ESTADO DA PARAÍBA
TRIBUNAL DE JUSTIÇA
GABINETE DA PRESIDÊNCIA

Resolução Nº 32 de 2022.

DJe Eletrônico
Disponibilização: quinta-feira, 01 de setembro de 2022
Publicação: sext a-feira, 02 de setembro de 2022

Dispõe sobre a atualização da Política de Segurança da informação do Poder Judiciário do Estado da Paraíba.

O **PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA**, no uso de suas atribuições constitucionais, legais e regimentais, e

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

CONSIDERANDO os termos da Resolução CNJ nº 370/2021, que Instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a necessidade de se implementar ações para garantir a adequada execução da Lei nº 13.709/2018 (LGPD), no que tange à Segurança da Informação;

CONSIDERANDO a Instrução Normativa nº 54/2013 do CNJ, que dispõe sobre o uso dos recursos de tecnologia da informação e comunicação do CNJ e dá outras providências;

CONSIDERANDO a Norma ISO/IEC 27002, traduzida pela Associação Brasileira de Normas Técnicas em ABNT NBR ISO/IEC 27002, que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da Segurança da Informação em instituições de qualquer esfera;

CONSIDERANDO a Norma Complementar nº 17/IN01/DSIC/GSIPR, de 10 de abril de 2013, que estabelece diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF), bem como a ampliação do conhecimento de seus profissionais, a troca de experiências, a capacitação e a consequente evolução da SIC nos órgãos e entidades da APF;

CONSIDERANDO a Lei 9.609/98 (Lei do Software), que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização e dá outras

providências;

CONSIDERANDO a necessidade de estabelecer políticas, diretrizes e procedimentos de segurança da informação, com vistas a oferecer um ambiente tecnológico com níveis aceitáveis de controle e confiabilidade, de forma a disponibilizar as informações necessárias aos processos de trabalho deste Tribunal com garantias de integridade, de disponibilidade, de confidencialidade, de autenticidade e de legalidade;

CONSIDERANDO a importância dos ativos de informação e a necessidade de regular a concessão de acessos aos sistemas informatizados e à rede de computadores; o uso da Internet e seus recursos; a utilização do serviço de correio eletrônico corporativo; bem como o controle, monitoramento e auditoria de segurança da informação no âmbito deste Tribunal;

CONSIDERANDO o dever do Estado de proteção das informações pessoais dos cidadãos.

RESOLVE:

Art. 1º Regulamentar a Política de Segurança da Informação (PSI) no âmbito do Poder Judiciário do Estado da Paraíba, composta por normas e procedimentos complementares editados por este Tribunal de Justiça.

CAPÍTULO I
DA VISÃO GERAL E DEFINIÇÕES

Art. 2º A PSI do TJPB é um conjunto de diretrizes que inclui, além desta PSI principal, normas e procedimentos complementares, que regulamentam o uso adequado dos recursos de tecnologia da informação deste Tribunal, conferindo direitos, deveres e responsabilidades a todos quantos deles desfrutem, devendo ser conhecida, compreendida e obedecida por todos os usuários dos recursos de tecnologia da informação do TJPB.

Art. 3º O uso adequado dos recursos de tecnologia da informação visa garantir a continuidade da prestação jurisdicional deste Tribunal.

Art. 4º Para efeito desta Resolução, aplicam-se as seguintes definições:

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

II - **Ativo:** elemento, tangível ou intangível, que tenha valor para a organização;

III - **Ativo de TI crítico:** são recursos computacionais que processam, armazenam e transmitem informações essenciais para que o TJPB alcance seus objetivos mais importantes e sensíveis no tempo, tais como aplicações, sistemas de informação, computadores, servidores e equipamentos de conectividade da infraestrutura;

IV - **Comitê de Gestão de Tecnologia da Informação – CGTI:** comitê que tem como principal objetivo elaborar planos táticos e operacionais, análise técnica de demandas, acompanhamento da execução de planos, projetos e ações que envolvam tecnologia da informação;

V - **Comitê de Segurança da Informação (CSI)**: equipe multidisciplinar, subordinada à Presidência, com responsabilidade de deliberar, conduzir e fiscalizar as ações de segurança da informação no TJPB;

VI - **Controle/Proteção/Contramedida:** forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

VII - **Coordenador de Segurança da Informação:** é o responsável pelas ações técnico-científicas de segurança da informação no TJPB e pela Coordenação de Segurança da Informação;

VIII - **Evento de Segurança da Informação:** ocorrência identificada de um sistema, serviço ou rede, que indica 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;

IX - **ETIR**: Equipe de Tratamento e Resposta a Incidentes de Segurança de Cibernética - denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem a tecnologia;

X - **Gestão de Riscos:** atividades coordenadas para direcionar e controlar uma organização no que se refere aos riscos, incluindo a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos;

XI - **Incidente de Segurança da Informação:** é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XII - **Política de Mesa Limpa e Tela Protegida:** procedimento de controle da segurança no âmbito da mesa de trabalho do usuário, incluindo o bloqueio da tela do computador com uso de senha e o cuidado com os papéis deixados sobre a mesa;

XIII - **Política de Segurança da Informação (PSI):** conjunto de diretrizes, podendo incluir normas, procedimentos e políticas auxiliares, que regulamentam o uso adequado dos recursos de tecnologia da informação.

XIV - **Processo de Elaboração, Acompanhamento e Revisão da PSI:** processo de gestão de TI que visa instituir os procedimentos para elaboração, revisão e acompanhamento do cumprimento das diretrizes da PSI;

XV - **Recursos de Tecnologia da Informação do TJPB:** todo e qualquer dispositivo ou sistemas de *software* que processe informações dentro dos domínios administrativos do TJPB, incluindo computadores, *notebooks*, impressoras, rede de comunicação de dados, dispositivos de armazenamento de dados, serviços de armazenamento de dados via rede, serviço de e-mail institucional, entre outros;

XVI - **Risco:** combinação da probabilidade e impacto de um evento ocorrer;

XVII - **Segurança da Informação:** refere-se a medidas que visam a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, incluindo a preservação da disponibilidade, da confidencialidade e da integridade das informações e dos sistemas;

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

CAPÍTULO II
DOS PRINCÍPIOS

Art. 5º A utilização dos recursos de tecnologia da informação do TJPB é pautada pelos princípios de celeridade, ética, segurança, responsabilidade e legalidade.

Parágrafo único. A regra prevista no *caput* deste artigo não exclui a adoção de outros princípios específicos, a exemplo da disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade e auditabilidade das informações produzidas, recebidas, armazenadas, tratadas ou transmitidas pelo TJPB, no exercício de suas atividades e funções.

CAPÍTULO III
DA UTILIZAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 6º O uso adequado dos recursos de tecnologia da informação visa garantir a continuidade da prestação jurisdicional deste Tribunal.

Art. 7º Os recursos de tecnologia da informação e comunicação, pertencentes ao TJPB e que estão disponíveis para os usuários, devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

Art. 8º A utilização dos recursos de tecnologia da informação e comunicação é passível de monitoramento e controle por parte deste Tribunal, respeitando, em todo caso, os

preceitos da Lei Geral de Proteção de Dados.

Art. 9º. As informações produzidas por usuários, no exercício de suas atividades e funções, são patrimônio intelectual do Tribunal, não cabendo a seus criadores qualquer forma de direito autoral.

CAPÍTULO IV
DOS OBJETIVOS E DA ABRANGÊNCIA

Art. 10. A PSI do TJPB tem como objetivos:

I - declarar, formalmente, o compromisso deste Tribunal com a segurança da informação;

II - garantir a confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade, auditabilidade e conformidade legal das informações em todos os níveis de atividades desenvolvidas;

III - estabelecer diretrizes e controles para o tratamento dos riscos referentes à violação da privacidade dos usuários, interrupções de serviços essenciais, revelação de informações sensíveis, modificações indevidas em ativos de informação, perda de dados institucionais, destruição e roubo de propriedade intelectual;

IV - informar e conscientizar os usuários sobre suas responsabilidades com relação ao uso adequado dos recursos de tecnologia informação do TJPB - serviços de redes de dados, estações de trabalho, internet e correio eletrônico institucional - visando incrementar e preservar os níveis de segurança de tais recursos;

V - designar papéis e responsabilidades referentes à segurança da informação.

Art. 11. A PSI do Tribunal de Justiça da Paraíba se aplica às atividades executadas por todas as partes que utilizam os recursos de tecnologia da informação deste Tribunal, bem como a seus executores, incluindo magistrados, servidores, colaboradores, consultores, estagiários e prestadores de serviço que exercem atividades no âmbito do Poder Judiciário, internos ou externos, além de qualquer outra parte que esteja a desfrutar de acesso à infraestrutura ou informações regidas por esta Resolução.

Art. 12. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo TJPB devem observar, no que couber, o constante nesta PSI.

CAPÍTULO V
DA ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Seção I
Da Estrutura Normativa

Art. 13. A Política de Segurança da Informação do TJPB deve ser estruturada em três níveis hierárquicos, assim dispostos:

I - nível estratégico: compreende a Política de Segurança da Informação (PSI) deste ato, que norteia a criação de normas e procedimentos complementares e traça diretrizes basilares de segurança da informação;

II - nível tático: compreende as normas complementares, que derivam da Política de Segurança da Informação principal, especificando obrigações a serem seguidas pelos usuários, regras e procedimentos em nível gerencial relacionados à gestão dos ativos de informação, definindo sua guarda e manutenção de acordo com as diretrizes estabelecidas nesta PSI, devendo abarcar, no mínimo, os seguintes temas:

a) Gestão de Ativos;

b) Controle de Acesso Físico e Lógico;

c) Gestão de Riscos de Segurança da Informação;

d) Uso Aceitável de Recursos de TI;

e) Geração e Restauração de Cópias de Segurança (backup);

f) Plano de Continuidade de Serviços Essenciais de TI;

g) Gestão de Incidentes de Segurança da Informação;

h) Gestão de Vulnerabilidades e Padrões de Configuração Segura;

i) Gestão e Monitoramento de Registros de Atividade (logs);

j) Desenvolvimento Seguro de Sistemas;

k) Uso de Recursos Criptográficos.

III - nível operacional: procedimentos de segurança da informação que contemplam regras operacionais, roteiros técnicos, fluxos de processos, manuais com informações técnicas que instrumentalizam o disposto na PSI e nas normas complementares referenciadas no plano tático.

Seção II
Da Aprovação e Revisão

Art. 14. Os documentos integrantes da estrutura normativa de segurança da informação do TJPB - Política, Normas Complementares e Procedimentos - serão submetidos à apreciação do Tribunal Pleno, Comitê de Segurança da Informação da Informação (CSI) e

Comitê de Gestão de Tecnologia da Informação (CGTI).

Art. 15. A PSI será submetida a revisões, no máximo, a cada dois anos, devendo ser feita uma análise crítica sistemática, a fim de mantê-la alinhada com os objetivos estratégicos institucionais e de tecnologia da informação.

Art. 16. O processo de elaboração, acompanhamento e revisão da PSI, devidamente instituído, definirá as atividades necessárias à sua consecução, obedecida a forma instituída no art. 35 desta Resolução.

Seção III
Do Comitê de Segurança da Informação

Art. 17. Fica instituído o Comitê de Segurança da Informação (CSI) do TJPB, equipe multidisciplinar com atribuições de caráter consultivo, normativo e fiscalizador.

§ 1º O CSI, designado pela Presidência do TJPB, compor-se-á dos seguintes membros: I

– um Desembargador, que será seu presidente;

II – o juiz auxiliar da Presidência, integrante do Comitê de Governança de TI - CGovTI;

III – o juiz auxiliar da Corregedoria Geral de Justiça, integrante do Comitê de Governança de TI - CGovTI;

IV – o Diretor de Tecnologia da Informação;

V – o Coordenador de Segurança da Informação;

VI – o Gerente de Segurança Institucional e

Militar;

VII - o Encarregado de Proteção de Dados Pessoais.

Seção IV
Da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernéticos (ETIR)

Art. 18. Fica instituída a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernéticos (ETIR), com a responsabilidade de receber, analisar, classificar, tratar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Parágrafo único. O funcionamento da ETIR - definição da missão, público-alvo, modelo de implementação, nível de autonomia, integrantes, canais de comunicação de incidentes e os serviços a serem prestados - deve ser regulado em norma específica.

CAPÍTULO VI

DAS DIRETRIZES GERAIS

Art. 19. Deverão ser criadas, consoante o estabelecido no art. 15 desta Resolução, normas complementares e procedimentos, sem prejuízo de normativos adicionais sobre outros temas e conforme necessidade e conveniência, para as seguintes seções elencadas neste capítulo:

I - uso dos recursos de TI pelos usuários;

II- controle de acesso;

III - uso do correio eletrônico;

IV - tratamento de incidentes em redes

computacionais; V - trabalho remoto;

VI - gerenciamento e monitoramento de logs;

VII - política de backup;

VIII - gestão de continuidade de TI;

IX - conscientização, educação e treinamento em segurança da

informação; X - classificação e tratamento da informação;

XI - proteção contra códigos maliciosos;

XII - política da mesa limpa e tela protegida;

XIII - gestão de riscos de segurança da informação.

Seção I
Do Uso dos Recursos de TI pelos Usuários

Art. 20. O uso dos recursos de TI será regulamentado em norma complementar, composta por diretrizes específicas e recursos próprios, considerando as seguintes diretrizes gerais:

I - os recursos de TI somente deverão ser utilizados em atividades relacionadas às funções institucionais;

II - a necessidade de organização e racionalização de recursos para imprimir mais eficiência e economicidade à manutenção e à evolução do parque de Tecnologia da Informação do TJPB;

III - os parâmetros de configuração das estações de trabalho devem levar em conta

requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional do Tribunal.

Seção II
Do Controle de Acesso

Art. 21. O controle de acesso será regulamentado em norma complementar, com diretrizes específicas e procedimentos próprios, a qual observará as seguintes diretrizes gerais:

I - o controle de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação do TJPB;

II - contas com perfil de administrador de rede somente serão criadas para usuários específicos da DITEC, estritamente por necessidade funcional, para que possam executar tarefas próprias inerentes à administração de ativos de informação;

III - o acesso à rede corporativa dar-se-á de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em norma complementar;

Seção III
Do Correio Eletrônico

Art. 22. O uso do correio eletrônico será regulamentado em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - o Correio Eletrônico institucional é um meio oficial de comunicação do órgão, sendo uma ferramenta disponível é obrigatória para todos os usuários do TJPB;

II - o uso do correio eletrônico no TJPB deve ocorrer com base em fins institucionais, relacionado exclusivamente às atividades que o usuário desempenha no âmbito do órgão.

Seção IV
Do Tratamento de Incidentes em Redes Computacionais

Art. 23. O tratamento de incidentes em redes computacionais será regulamentado em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas;

II - deve ser criado um processo de Tratamento e Resposta a Incidentes, visando impedir, interromper ou minimizar o impacto de ações maliciosas ou acidentais.

Seção V
Do Trabalho Remoto

Art. 24. O trabalho remoto será regulamentado em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - o acesso remoto deve ser concedido estritamente por necessidade funcional justificada;

II - nas comunicações remotas, deve ser usado equipamento de comunicação apropriado, que esteja com os níveis adequados de proteção, incluindo métodos de acesso remoto seguro;

III - medidas que apoiam a segurança da informação devem ser implementadas para proteger as informações em trânsito, acessadas, processadas ou armazenadas em locais de trabalho remoto;

Seção VI
Do Gerenciamento e Monitoramento de Logs

Art. 25. O gerenciamento e monitoramento de logs será regulamentado em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - devem ser implantados sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para detectar não conformidades com as regras, com as responsabilidades definidas nesta PSI e para identificar usuários e seus respectivos acessos, assim como o material manipulado;

II - os registros (logs) de auditoria de todos os recursos de tecnologia da informação do TJPB devem ser guardados pelo tempo exigido em Lei, conforme será regulado em norma complementar específica;

III - os registros (log) de eventos podem conter dados confidenciais e informação de identificação pessoal, assim convém que medidas apropriadas de proteção de privacidade sejam tomadas;

IV - informações obtidas pelos sistemas de monitoramento e auditoria do TJPB poderão tornar-se públicas em caso de exigência judicial;

V - deverá ser validada a eficácia de controles adotados e a respectiva conformidade com as diretrizes definidas nesta PSI e nas suas políticas auxiliares.

Seção VII
Da Política de Backup

Art. 26. A política de backup será regulamentada em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - o serviço de backup deve ser automatizado por sistemas informacionais próprios considerando, inclusive, a execução agendada fora do horário de expediente normal do órgão, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados nos sistemas de informática;

II - a solução de backup deverá ser mantida atualizada, considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros);

III - a administração das mídias de backup deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter sua segurança e integridade;

IV - a execução de rotinas de backup e restore deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

Seção VIII
Da Gestão de Continuidade de TI

Art. 27. A gestão de continuidade de TI será regulamentada em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - o TJPB deverá elaborar e manter um Programa de Gestão de Continuidade de Negócios, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas, devendo ser composto, no mínimo, pelos seguintes planos:

a) Plano de Gerenciamento de Incidentes de Segurança da Informação: plano de ação claramente definido e documentado, a ser usado quando ocorrer um incidente, abrangendo as principais pessoas, recursos, serviços e ações necessárias para implementar o processo de gerenciamento de incidentes;

b) Plano de Continuidade de TI: documentação dos procedimentos e informações necessárias para que o TJPB mantenha seus ativos e atividades críticas funcionando num nível previamente definido, caso haja incidente;

c) Plano de Recuperação de TI: documentação dos procedimentos e informações necessárias para que o TJPB operacionalize o retorno das atividades críticas de TI à

normalidade.

Seção IX
Da Conscientização, Educação e Treinamento em Segurança da Informação

Art. 28. A conscientização, educação e treinamento em segurança da informação será regulamentada em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - o programa de conscientização em segurança da informação deve focar em tornar os usuários conscientes de suas responsabilidades em relação à segurança da informação;

II - o programa de conscientização precisa estar alinhado às normas e procedimentos relevantes de segurança da informação;

III - atividades do programa de conscientização em segurança da informação devem ser realizadas periodicamente.

Seção X
Da Classificação e Tratamento da Informação

Art. 29. A classificação e tratamento da informação será regulamentada em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - normas de classificação de informações, acesso à informação, uso e descarte de ativos de informação, dentre outros temas afins, serão fixadas, considerando as necessidades do negócio para compartilhar ou restringir a informação, em estrita aderência às leis e normas existentes;

II - deve ser criado um conjunto apropriado de procedimentos para rotular e tratar a informação, devendo ser implementado de acordo com o esquema de classificação da informação do TJPB;

III - o tratamento da informação deve abranger normas, processos, procedimentos, práticas e outros instrumentos adotados pelo TJPB para lidar com a informação ao longo de cada fase do ciclo de vida, contemplando o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação e destinação ou controle da informação.

Seção XI
Da Proteção Contra Códigos Maliciosos

Art. 30. A proteção contra códigos maliciosos será regulamentada em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - todos os dispositivos de processamento do Tribunal devam estar configurados de acordo com os padrões de segurança mais adequados;

II - os recursos de Tecnologia da Informação devem estar protegidos por sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, tais como programas antivírus, firewall, dentre outros.

Seção XII
Da Política da Mesa limpa e Tela Protegida

Art. 31. A política da mesa limpa e tela protegida será regulamentada em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - a política de mesa limpa e tela protegida deve levar em consideração a classificação da informação, requisitos contratuais e legais, risco correspondente e aspectos culturais da organização;

II - as medidas adotadas devem contribuir para a redução de riscos de ocorrência de perdas, alterações e acessos indevidos a documentos sigilosos e ativos de Tecnologia da Informação e Comunicação;

III - as melhores práticas para a guarda e manuseio de documentos físicos e arquivos digitais nos ativos de TI do TJPB devem ser criadas e implementadas.

Seção XIII
Da Gestão de Riscos de Segurança da Informação

Art. 32. O uso do correio eletrônico será regulamentado em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - deverá ser estabelecido um Processo de Gestão de Riscos, visando a identificação, avaliação e posterior tratamento e monitoramento dos riscos considerados críticos para a segurança da informação;

II - o processo de Gestão de Riscos do TJPB deverá considerar, prioritariamente, os objetivos estratégico e requisitos legais, além de estar alinhado a esta Política de Segurança da Informação;

III - Deverá ser instituído um Plano de Gestão de Riscos, que é um esquema dentro da estrutura de gestão de riscos que especifica a abordagem e recursos para gerenciar riscos, incluindo procedimentos, práticas, sequência e cronologia das atividades e atribuição de responsabilidades.

CAPÍTULO VII
DOS PAPÉIS E RESPONSABILIDADES

Art. 33. As normas previstas nesta resolução devem ser obedecidas por todos os usuários, observando-se as funções e responsabilidades gerais estabelecidas nas seções subsequentes.

Seção I
Do Tribunal Pleno

Art. 34. Compete ao Tribunal Pleno a apreciação, a aprovação da revisão da PSI do TJPB

Seção II
Da Presidência

Art. 35. Compete à Presidência:

I - apoiar a aplicação das ações estabelecidas na Política de Segurança da Informação;

II - nomear os integrantes:

a) do Comitê de Segurança da Informação (CSI);

b) Comitê de Gestão de Tecnologia da Informação (CGTI)

c) Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernéticos (ETIR).

III - Apreciação e aprovação das Normas Complementares da PSI.

Seção III
Do Comitê de Segurança da Informação - CSI

Art. 36. Compete ao CSI do TJPB:

I – Revisar, periodicamente a Política de Segurança da Informação e submetê-la à aprovação ao Tribunal Pleno

II – elaborar as normas complementares definidas no art. 19 desta PSI e submetê-las à aprovação da Presidência do Tribunal de Justiça;

III – constituir grupo de trabalho incumbido de realizar análises e avaliações de riscos, em

conformidade com a norma ABNT NBR ISO/IEC 27005, que devem guiar as ações estratégicas de segurança da informação;

IV - promover a cultura de segurança da informação;

VI – deliberar sobre revisões da PSI, consoante definido no art. 15, desta Resolução;

VII - definir e fiscalizar o uso de padrões de segurança da informação nas soluções tecnológicas desenvolvidas ou adquiridas pelo TJPB, sejam em nível de hardware ou de software;

VIII - analisar e deliberar os pedidos de autorização para uso de ferramentas, soluções e serviços com potenciais danosos para a segurança da informação;

IX - constituir, quando necessário, grupos de trabalho para tratar de questões específicas sobre segurança da informação;

X – deliberar sobre a realização de auditorias em ativos e serviços de tecnologia da informação do TJPB quando houver suspeita de violações;

XI - propor normas e procedimentos internos relativos à segurança da informação, em conformidade com a legislação vigente;

XII - realizar reuniões, com periodicidade mínima semestral, para acompanhamento dos resultados, das metas e processos de gestão relativos à segurança da informação;

XIII – tratar os casos omissos ou divergências de interpretação dos artigos dessa PSI e dos seus documentos auxiliares.

Art. 37. O CSI coordenará a elaboração e execução dos seguintes planos e protocolos de segurança cibernética para o TJPB:

I – Plano de Ação para Proteção da Infraestruturas Críticas de TIC;

II – Plano de Ação para Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;

III – Plano de Ação para Gestão de Identidades;

IV – Plano de Ação para Política de Educação e Cultura em Segurança Cibernética;

V – Protocolo de Prevenção de Incidentes Cibernéticos;

VI – Protocolo de Gerenciamento de Crises Cibernéticas e;

VII – Protocolo de Investigação de Ilícitos Cibernéticos.

Art. 38. As deliberações do CSI serão tomadas pela maioria simples de seus membros.

Seção IV
Do Comitê de Gestão de Tecnologia Da Informação

Art. 39. Compete ao Comitê de Gestão de Tecnologia da Informação (CGTI):

I - monitorar o cumprimento da PSI e das normas complementares;

II - apoiar as campanhas de conscientização de segurança da informação, fornecendo os recursos necessários;

III - promover a segurança da informação;

IV - adotar medidas de segurança técnica aptas a proteger os dados e privacidade dos usuários de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

V - implantar controles de monitoramento, com finalidade de detectar divergências entre as normas que integram a política de segurança da informação e os respectivos registros de eventos monitorados;

VI - estabelecer e implementar quotas de armazenamento de dados por usuários e/ou unidades de trabalho, seja no uso do servidor de arquivos, e-mail institucional ou outros, de acordo com a necessidade de trabalho e disponibilidade dos recursos;

VII - assegurar que os novos serviços a serem disponibilizados pela DITEC sejam avaliados levando em consideração os aspectos da Lei Geral de Proteção de Dados.

Seção V
Da Coordenação de Segurança da Informação

Art. 40. Cabe à Coordenação de Segurança da Informação:

I - coordenar a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernéticos (ETIR);

II - acompanhar as investigações e as avaliações dos danos decorrentes de violações de segurança da informação, conduzindo a equipe e os procedimentos técnicos adotados;

III - propor recursos necessários às ações de segurança da informação;

IV - realizar e acompanhar estudos de novas tecnologias de segurança da informação com potenciais de agregar valor aos recursos de tecnologia da informação do TJPB;

V - propiciar orientação sobre a Política de Segurança da Informação e suas normas aos usuários;

VI - apoiar as campanhas de conscientização de segurança da informação.

Seção VI
Dos Usuários

Art. 41. É dever de todos os usuários dos ativos de tecnologia da informação do TJPB:

I - conhecer e cumprir esta Política de Segurança da informação, bem como suas normas e procedimentos complementares, aplicáveis às suas atividades;

II - utilizar os recursos de tecnologia da informação do TJPB apenas para os fins previstos institucionalmente;

III - alertar a área de segurança da informação sobre violações de normas ou desta Política;

IV - proteger as informações sigilosas e pessoais obtidas em decorrência do exercício de suas atividades profissionais;

V - preservar o sigilo da identificação de usuário e de senhas de acessos individuais a sistemas de informação, ou outros tipos de credenciais de acesso que lhes forem atribuídos;

VI - participar das campanhas de conscientização e dos treinamentos pertinentes aos temas segurança da informação e proteção de dados pessoais, conforme planejamento deste Tribunal;

VII - utilizar os ativos sob sua responsabilidade de forma segura, em observância ao disposto nesta PSI e nas normas e procedimentos complementares;

VIII - executar as orientações técnicas e os procedimentos estabelecidos pelo

CSI; IX- evitar discutir assuntos confidenciais de trabalho em ambientes públicos;

X - seguir rigorosamente as normas de uso do Correio Eletrônico;

XI - buscar orientação da área de segurança da informação em caso de dúvidas relacionadas à segurança da informação.

Seção VII
Dos Gestores das Unidades Judiciais ou Administrativas

Art. 42. É responsabilidade dos Gestores das Unidades Judiciais ou Administrativas:

I - conhecer, divulgar, cumprir e estimular o cumprimento da PSI e suas Normas Complementares;

II – assegurar a observância da PSI no âmbito de sua unidade, bem como comunicar, de imediato, à DITEC qualquer irregularidade constatada, para as providências;

III – solicitar formalmente à DITEC a concessão de permissões de acesso aos usuários sob sua supervisão, sempre com base no binômio: necessidade e mínimo de permissões;

IV – comunicar formalmente à Diretoria de Gestão de Pessoas e à Diretoria de Tecnologia da Informação qualquer ocorrência de mudança de lotação, afastamento, retorno ou desligamento dos seus integrantes;

V – manter o zelo, em nível físico e lógico, dos recursos de tecnologia da informação sob sua unidade de atuação;

VI - identificar o uso inadequado dos ativos e adotar as medidas apropriadas.

Seção VIII
Da Diretoria de Gestão de Pessoas

Art. 43. É responsabilidade da Diretoria de Gestão de Pessoas:

I – manter atualizadas as informações do sistema recursos humanos, priorizando aquelas que se referem a desligamentos, retornos, afastamentos, ou qualquer outra mudança no quadro funcional do TJPB e órgãos subordinados;

II – apoiar as campanhas de conscientização de segurança da informação;

III – incluir o Termo de Responsabilidade e Confidencialidade como documento obrigatório para o exercício dos cargos e funções, bem como proceder com a guarda segura e adequada dos documentos assinados, conforme estabelecido pela tabela de temporalidade vigente;

IV - adotar as medidas necessárias por ocasião do desligamento de pessoal e comunicar às unidades do TJPB, com vistas à pertinente remoção dos acessos na DITEC;

V - conhecer, divulgar, cumprir e estimular o cumprimento desta PSI e das suas normas complementares pertinentes.

Seção IX
Da Gerência de Comunicação

Art. 44. Compete à Gerência de Comunicação:

I - promover campanhas de conscientização sobre segurança da informação;

II - conhecer, divulgar, cumprir e estimular o cumprimento desta PSI e das suas normas complementares que forem pertinentes.

Seção X
Da Diretoria Jurídica

Art. 45. Compete à Diretoria Jurídica do TJPB:

I - avaliar, sempre que solicitada, as normas, os procedimentos e o termo de responsabilidade e confidencialidade referentes à gestão da segurança da informação;

II - informar ao Comitê de Segurança da Informação alterações legais ou regulatórias que impliquem responsabilidade ou ação que envolvam a gestão da segurança da informação;

III - auxiliar o Comitê nas demais questões legais.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 46. Além do presente documento, as normas complementares e procedimentos, destacadas no art. 19, também fazem parte desta Política de Segurança da Informação.

Parágrafo único. A Política, as normas complementares e os procedimentos deverão estar disponíveis na página principal da intranet institucional ou em site específico mantido por este Tribunal.

Art. 47. Fica revogada a Resolução TJPB nº 28, de 03 de setembro de 2020.

Art. 48. Esta Resolução entra em vigor na data de sua publicação

Tribunal de Justiça, em João Pessoa, datado e assinado eletronicamente.

SAULO HENRIQUES DE SA E BENEVIDES:4682483

Assinado de forma digital por SAULO HENRIQUES DE SA E BENEVIDES:4682483
Dados: 2022.09.01 16:28:38 -03'00'

DESEMBARGADOR SAULO HENRIQUES DE SÁ E BENEVIDES
PRESIDENTE DO TRIBUNAL DE JUSTIÇA DA PARAÍBA