TRIBUNAL DE CONTAS DO ESTADO

RESOLUÇÃO ADMINISTRATIVA RA-TC Nº 06/2022

Institui a Política de Segurança da Informação no âmbito do Tribunal de Contas da Paraíba.

O TRIBUNAL DE CONTAS DO ESTADO - TCE-PB, no exercício de suas atribuições, constitucionais e legais, conferidas pelo art. 3º da Lei Complementar 18/93-LOTCE/PB, e pelo inciso III do art. 4º c/c o art. 133, ambos do Regimento Interno do Tribunal de Contas do Estado da Paraíba, e

CONSIDERANDO que a Constituição garante o acesso à informação e a proteção aos dados pessoais, no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216;

CONSIDERANDO o que estabelece a Lei de Acesso à Informação (LAI), Lei n. 12.527, de 18 de novembro de 2011, e a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018;

CONSIDERANDO os avanços tecnológicos vivenciados e a disponibilidade desta Corte em dotar o controle externo e as atividades internas de ferramentas de informação que dinamizam as atividades, isso em conformidade com o Plano Estratégico 2022-2024 aprovado pela Resolução Administrativa RA - TC nº 04/2022;

CONSIDERANDO a necessidade de estabelecer princípios, diretrizes e requisitos gerais que promovam a gestão de processos voltados à segurança da informação, privacidade e proteção de dados, que sejam periodicamente revistos;

CONSIDERANDO que a informação, em todo o seu ciclo de vida, constitui bem estratégico para o desempenho das atribuições constitucionais do Tribunal;

R E S O L V E:

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º. A Política de Segurança da Informação tem como objetivo assegurar, por meio de princípios, diretrizes, normas e ações, que toda a informação coletada, gerada, adquirida e armazenada, própria ou custodiada, por meio de tecnologias, procedimentos, pessoas e ambientes do Tribunal de Contas da Paraíba (TCE/PB), seja tratada como parte do

seu patrimônio e protegida quanto aos aspectos de autenticidade, confidencialidade, integridade e disponibilidade, bem como de proteção de dados pessoais.

Art. 2º. Para fins de aplicação da Política no âmbito do Tribunal, serão adotadas as definições do art. 5º da Lei nº 13.709/2018, do art. 5º da Lei nº 12.965/2014, do art. 4º da Lei nº 12.527/2011 e os constantes do Anexo II desta Resolução.

Art. 3º. Estão sujeitos à Política de Segurança da Informação do Tribunal:

I – Conselheiros, conselheiros-substitutos, procuradores, servidores, colaboradores, estagiários e prestadores de serviços do Tribunal de Contas;

II – qualquer pessoa física ou jurídica, pública ou privada, que venha a ter acesso a dados, informações e ativos de informação do Tribunal de Contas.

Art. 4º. Todos deverão observar as diretrizes, normas e procedimentos de segurança da informação e proteção de dados concernentes à política de que trata esta Resolução, e serão responsáveis por garantir a segurança dos dados e informações a que tenham acesso.

Art. 5º. Na gestão da segurança da informação deverão ser observadas as seguintes normas e referências legais:

I - Lei n. 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

II - Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet Brasileira), que estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

III - Lei n. 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências;

IV - Lei n. 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso à informação;

V – Resolução Administrativa TC-06/2013 que dispõe sobre o Código de Ética do TCE-PB;

VI – Resolução Administrativa TC-01/2018 que Institui e disciplina o funcionamento do Comitê Gestor de Tecnologia da Informação do TCE-PB;

VII – Resolução Administrativa TC-07/2021 que Institui a Política de proteção de dados pessoais do TCE-PB;

VIII - as normas da ABNT vigentes e pertinente à presente Política de Segurança da Informação, especialmente as da família ABNT NBR ISO/IEC 27000.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 6º. A Política de Segurança da Informação rege-se pelos seguintes princípios:

I – transparência: as diretrizes, as normas e os procedimentos da política de segurança da informação e proteção de dados, além de publicados, devem ser amplamente divulgados aos usuários a fim de orientarem o desempenho de suas atribuições;

II – celeridade: as ações de segurança da informação e proteção de dados devem oferecer respostas tempestivas a incidentes e falhas;

III – ciência: todos os usuários devem ter conhecimento sobre as normas, os procedimentos, as orientações e demais informações que permitam a execução de suas atribuições sem comprometimento da segurança de dados, informações e ativos de informação do Tribunal de Contas;

IV – clareza: as regras sobre a segurança da informação e proteção de dados devem adotar linguagem simples, precisa, concisa, acessível e de fácil entendimento;

V – criticidade: princípio de segurança que define a importância da informação para a continuidade das atividades da instituição;

VI – dignidade da pessoa humana: devem ser respeitados todos os direitos e interesses legítimos dos usuários;

VII – Impessoalidade: a Política de Segurança da Informação não será utilizada para finalidades particulares ou para a obtenção de benefícios ou promoção pessoais;

VIII – legalidade: a Política de Segurança da Informação observará a política institucional, os atos normativos, os procedimentos e as instruções formalmente estabelecidos pelo Tribunal de Contas;

IX – publicidade: Os dados acessíveis ao público terão consulta facilitada inclusive através de dados abertos

X – moralidade: a Política de Segurança da Informação deverá observar os preceitos da boa-fé, da boa administração pública e estar pautada pela atuação ética e nos ideais de honestidade, probidade e justiça;

XI – não discriminação: o tratamento de dados não deve ser realizado com fins discriminatórios ilícitos ou abusivos;

XII – proporcionalidade: o custo das ações de segurança da informação, comunicação, privacidade e proteção de dados não deve ser maior do que o valor do ativo da informação a ser protegido, salvo os casos formalmente analisados e justificados durante o processo de Gestão de Riscos;

XIII – privacidade: informações relativas à intimidade, à integridade e à honra dos cidadãos devem ser resguardadas, de acordo com a legislação vigente.

CAPÍTULO III

DAS INSTÂNCIAS ADMINISTRATIVAS

Art. 7º São instâncias administrativas envolvidas na gestão da Segurança da Informação:

I - Presidente do Tribunal de Contas do Estado da Paraíba;

II - Comitê Gestor de Tecnologia da Informação no âmbito do Tribunal de Contas do Estado da Paraíba (CGTI);

III - Comitê Gestor de Privacidade e Proteção de Dados Pessoais do Tribunal de Contas do Estado da Paraíba (CGPPD);

IV – Assessoria Técnica do Tribunal (ASTEC);

V - Gestão da Informação (GI);

VI - Encarregado de dados (Lei n. 13.709, de 14 de agosto de 2018).

Parágrafo único. Sem prejuízo do disposto neste normativo, a composição e as atribuições das instâncias administrativas são estabelecidas em instrumentos próprios.

CAPÍTULO IV
DA ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO

Art. 8º. A estrutura normativa da Segurança da Informação é composta por dois níveis de governança, a saber:

I – A política de segurança da informação instituída por meio desta Resolução, detalhada em Normas de Segurança da Informação, aprovadas por Portaria do Presidente;

II – Normas de Segurança da Informação (NSI) que estabelecem as obrigações e os procedimentos que devem ser observadas nas diversas instâncias em que a informação seja tratada, que poderá ser complementada para a sua operacionalização, através de instruções técnicas de uso interno.

Art. 9º. A ASTEC, com a colaboração dos setores do Tribunal, deverá elaborar e manter atualizadas as NSI sobre: dispositivos móveis e trabalho remoto, contrato de terceirizados, gestão de equipamentos, classificação da informação, tratamento de mídias removíveis, controle de acesso lógico, criptografia, segurança física e do ambiente, segurança nas operações, segurança na rede (internet e intranet), comunicação e transferência de informação, ciclo de vida de aplicações adquiridas e desenvolvidas, gestão de incidentes e plano de continuidade.

Parágrafo único. A ASTEC poderá elaborar outras NSIs, a depender do surgimento das demandas.

Art. 10. As normas de segurança da informação serão elaboradas e submetidas para a aprovação do Presidente que poderá encaminhar para deliberação do CGTI e/ou CGPPD.

Art. 11. A Política de Segurança da Informação será complementada por Instruções Técnicas, elaboradas pela ASTEC, as quais integrarão a presente política.

Art. 12. Os membros e os servidores do Tribunal poderão encaminhar para a Presidência, propostas de alteração ou criação de normas sobre segurança da informação (NSI) que poderá encaminhar para deliberação do CGTI e/ou CGPPD.

CAPÍTULO V

DAS DIRETRIZES

Art. 13. A política de segurança da informação deverá ser revisada e atualizada a cada período de 2 (dois) anos, ou a qualquer tempo em resposta às mudanças do ambiente organizacional, às circunstâncias, às condições legais, ou ao ambiente de tecnologia, e deverá ser amplamente divulgada para o público de interesse descrito no art. 3° desta resolução.

Art. 14. O descumprimento às disposições desta política de segurança da informação, bem como às suas normas complementares e violações aos controles de segurança por ela estabelecidos, caracterizam infração funcional a ser devidamente apurada no âmbito administrativo, sem prejuízo das sanções cíveis e penais cabíveis.

Art. 15. As funções conflitantes e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização. — ABNT 27002- item 6

CAPÍTULO VI

DA GESTÃO DE RISCO

Art. 16. A gestão de risco deverá ser um processo contínuo de planejamento, execução, verificação e revisão das ações, com o objetivo de manter em níveis aceitáveis os riscos de segurança da informação e proteção de dados.

Art. 17. As ações serão estabelecidas em função dos riscos de impacto nas atividades e objetivos institucionais do Tribunal, considerando os aspectos tecnológicos, financeiros e de qualidade.

Art. 18. O Tribunal deverá proteger os dados pessoais coletados ou que estejam sob sua custódia de acessos não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que possa afetar a privacidade do titular.

Art. 19. Na ASTEC, o Grupo de infraestrutura e segurança de TI é o responsável por receber, analisar, executar as ações necessárias e responder às notificações de incidentes que envolvam implementação de controles de segurança da informação e proteção de dados, bem como atuar de forma preventiva a incidentes dessa natureza.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 20. Todos os contratos, convênios, acordos e instrumentos congêneres firmados pelo Tribunal de Contas deverão conter cláusulas exigindo a observância desta Resolução e de seus normativos, bem como estabelecer como obrigação a sua divulgação aos

seus empregados e prepostos envolvidos nas atividades que envolvam a utilização de dados ou informações do Tribunal.

Art. 21. Esta Resolução entra em vigor na data de sua publicação.

Publique-se, registre-se e cumpra-se.
Sessão Ordinária do Tribunal Pleno.
João Pessoa, 1º de junho de 2022.

Conselheiro **Fernando Rodrigues Catão**
Presidente

Conselheiro **Arnóbio Alves Viana**

Conselheiro **Antônio Nominando Diniz Filho**

Conselheiro **Fábio Túlio Filgueiras Nogueira**

Conselheiro **André Carlo Torres Pontes**

Conselheiro **Antônio Gomes Vieira Filho**

Conselheiro em exercício **Antônio Cláudio Silva Santos**

Bradson Tibério Luna Camelo
Procurador-Geral do Ministério Público de Contas em exercício

ANEXO I

CONTEÚDOS MÍNIMOS DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO (NSI)

NSI sobre dispositivos móveis e trabalho remoto deverá considerar, entre outras questões: definição de seu objetivo; registros dos dispositivos móveis; cuidados quanto à instalação de software e aplicações de patches; controle de acesso; proteção contra malware; backups; o ambiente e a segurança física no local do trabalho remoto; os requisitos de segurança do acesso remoto aos sistemas internos da organização; o uso de redes domésticas e equipamentos de propriedade; acordos de licenciamento de software e requisitos de firewall e proteção antivírus.

A NSI de contrato de terceirizados (estagiários e colaboradores) deverá considerar, entre outras questões: definição de seu objetivo; verificação das qualificações acadêmicas e profissionais; certidões negativas de registros civis e criminais; termo de confidencialidade ou de não divulgação; cláusulas de confidencialidade e sigilo nos contratos (inclusive após o encerramento da sua vigência) e capacitação introdutória sobre o sistema de segurança da informação da organização.

NSI sobre gestão de equipamentos deverá considerar, entre outras questões: definição de seu objetivo; sejam adequadamente inventariados; plano de manutenção periódica de equipamentos; procedimento para excluir/destruir e controle de entrega e devolução.

NSI de classificação da informação deverá considerar, entre outras questões: definição de seu objetivo; requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada e os rótulos da classificação e reclassificação quando necessário.

NSI sobre tratamento de mídias removíveis deverá considerar, entre outras questões: definição de seu objetivo; indicar os casos de utilização; procedimento para reutilização e descarte; uso de criptografia de acordo com a classificação da informação e os cuidados necessários quando for necessário a mídia sair do ambiente da organização.

NSI de Controle de acesso lógico deverá considerar, entre outras questões: definição de seu objetivo; autenticação dos usuários; autorização de acesso; remoção/alteração dos direitos de acesso; critérios de qualidade de senhas; casos de uso de certificação digital e monitoramento do acesso.

NSI sobre Criptografia deverá considerar, entre outras questões: definição de seu objetivo; os padrões adotados; criptografia para os backups responsáveis pela geração e guarda; procedimentos para chaves comprometidas, perdidas, corrompidas e arquivadas.

NSI de segurança física e do ambiente deverá considerar, entre outras questões: definição de seu objetivo; adequação física para proteção de ação criminosa ou incidentes naturais; climatização; instalações elétricas; cabeamento lógico; controle de acesso remoto e físico; sistemas de alarme; plano de manutenção, remoção e descarte.

NSI sobre segurança nas operações deverá considerar, entre outras questões: definição de seu objetivo; procedimentos de backup dos dados, softwares e das imagens do sistema; frequência, abrangência e local de guarda dos backups; monitoramento do desempenho dos recursos disponíveis e projeções para garantir a sua capacidade futura; definição de ambientes de desenvolvimento e de produção; controles de detecção e conscientização de usuários contra malware e registros de eventos (logs).

NSI de segurança na rede (internet e intranet) deverá considerar, entre outras questões: definição de seu objetivo; utilização de firewalls; segregação de redes; VPN e rede wireless.

NSI sobre comunicação e transferência de informação deverá considerar, entre outras questões: definição de seu objetivo; uso de e-mail institucional e requisitos básicos dos acordos formais de transferência e compartilhamento de informações com entidades externas.

NSI do ciclo de vida de aplicações adquiridas e desenvolvidas deverá considerar, entre outras questões: definição de seu objetivo; pilha de tecnologia para cada aplicação; documentação das aplicações; controle de versões; procedimento de suporte e plano para manutenção.

NSI sobre gestão de incidentes deverá considerar, entre outras questões: definição de seu objetivo; tipos de notificação de incidentes; modelo das notificações; meio de comunicação e registro das notificações e ações realizadas.

NSI do plano de continuidade deverá considerar, entre outras questões: definição de seu objetivo; redundâncias, relatório de impacto de proteção de dados pessoais; plano de continuidade e plano de gerenciamento de incidentes.

ANEXO II

GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

ATIVO – qualquer coisa que tenha valor para a organização.

ATIVO CRÍTICO – ativo do qual o Tribunal depende, em maior ou menor grau, para a continuidade de suas atividades e seus serviços.

ATIVOS FÍSICOS – equipamentos, tais como servidores de rede e equipamentos de armazenamento de dados, responsáveis pelo processamento, armazenamento e pela transmissão de dados no âmbito do Tribunal.

ATIVO DE REDE – equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores.

ATIVOS DE INFORMAÇÃO – os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários para isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos a que eles têm acesso.

AUTENTICAÇÃO – processo que busca verificar a identidade digital de uma entidade de um sistema no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já predefinidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo. Podem ser utilizados fatores múltiplos de autenticação, a exemplo de certificação digital, informações biométricas, login e senha.

AUTORIZAÇÃO – é o direito ou permissão de acesso a um recurso de um sistema. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence.

AVALIAÇÃO DE RISCOS – processo de comparar o risco estimado com critérios de risco predefinidos, para determinar a importância do risco.

BACKUP OU CÓPIA DE SEGURANÇA – conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.

BLOQUEIO - suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

CICLO DE VIDA DE APLICAÇÕES - Consiste em todas as etapas ao longo de sua trajetória, desde a ideia inicial até o abandono do software pelos seus usuários. Este processo passa pelo design, implementação, manutenção e, eventualmente, retirada do serviço e descarte.

CLASSIFICAÇÃO DA INFORMAÇÃO – identificação dos níveis de proteção das informações e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.

CÓDIGO MALICIOSO – programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente por meio de exploração de alguma vulnerabilidade de sistema.

COMUNICAÇÃO DE DADOS – transmissão, emissão ou recepção de dados ou informações de qualquer natureza por meios confinados, por radiofrequência ou por qualquer outro processo eletrônico ou eletromagnético ou ótico.

CONFIDENCIALIDADE – propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, a órgãos ou a entidades não autorizados ou não credenciados.

CONSCIENTIZAÇÃO – atividade que tem por finalidade orientar sobre o que é segurança da informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do TCE/PB, minimizar os danos e reduzir eventuais prejuízos.

CONSENTIMENTO – manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

CONTROLE DE ACESSO – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Por regra, requer procedimentos de autenticação.

CREDENCIAL DE ACESSO – recursos que identifiquem univocamente determinado usuário nos mais variados cenários: usuário/senha de rede, crachá, carimbo, correio eletrônico, certificado digital.

CREDENCIAMENTO – processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.

CRIPTOGRAFIA – arte de proteção da informação por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem.

CUSTÓDIA – consiste na responsabilidade de se guardar um ativo para terceiros. A custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros.

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.

DADOS ABERTOS - dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte.

DESASTRE – evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, causando perda para toda ou parte da organização e gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.

DESCARTE – eliminação correta de informações, documentos, mídias e acervos digitais.

DISPONIBILIDADE – propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

ELIMINAÇÃO – exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

GRUPO DE INFRAESTRUTURA E SEGURANÇA DE TI – grupo de pessoas, lotados na ASTEC, com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, privacidade e proteção de dados.

ESTIMATIVA DE RISCOS – processo utilizado para atribuir valores à probabilidade e às consequências de um risco.

GESTÃO DE RISCOS – processo de natureza permanente que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

INCIDENTE – evento, ação ou omissão que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso

da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica.

INFORMAÇÃO – dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

LINGUAGEM SIMPLES - é um estilo de escrita que permite ao leitor entender facilmente o que está escrito. A linguagem simples tem por objetivo ser fácil de ler, entender e usar.

LOG OU REGISTRO DE AUDITORIA – registro de eventos relevantes em um dispositivo ou sistema computacional.

MEDIDAS DE SEGURANÇA – medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo.

MÍDIA – mecanismos em que dados podem ser armazenados além da forma e da tecnologia utilizada para a comunicação – inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos, que são diferentes tipos de mídia.

NOTIFICAÇÃO DE INCIDENTE – ato de informar eventos ou incidentes para o Grupo de Infraestrutura e segurança de TI.

PATCHES – pequena correção executada pelo administrador da rede em um software, com as instruções do fabricante do software.

PERFIL DE ACESSO – conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

PILHA DE TECNOLOGIA – conjunto de tecnologia escolhida para desenvolvimento de uma aplicação tais como: linguagem de programação, banco de dados, frameworks, bibliotecas e servidor da aplicação que serão utilizados

PLANO DE CONTINUIDADE – documentação dos passos estratégicos e táticos de um órgão ou entidade de 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.

PLANO DE GERENCIAMENTO DE INCIDENTES – documentação dos procedimentos e informações necessárias para que o TCE/PB mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes.

PORTAL – endereço eletrônico do Tribunal de Contas na Internet, que funciona como aglomerado de informações referentes ao Tribunal e ao controle externo. Pode ser constituído

por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia

PRESTADOR DE SERVIÇO – pessoa envolvida com o desenvolvimento de atividades, de caráter permanente ou eventual, que poderá receber credencial especial de acesso.

RECURSOS DE TECNOLOGIA DA INFORMAÇÃO – são equipamentos, instalações, sistemas adquiridos e/ou desenvolvidos, dados e informações mantidas ou operadas em meio informatizado.

REDE INTERNA – conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação.

REDE DE TELECOMUNICAÇÕES – conjunto operacional contínuo de enlaces e equipamentos, incluindo funções de transmissão, comutação ou quaisquer outras indispensáveis à operação de Serviço de Telecomunicações.

REDUNDÂNCIA – medidas de adicionar componentes ou funcionalidades à infraestrutura de TI para garantir continuidade e disponibilidade de um serviço quando um dispositivo ou componente principal falha.

SCRIPTS – conjunto de instruções, em geral escritos para automatizar alguma atividade.

SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO – provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação.

SISTEMA CORPORATIVO – sistema informatizado criado ou adquirido pelo Tribunal de Contas para a consecução das suas atividades institucionais e administrativas.

TECNOLOGIA DA INFORMAÇÃO – ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações.

TRATAMENTO DE INCIDENTES – serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar as análises dos incidentes, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências com propostas de ações para evitar ou reduzir o risco de novo incidente.

TRILHA DE AUDITORIA – registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento.

USUÁRIO – são considerados usuários os servidores efetivos, comissionados, cedidos, requisitados, estagiários, e empregados de empresas contratadas para prestar serviços no âmbito do TCE/PB que se utilizem dos recursos de tecnologia da informação do Tribunal.

USUÁRIO EXTERNO – são considerados usuários externos as pessoas designadas pelo jurisdicionado que utilizem dos recursos de tecnologia da informação do Tribunal.

USUÁRIO VISITANTE COM DISPOSITIVO MÓVEL – agentes públicos ou não que utilizem dispositivos móveis, de sua propriedade ou do órgão ou entidade a que pertencem, dentro dos ambientes físicos do TCE/PB dos quais não fazem parte.

VAZAMENTO DE DADOS – transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo. O termo pode ser usado para descrever dados que são transferidos eletronicamente ou fisicamente. Pode ocorrer de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso).

VÍRUS – seção oculta e autorreplicante de um software de computador, geralmente utilizando lógica maliciosa, que se propaga pela infecção de outro programa. Necessita que o seu programa hospedeiro seja executado para se tornar ativo.

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

WORM – programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de programas instalados em computadores.