construída, geralmente, sobre uma rede de comunicações pública, como, por exemplo, a *internet*. É uma espécie de túnel virtual seguro que conecta diretamente o remetente de uma informação ao seu destinatário e que emprega a criptografia para garantia da segurança do tráfego que passa por ele.

Vulnerabilidade
Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Designa também um ponto fraco ou falha existente num determinado sistema ou recurso.

Wireless
Sistema de comunicação que não requer fios para transportar sinais.

WS-ReliableMessaging
Descreve um protocolo que permite que mensagens SOAP sejam entregues de forma confiável entre aplicativos distribuídos na presença de falhas de componentes de *software*, sistema ou rede. Protocolo para entrega segura de mensagens SOAP.