Parágrafo único. Excluem-se deste Catálogo os softwares desativados e os adquiridos que não requeiram contrato de manutenção de código, tais como os de infraestrutura de TIC e os aplicativos.

Art. 19. A priorização das demandas de implantação ou desenvolvimento de sistemas ocorrerá segundo critérios objetivos previstos na Portaria TRE-AP nº 23/2020 e segundo os critérios técnicos estabelecidos pelo CGTIC.

Parágrafo único. O demandante, ao criar o formulário de solicitação de demandas informatizadas para a STI, deverá preencher os critérios estabelecidos Portaria TRE-AP nº 23/2020 e o CGTIC deverá preencher os critérios técnicos para desenvolvimento ou implantação da solução, os quais serão utilizados para priorizar a demanda internamente na STI. Eventual conflito de priorização será encaminhado ao CGOVTIC.

Art. 20. Diretrizes técnicas adicionais, inclusive de controle e garantia de qualidade, e os processos de desenvolvimento e implantação de sistemas serão descritas e mantidas em documentos a parte, disponíveis na página principal da intranet do Regional ou em site específico mantido por este Tribunal.

Art. 21. Fica revogada a Portaria TRE-AP nº 120/2021.

Art. 22. Esta portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por JOÃO GUILHERME LAGES MENDES, Presidente, em 13/03/2023, conforme art. 1º, III, "b", da Lei 11.419/2006.

PORTARIA PRESIDÊNCIA Nº 25/2023 TRE-AP/PRES/ASPRES

Portaria Presidência Nº 25/2023 TRE-AP/PRES/ASPRES

Dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Regional Eleitoral do Amapá.

O PRESIDENTE do Tribunal Regional Eleitoral Amapá, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução do Conselho Nacional de Justiça (CNJ) nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução do Tribunal Superior Eleitoral (TSE) nº 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução do Tribunal Regional Eleitoral do Amapá (TRE/AP) nº 570/2022, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral do Amapá;

CONSIDERANDO a Portaria da Diretoria Geral do TSE nº 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas da Associação Brasileira de Normas Técnicas (ABNT), ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo *Center for Internet Security* (CIS) *Controls* V.8;

RESOLVE:

Art. 1º. Instituir a norma de termos e definições, em consonância com a Política de Segurança da Informação do Tribunal Regional Eleitoral do Amapá.

CAPÍTULO I

DOS TERMOS E DEFINIÇÕES

Art. 2º Para os efeitos da Política de Segurança da Informação do Tribunal Regional Eleitoral do Amapá, aplicam-se os seguintes termos e definições:

I - *Acesso Remoto*: toda conexão estabelecida com a rede do Tribunal Superior Eleitoral (TSE) ou dos Tribunais Eleitorais originada de um ponto externo, fora das dependências do Tribunal ou de suas unidades administrativas;

II - *Agente Público*: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta;

III - *Acordo de Nível de Serviço* (ANS): Um acordo entre um provedor de serviço de tecnologia da informação e comunicação (TIC) e um cliente. O acordo de nível de serviço descreve o serviço de TIC, documenta metas de nível de serviço e especifica as responsabilidades do provedor de serviço de TIC e do cliente

IV - *Acordo de Nível Operacional* (ANO): Um acordo entre um provedor de serviço de TIC e outra parte da mesma organização. Ele dá apoio à entrega, pelo provedor de serviços de TIC a clientes e define os produtos ou serviços a serem fornecidos e as responsabilidades de ambas as partes;

V - *Administrador de Backup*: unidade responsável pelo planejamento de soluções de *backup*, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas;

VI - *Adulteração* (*Tampering*): alterar informação sem autorização;

VII - *Ameaça*: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a instituição;

VIII - *Análise de Impacto no Negócio/Business Analysis Impact* (AIN/BIA): documento que registra a análise de uma disrupção na organização ao longo do tempo;

IX - *Antimalware*: programas desenvolvidos para prevenir, detectar e eliminar *malware* de computador;

X - Antispam: serviço de detecção e análise que tem como objetivo bloquear o recebimento de *spam*;

XI - *Área Técnica*: unidade responsável pela operação técnica dos ativos e serviços de TI;

XII - *Assinatura Digital*: tipo de assinatura eletrônica que usa operações matemáticas com base em algoritmos criptográficos de criptografia assimétrica para garantir segurança na autenticidade das documentações. Para assinar digitalmente um documento é necessário possuir um certificado digital. Entre as principais vantagens do uso de assinatura digital estão o não repúdio (não deixa dúvidas quanto ao seu remetente) e tempestividade (a Autoridade Certificadora - AC pode verificar data e hora da assinatura de um documento);

XIII - *Atividades Críticas*: atividades precípuas da Justiça Eleitoral cuja interrupção ocasiona severos transtornos, como, por exemplo, perda de prazos administrativos e judiciais, dano à imagem institucional, prejuízo ao Erário, entre outros;

XIV - *Atividades Precípuas*: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Justiça Eleitoral;

XV - *Ativo Crítico*: equipamento físico, unidade de armazenamento e dados que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização;

XVI - *Ativo de Informação*: ver Ativo de TIC;

XVII - *Ativo de TIC*: 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;

XVIII - *Ativo*: qualquer bem, tangível ou intangível, que tenha valor para a organização;
XIX - *Atributos de Valor para a Sociedade*: princípios balizadores dos objetivos estratégicos e das decisões tomadas;
XX - *Autenticidade*: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
XXI - *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*;
XXII - *Backup Diferencial*: modalidade de *backup* em que são salvaguardados apenas dados novos ou modificados desde o último *backup* completo efetuado;
XXIII - *Backup Incremental*: modalidade de *backup* em que são salvaguardados apenas os dados novos ou modificados desde o último *backup* de qualquer modalidade efetuado;
XXIV - *Processo de Backup ou cópia de segurança*: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;
XXV - *Backup*: cópia de segurança de dados computacionais, que pode ser utilizada ou consultada após sua restauração, em caso de indisponibilidade, perda ou alteração dos dados originais;
XXVI - *Ciclo de Vida da Informação*: ciclo formado pelas fases de produção, recepção, organização, uso, disseminação e destinação;
XXVII - *Cifração*: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis;
XXVIII - *Código Malicioso (malware)*: termo comumente utilizado para, genericamente, se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel, cujos tipos específicos são vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de tróia e *rootkit*;
XXIX - *Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário*: responsável pela formulação, acompanhamento e revisão da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), seus indicadores e suas metas;
XXX - *Confidencialidade*: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;
XXXI - *Conta de usuário*: ver Credencial;
XXXII - *Contrato de Apoio (CA)*: Um contrato entre um provedor de serviço de TIC e um terceiro (agente externo a organização). O terceiro fornece produtos ou serviços que são necessários para a execução de um serviço de TIC a um cliente. O contrato de apoio define metas e responsabilidades que são requeridas para atender metas de nível de serviço acordadas em um ou mais acordos de nível de serviço.
XXXIII - *Contêiner dos Ativos de Informação*: local onde "vive" o ativo de informação. Geralmente, um contêiner descreve algum tipo de ativo tecnológico - *hardware*, *software* ou sistema de informação (mas também pode se referir a pessoas ou mídias como papel, CD-ROM ou DVD-ROM). Portanto, um contêiner é qualquer tipo de ativo no qual um ativo de informação é armazenado, transportado ou processado. Ele pode ser um único ativo tecnológico (como um servidor), uma coleção de ativos tecnológicos (como uma rede) ou uma coletânea de mídias digitais, entre outros;
XXXIV - *Contexto Externo*: Conjunto de circunstâncias a que o risco de segurança da informação está associado, com perspectiva focada na sociedade;

XXXV - *Contexto Interno*: Conjunto de circunstâncias a que o risco de segurança da informação está associado, com perspectiva focada apenas no ambiente interno da instituição;
XXXVI - *Continuidade de Negócios*: capacidade estratégica e tática de um órgão ou entidade de planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;
XXXVII - *Credencial (ou Conta de Acesso)*: conjunto de atributos (lógicos ou físicos) que identifica univocamente um usuário, previamente cadastrado, para concessão de acesso aos sistemas ou serviços de informação. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha, certificado digital, etc);
XXXVIII - *Criticidade*: grau de importância dos dados para a continuidade das atividades e serviços da organização;
XXXIX - *Custodiante*: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia;
XL - *CVE*: acrônimo de *Common Vulnerabilities and Exposures*, é um dicionário de vulnerabilidades com nomes padronizados para vulnerabilidades e outras informações de exposições de segurança;
XLI - *CVSS*: é um padrão criado pelo *Forum for Incident Response and Security Teams* (FIRST) para calcular a severidade de uma vulnerabilidade técnica com base em características do ambiente e ajudar na priorização das atividades de correção de acordo com os riscos;
XLII - *Decifração*: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;
XLIII - *Descarte*: eliminação correta de dados, documentos, unidades de armazenamento e acervos digitais;
XLIV - *Diretório compartilhado ou área compartilhada*: espaço de armazenamento e compartilhamento de informações de um grupo de usuários específico na rede do Tribunal;
XLV - *Diretório pessoal ou área privativa*: área reservada para armazenamento e compartilhamento de informações de um usuário interno, incluindo seu e-mail;
XLVI - *Diretriz Estratégica de Nivelamento*: determinações, instruções ou indicações a serem observadas na execução da ENTIC-JUD tendo em vista o alcance dos objetivos estratégicos;
XLVII - *Disponibilidade*: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;
XLVIII - *Disrupção:* Incidente, seja 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;
XLIX - *Divulgação de Informação (Information Disclosure)*: divulgar ou tornar a informação disponível para uma pessoa que não possua autorização;
L - *Elevação de Privilégio (Elevation of Privilege)*: obter controle não autorizado sobre um sistema ou processo:
LI - *Estação de trabalho*: conjunto de *hardware* e *software* fornecido ao usuário para que este possa executar suas atribuições;
LII - *Evento de Segurança da Informação*: Alguma mudança de estado em algum ativo ou serviço de tecnologia da informação (TI), como troca de uma senha, *log* de acesso a um serviço *web*, bloqueio da execução de um aplicativo pelo antivírus etc;
LIII - *Falsificação (Spoofing)*: capacidade de se passar por outra pessoa, processo ou sistema;

LIV - *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;
LV - *Geolocalização*: recurso tecnológico que permite localizar qualquer objeto ou pessoa, por meio da sua posição geográfica, detectada automaticamente por um sistema de coordenadas.
LVI - *Gestão de Segurança da Informação*: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade de negócios, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando à tecnologia da informação;
LVII - *Gestor da Informação*: agente público formalmente responsável pela administração de serviço de TI e pelas informações produzidas em seu processo de trabalho;
LVIII - *Governança de TIC*: conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle que visam assegurar que as decisões e ações relativas à gestão e ao uso de TIC mantenham-se harmoniosas às necessidades institucionais e contribuam para o cumprimento da missão e o alcance das metas organizacionais;
LIX - *Hora Legal Brasileira (HLB)*: gerada pelo Observatório Nacional a partir de um conjunto de 7 padrões atômicos de feixe de césio e 2 padrões atômicos de MASER de hidrogênio, é a referência brasileira das grandezas de tempo e frequência;
LX - *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;
LXI - *HTTPS (Hypertext Transfer Protocol Secure)*: é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL (*Security Socket Layer*)/TLS (*Transport Layer Security*). 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;
LXII - *Imagem de Backup*: arquivo gerado pela solução de *backup*, não necessariamente no formato original dos arquivos que contêm os dados salvaguardados;
LXIII - *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 dos titulares dos dados pessoais;
LXIV - *Incidente de Segurança da Informação*: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação ou das redes de computadores;
LXV - *Incidente Grave*: A mais alta categoria de impacto para um incidente. Um incidente grave resulta em interrupção significativa do negócio. Incidente Grave deve ter um tratamento diferente ou separado de um incidente não grave.
LXVI - *Indicadores Nacionais*: conjunto de indicadores estratégicos de resultado estabelecidos pela Rede de Governança Colaborativa do Poder Judiciário;
LXVII - *Informação*: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
LXVIII - *Iniciativa Estratégica Nacional*: programa, projeto ou operação alinhada à Estratégia Nacional de Tecnologia da Informação e Comunicação;

LXIX - *Integridade*: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;
LXX - *IPTV (Internet Protocol Television)*: é um método de transmissão de sinais televisivos através de redes IP (*Internet Protocol*);
LXXI - *Irretratabilidade (ou não repúdio)*: garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;
LXXII - *Janela de Backup*: período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;
LXXIII - *Macrodesafio de TIC*: diretriz estratégica nacional destinada a impulsionar a melhoria da infraestrutura e da governança de TIC no Poder Judiciário;
LXXIV - *Matriz RACI*: Um modelo usado para ajudar a definir papéis e responsabilidades.
LXXV - *Metas de Medição Periódica*: metas aplicáveis aos órgãos do Poder Judiciário e acompanhadas pelo CNJ para períodos predefinidos durante a vigência da Estratégia Nacional de Tecnologia da Informação e Comunicação;
LXXVI - *Metas Nacionais*: conjunto de metas estratégicas estabelecidas pela Rede de Governança Colaborativa do Poder Judiciário que permitem gerir desempenhos;
LXXVII - *Missão*: definição de finalidade da área;
LXXVIII - *Negação de Serviço (Denial of Service)*: causar interferência ou mal funcionamento de um sistema ou serviço;
LXXIX - *Objetivo de Ponto de Recuperação/Recovery Point Objective (OPR/RPO):* Posição (no tempo) na qual deverão estar disponíveis os dados das aplicações recuperadas após a ocorrência de uma disrupção;
LXXX - *Objetivo de Tempo de Recuperação/Recovery Time Point (OTR/RTO)*: Período de tempo gasto pela organização para recuperar uma atividade ou processo crítico após sua interrupção;
LXXXI - *Objetivos Estratégicos*: resultados que a TIC pretende atingir, com vistas à concretização da missão e ao alcance da visão, observando as diretrizes estratégicas do planejamento institucional do órgão;
LXXXII - *Operador de Backup*: pessoa responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de *backup*, realização de restaurações de arquivos de usuários, manutenção de troca de fitas no robô e gerenciamento de estoque de fitas locais;
LXXXIII - *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;
LXXXIV - *Período Máximo de Interrupção Tolerável/Maximum Tolerable Period of Disruption (PMIT /MTPD)*: 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;
LXXXV - *Phishing*: técnica de fraude utilizada por criminosos para roubar senhas de banco e demais informações pessoais, usando-as posteriormente de maneira fraudulenta;
LXXXVI - *Plano de Administração de Crise (PAC)*: documento disponibilizado para a alta gestão que objetiva dá mais controle para a organização em caso de uma situação de crise. Contém informações como: listas de contatos e relação de atividades das equipes envolvidas;
LXXXVII - *Plano de Continuidade de Negócios (PCN)*: documento que descreve plano focado em sustentar a missão da organização ou seus processos de negócios durante uma interrupção de suas atividades ou garantir uma rápida recuperação;

LXXXVIII - *Plano de Continuidade de Serviços de TI (PCNSTI)*: plano de nível operacional que contém os detalhes para manter ou recuperar os serviços essenciais da organização;
LXXXIX - *Plano de Continuidade Operacional (PCO)*: documento onde são definidos os procedimentos de resposta para estabilizar a situação na ocorrência de um incidente ou evento indesejado. Seu principal objetivo é identificar principais tipos de incidentes, checar a existência de procedimentos de respostas apropriados e criar procedimentos novos de contingência que ainda não existem.
XC - *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 portaria complementar da Política de Segurança da Informação para gerenciamento de *backup* e restauração de dados;
XCI - *Plano de Recuperação de Desastre (PRD)*: define os procedimentos para restaurar, no menor tempo possível, as operações de tecnologia da informação em caso de interrupção não-programada. Também devem prever os impactos da paralisação e o tempo máximo necessário para a recuperação as atividades da organização;
XCII - *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 direitos mínimos necessários para as suas tarefas;
XCIII - *Proprietário do Ativo de Informação*: refere-se à parte interessada do órgão ou entidade, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;
XCIV - *Proprietário do Risco*: Unidade Organizacional responsável pelo ativo ou processo de negócio a que o risco se refere;
XCV - *Proxy externo*: são servidores não administrados pelo TSE ou pelo Tribunal 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 Eleitorais;
XCVI - *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, e por controlar a alocação de recursos de rede;
XCVII - *Quebra de Segurança*: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;
XCVIII - *Recurso Criptográfico*: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;
XCIX - *Recurso*: conjunto formado pelos bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;
C - *Recursos de Tecnologia da Informação*: são o conjunto de bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;
CI - *Rede Corporativa de Comunicação de Dados da Justiça Eleitoral (RCJE)*: o 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;
CII - *Rede de Computadores*: rede formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema

de comunicação, ou seja, existência de dois ou mais computadores, e outros dispositivos interligados entre si de modo a poder compartilhar recursos físicos e lógicos, sendo que estes podem ser do tipo dados, impressoras, mensagens (e-mails), entre outros;

CIII - *Registro de Eventos (log)*: processo com a finalidade de registrar eventos durante o seu ciclo de vida, podendo ser gerado por sistemas operacionais, aplicações, entre outros, e armazenado durante um período pré-determinado;

CIV - *Remediação (Rollback)*: Ações tomadas para recuperação após uma mudança ou liberação que falhou. A remediação está inclusa nos planos de continuidade de serviço e/ou outras ações projetadas para permitir que o processo de negócio continue;

CV - *Repúdio (Repudiation)*: evitar responsabilidade por uma ação;

CVI - *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;

CVII - *Restauração*: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de backup;

CVIII - *Resumo Criptográfico*: resultado da ação de algoritmos que fazem o mapeamento de *bits* de tamanho arbitrário para uma sequência de *bits* de tamanho fixo menor - conhecida como resultado *hash* - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão) e que o processo reverso também não seja realizável (utilizando-se apenas o *hash* não é possível recuperar a mensagem que o gerou);

CIX - *Retenção*: período de tempo pelo qual os dados devem ser salvaguardados e estarem aptos à restauração;

CX - *Risco*: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

CXI - *Rotina de Backup*: procedimento utilizado para se realizar um *backup*;

CXII - *Security Content Automation Protocol (SCAP)*: especificação estabelecida pelo NIST (*National Institute of Standards and Technology*) para expressar e manipular dados de segurança de forma padronizada;

CXIII - *Segurança da Informação*: abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos princípios da autenticidade, da confidencialidade, da integridade, da disponibilidade e da irretratabilidade da informação, entre outras propriedades;

CXIV - *Serviço de TI*: serviço provido para um ou mais clientes por um provedor de serviços, que suporta os processos de negócios deste(s) cliente(s), é feito de uma combinação de pessoas, processos e tecnologia;

CXV - *Serviços de DHCP (Dynamic Host Configuration Protocol)*: servidores que fornecem endereços IP (*Internet Protocol*) e outras configurações de forma dinâmica para o ambiente de rede de computadores;

CXVI - *Serviços de DNS (Domain name system)*: servidores que fazem localização e tradução de nomes de hosts e serviços de rede para números de endereços IP;

CXVII - *Servidor de Arquivos*: equipamento disponibilizado para acesso dos usuários da rede com o intuito de armazenar todos os documentos e mídias de cunho institucional;

CXVIII - *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;

CXIX - *Site (ou sítio)*: conjunto de páginas web organizadas e acessíveis a partir de um URL da rede interna (intranet) ou da Internet;

CXX - *Site Principal*: centro de processamento de dados (datacenter);
CXXI - *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;
CXXII - *Softwares de Mensagens Instantâneas*: são programas e os serviços de comunicações online que possibilitem a troca de mensagens textuais ou audiovisuais de forma imediata entre duas ou mais pessoas;
CXXIII - *SPAM*: prática de envio em massa de e-mails não solicitados;
CXXIV - *Tecnologia da Informação e Comunicação (TIC)*: ativo estratégico que suporta processos institucionais, por meio da conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, fazer uso e disseminar informações;
CXXV - *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;
CXXVI - *Tratamento da Informação*: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
CXXVII - *Unidade de Armazenamento de Backup*: dispositivo para armazenamento de dados digital com características específicas para retenção de cópia de segurança de dados digitais;
CXXVIII - *Unidade de Armazenamento*: dispositivo para armazenamento de dados em suporte digital;
CXXIX - *URL*: sigla correspondente às palavras inglesas "*Uniform Resource Locator*", traduzidas para o português como "Localizador Uniforme de Recursos". Trata-se do endereço de um recurso de informática disponível em uma rede, seja ela a internet ou a intranet de uma organização;
CXXX - *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;
CXXXI - Usuário Externo: servidor inativo, pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas no âmbito da Justiça Eleitoral e que não se enquadre nas definições de Usuário Interno ou Usuário Colaborador;
CXXXII - *Usuário Interno*: autoridade ou servidor ativo do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo órgão;
CXXXIII - *Usuário*: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;
CXXXIV - *Verificação em Duas Etapas*: também conhecido como autenticação de dois fatores ou duplo fator de autenticação (2FA), é um recurso de segurança que fornece uma camada a mais de autenticação de usuário exigindo uma informação extra para confirmar sua identificação;
CXXXV - *Viabilizadores de Governança de TIC*: fatores que, individualmente ou coletivamente, tenham a capacidade de afetar o funcionamento da governança, da gestão e da infraestrutura de Tecnologia da Informação e Comunicação;
CXXXVI - *Visão*: declaração de propósito e futuro desejado, com perspectiva de longo prazo;
CXXXVII - *Vulnerabilidade de Dia Zero*: falha na segurança de um *software* que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral. Também é considerada uma Vulnerabilidade de Dia Zero a falha de segurança que já é conhecida pelo fornecedor do produto, mas para a qual ainda não existe um pacote de segurança para corrigi-la. Por não ser conhecida ou por não haver ainda um *patch* de segurança para essa falha, ela pode ser explorada por ataques em Explorações de Dia Zero. A correção deste tipo de

vulnerabilidade geralmente é tarefa do fabricante do *software*, que precisará lançar um pacote de segurança para consertar a falha;

CXXXVIII - *Vulnerabilidade*: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Parágrafo único: os termos e definições apresentados foram definidos conforme as seguintes referências: Portaria TSE nº 444/2021, Portaria GSI/PR nº 93/2019, Resolução CNJ nº 370/2021, Resolução CNJ 396/2021 e Resolução TSE nº 23.644/2021.

CAPÍTULO II

DISPOSIÇÕES FINAIS

Art. 3º Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação deste Tribunal.

Art. 4º A revisão desta portaria relativa à Política de Segurança da Informação ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal, não excedendo o período máximo de 3 (três) anos.

Art. 5º Esta portaria será publicada no portal de *Intranet* do Tribunal Regional Eleitoral do Amapá.

Art. 6º Esta portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por JOÃO GUILHERME LAGES MENDES, Presidente, em 13/03/2023, conforme art. 1º, III, "b", da Lei 11.419/2006.

PORTARIA PRESIDÊNCIA Nº 50/2023 TRE-AP/PRES

Portaria Presidência Nº 50/2023 TRE-AP/PRES/DG/SGP/COPES/SRFD

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ, no uso de suas atribuições que lhe são conferidas pelo artigo 7º da Resolução TRE/AP nº 393/2011,

RESOLVE:

Art. 1º Fixar o número de vagas para a concessão de Auxílio-Bolsa de Estudos aos servidores ocupantes de cargo efetivo e os removidos para este Tribunal, para os cursos de graduação e pós - graduação, no processo seletivo de 2023, conforme quadro abaixo:

CURSO	VAGAS
Graduação	01
Pós-Graduação *Latu Sensu*	03

Art. 2º As inscrições estarão abertas no período de 20/03 a 03/04/2023 e o processo seletivo será regulamentado por meio de Edital publicado pela Escola Judiciária Eleitoral-EJE , em consonância com a Resolução TRE/AP nº 393/2011 .

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por JOÃO GUILHERME LAGES MENDES, Presidente, em 15/03/2023, conforme art. 1º, III, "b", da Lei 11.419/2006.

PORTARIA PRESIDÊNCIA Nº 45/2023 TRE-AP/PRES

Portaria Presidência Nº 45/2023 TRE-AP/PRES/DG/SGP/COPES/SRFD

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ, no uso de suas atribuições legais definidas pelo Regimento Interno desta Corte e, tendo em vista o contido no P.A. nº 0000490-85.2023.6.03.8000,

RESOLVE:

Artigo 1º Oficializar as substituições dos servidores abaixo nominados, referentes ao mês de fevereiro de 2023, conforme planilha a seguir:

Substituto	Titular	Cargo	Período	Motivo