PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SETIC/CGTIC-DPPE

Versão 1.0

Válida a partir da publicação da portaria 233/2021

Publicada em Diário Oficial da Defensoria Pública do Estado de Pernambuco em 24 de abril de 2021.

DEFENSORIA
PÚBLICA DO ESTADO
DE PERNAMBUCO

Defensoria Pública do Estado de Pernambuco
Rua Marques do Amorim, nº 127, CEP: 50070-330, Boa Vista, Recife-PE

PORTARIA Nº 233, de 23 de abril de 2021.

Institui a Política de Segurança da Informação e Comunicação no âmbito da Defensoria Pública do Estado de Pernambuco.

1. **O CONSELHO DA DEFENSORIA PÚBLICA DO ESTADO DE PERNAMBUCO (DPPE)**, no uso de suas atribuições legais e regimentais e,

CONSIDERANDO a importância dos ativos de informações para a organização e a necessidade de garantia de sua integridade, disponibilidade, confidencialidade, autenticidade e legalidade;

CONSIDERANDO que a Segurança da Informação tem como objetivo aplicar controles e medidas protetivas no uso regular da Tecnologia da Informação e Comunicação (TIC) para o negócio, com o objetivo de garantir a continuidade dos seus serviços e mitigar riscos decorrentes;

CONSIDERANDO o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) da Defensoria Pública do Estado de Pernambuco, que prevê a adoção de medidas de Segurança da Informação, ressaltando explicitamente a necessidade na meta M27, através da criação, publicação, implantação e divulgação ampla de uma Política de Segurança da Informação (PSI);

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação (PSI) da Defensoria Pública do Estado de Pernambuco (DPPE).

2. CAPÍTULO I - VISÃO GERAL E GLOSSÁRIO.

Art. 2º A Política de Segurança da Informação (PSI) da DPPE e de seus órgãos subordinados é uma declaração de compromisso com a proteção das informações que cria, manipula, custodia ou que são de sua propriedade, sob o gerenciamento de sua infraestrutura de Tecnologia da Informação (TIC), devendo ser conhecida, compreendida e cumprida por todos que tenham acesso às informações.

Parágrafo único. A utilização dos recursos e dispositivos de TIC da DPPE, ou pessoais em seu proveito, deve ser pautado pelos princípios da ética, segurança e legalidade.

Art. 3º Setor de Tecnologia da Informação e Comunicação (SETIC) publicará glossário específico, o qual conterá denominações e limitará conceitos que se aplicarão à PSI, suas normas e procedimentos correlatos, de indispensável conhecimento pelos agentes da Defensoria ou terceiros interessados que tiverem contato com informações e demais recursos de TIC.

3. CAPÍTULO II - ESTRUTURA NORMATIVA, APROVAÇÃO E REVISÃO.

Art. 4º A Estrutura Normativa da Segurança da Informação da DPPE é composta pelos seguintes documentos, hierarquicamente organizados, com a indicação de seus respectivos responsáveis por aprovação e periodicidade de revisão:

I - Política de Segurança da Informação (PSI): consiste em diretrizes gerais e princípios básicos, com a finalidade de nortear todas as ações que garantirão a manutenção da Segurança da Informação. A Política e suas revisões serão aprovadas pelo Conselho Superior da DPPE, com periodicidade de revisão bienal ou conforme a necessidade;

II - Normas de Segurança da Informação: estabelecem os controles, os métodos, as restrições e as responsabilidades para atendimento à PSI. As normas e suas revisões serão aprovadas pelo Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC), com periodicidade de revisão anual ou conforme necessidade;

III - Procedimentos de Segurança da Informação: Definem como as operações de atendimento à PSI e normas correlatas devem ser realizadas. Os procedimentos e suas revisões serão aprovados pela Setor de Tecnologia da Informação e Comunicação (SETIC), com periodicidade de revisão anual ou conforme a necessidade.

Art. 5º Também compõem a Estrutura Normativa da Segurança da Informação outros documentos acessórios, a saber: termos e acordos de responsabilidade e confidencialidade perante quem tomar contato com informações da DPPE e seus órgãos subordinados.

4. CAPÍTULO III - REQUISITOS DE CAPITAL HUMANO, SUAS OBRIGAÇÕES E RESPONSABILIDADES.

Art. 6º Para os efeitos desta Política entende-se por classes de agentes da Defensoria: membros, servidores efetivos, servidores cedidos, servidores comissionados, estagiários, voluntários e terceirizados que possuam um vínculo formal com a DPPE.

Art. 7º Cabe aos agentes da Defensoria:

- Firmar, obrigatoriamente, **Termo de Responsabilidade e Confidencialidade** sobre as informações;
- Participar das campanhas, eventos ou atualizações promovidas sobre Segurança da Informação no âmbito da DPPE;
- Estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes da DPPE ou do órgão subordinado que executar suas tarefas;
- Cumprir o disposto nos documentos da Estrutura Normativa de Segurança da Informação da DPPE, sem exceção;

- Utilizar, modificar ou reproduzir dados e informações da DPPE exclusivamente para o desempenho de suas funções, da mesma forma que a utilização dos dispositivos de TIC em nome da DPPE;
- Não divulgar, compartilhar, transmitir ou deixar-se conhecer informações a pessoas que não tenham nível de autorização suficiente;
- Não divulgar, compartilhar, transmitir, veicular ou permitir a divulgação, por qualquer meio, informações sobre ativos ou de procedimentos da DPPE, exceto quando houver autorização prévia e formal por superior hierárquico ou de acordo com a legislação vigente para tanto;
- Não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações alcancem ambiente ou destinatário fora das dependências ou controle da DPPE sem autorização formal;
- Proteger ativos de informação contra acesso, divulgação, transmissão, compartilhamento, modificação, destruição ou interferência não autorizados;
- Estar atento ao repassar ou transmitir informações para outras pessoas, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais. Confirmar a identidade e idoneidade do solicitante ou destinatário antes do envio de informações e, sempre que possível, a real necessidade do compartilhamento de alguma informação solicitada por outra pessoa, mesmo que de sua confiança;
- Reportar ao Grupo de Trabalho de Tecnologia (Portaria n° 523/20) quaisquer eventos ou incidentes potenciais ou reais que causem riscos à segurança das informações da DPPE, ou ainda sua mera suspeita.

Art. 8º Cabe ao setor da Coordenadoria de Planejamento e Gestão e a Unidade de Apoio à Gestão:

- Conhecer, divulgar, cumprir e estimular o cumprimento da PSI, normas e procedimentos correlatos;
- Indicar o perfil adequado para acesso a recursos, dados e informações conforme a necessidade, com base nos princípios do conjunto mínimo de permissões que precisam ser atribuídos ("*least privilege"* e *"need to know*");
- Informar ao Setor de Tecnologia da Informação e Comunicação (SETIC) as mudanças de lotação, afastamentos, retornos ou desligamentos ocorridos em suas equipes; a responsabilidade por gerir os recursos de TIC e postura dos agentes da Defensoria que compõem sua área ou equipe em relação à Segurança da Informação;
- Manter atualizados, no sistema informatizado de gestão de pessoas, todos os dados referentes a: desligamentos, afastamentos, retornos e modificações no quadro funcional da DPPE e de seus órgãos subordinados. Da mesma forma, manter o *status* atualizado das credenciais que precisem ser emitidas, revogadas e suspensas;
- Apoiar as campanhas de conscientização de Segurança da Informação, juntamente com a SETIC; incluir o **Termo de Responsabilidade e**

Confidencialidade como documento obrigatório para exercício dos agentes da Defensoria e proceder à guarda segura e adequada dos documentos assinados, conforme estabelecido pela tabela de temporalidade vigente.

Art. 9º Cabe ao Conselho Superior da DPPE aprovar e publicar a PSI, suas revisões e documentos acessórios, encaminhados pelo Grupo de Trabalho de Tecnologia (Portaria n° 523/20) e Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC).

Art. 10º Cabe ao Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC):

- Propor alterações na Política de Segurança da Informação (PSI); elaborar e promover alterações das Normas de Segurança da Informação, sempre que pertinente; propor alterações e aprovar os termos acessórios da PSI;
- Analisar os casos de violação da PSI, incidentes, vulnerabilidades e tentativas de burla, encaminhando-os ao Conselho da DPPE, quando providências a serem autorizadas por este colegiado forem requeridas; propor medidas relacionadas à melhoria da Segurança da Informação da DPPE;
- Propor o planejamento e a alocação de recursos no que tange à Segurança da Informação da DPPE; aprovar a relação de responsáveis pelas informações pertencentes ou sob a guarda da DPPE; aprovar ou reprovar o acesso a locais de rede, sítios de internet, uso de dispositivos de TIC pessoais no ambiente da instituição e demais regras de uso dos recursos de TIC oferecidos pela DPPE aos agentes da Defensoria.

Art. 11º Cabe à Setor de Tecnologia da Informação e Comunicação (SETIC):

- Emitir, revogar ou suspender as credenciais de acesso, sempre que solicitadas pela SGP. No caso de emissão, tais ações somente serão efetuadas depois de determinação do perfil do usuário, sempre baseada apenas nas permissões indispensáveis para realização das suas atividades, com orientação nos princípios do conjunto mínimo de permissões que precisam ser atribuídos ("*least privilege"* e *"need to know*");
- Manter registros de atividades dos usuários pelo tempo correspondente na tabela de temporalidade em vigor, permitindo controles e auditorias;
- Formalizar orientação para a Coordenadoria de Planejamento e Gestão e a Unidade de Apoio à Gestão nas políticas adequadas e aplicáveis aos usuários, cargos, funções e lotação, sempre que necessário; apoiar as campanhas de conscientização de Segurança da Informação, fornecendo os recursos de TIC necessários; publicar e manter atualizado o Glossário da PSI, referido no art. 3º da presente Resolução.

Art. 12º Cabe ao Núcleo de Segurança da Informação (NSI), vinculado à SETIC:

- Promover campanhas com o objetivo de conscientizar os agentes da Defensoria sobre a Estrutura Normativa de Segurança da Informação;

fomentar ações para implementar as diretrizes previstas na PSI, normas e procedimentos correlatos;

- Reportar imediatamente à SETIC os eventos que violem, ou tentem violar, os termos da PSI, das normas ou procedimentos correlatos, ainda que por mera suspeita;
- Promover a criação e manutenção de diretrizes, princípios e conteúdo da Estrutura Normativa de Segurança da Informação;
- Solicitar a revogação ou suspensão das credenciais de acesso sempre que detectar a utilização inadequada das mesmas ou a reativação, conforme o caso;
- Coordenar a elaboração, manutenção, implementação e testes do plano de continuidade do negócio e prevenção a desastres;
- Zelar para que as diretrizes e os princípios desta política sejam respeitados, informando, via procedimento administrativo de ofício, os incidentes e ações à SETIC, ainda que por mera suspeita;
- Responder, adequadamente, a quaisquer consultas das outras áreas sobre a aplicação da PSI, normas e procedimentos de Segurança da Informação e uso aceitável da infraestrutura de tecnologia e comunicação, orientando-as sobre as melhores práticas;
- Aprovar, reprovar, suspender ou promover a homologação de softwares e hardwares para o uso dos agentes da Defensoria e divulgar lista com permissões e proibições que julgar pertinente;
- Aprovar, reprovar, suspender ou promover a liberação do uso de dispositivos de TIC pessoais dos agentes da Defensoria no ambiente institucional e aplicar as medidas de segurança cabíveis para a preservação da infraestrutura de TIC da DPPE.

5. CAPÍTULO IV - CLASSIFICAÇÃO DA INFORMAÇÃO, CONTROLE E CREDENCIAIS DE ACESSO.

Art. 13º Cabe aos responsáveis pela informação a classificação e a definição de quem possui acesso e o tipo de privilégios de acesso, sem prejuízo do disposto na legislação vigente.

Art. 14º Os agentes da Defensoria têm o dever de cumprir com o nível de segurança exigido pela classificação das informações, sob pena de abertura de Processo Administrativo, que poderá resultar em sanção disciplinar.

Art. 15º Não é permitido o acesso ou uso de qualquer recurso de TIC ou ativo da informação sem as credenciais de acesso correspondentes, a partir da utilização do AD..

Art. 16º O agente da Defensoria deve proteger sua identidade digital, devendo suas credenciais, senhas e acessos serem pessoais e tratados de forma segura, confidencial,

intransferível, intransmissível, possuindo apenas as permissões suficientes para realização das suas atividades, com orientação nos princípios do conjunto mínimo de permissões que precisam ser atribuídos (“*least privilege”* e *“need to know*”).

Art. 17º O acesso aos ambientes físicos e recursos lógicos de TIC devem ser controlados e restritos às pessoas autorizadas pela SETIC, conforme orientação do binômio de necessidade funcional e mais restrita permissão cabível.

6. CAPÍTULO V - AQUISIÇÃO, UTILIZAÇÃO, CONTROLE E DESCARTE DE RECURSOS DE TIC.

Art. 18º Todas as informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao agente da Defensoria ou das quais tiver acesso no exercício de suas atividades, são de propriedade e/ou direito de uso exclusivo da DPPE.

Parágrafo único. Todos os ativos e informações da DPPE devem ser utilizados apenas para o cumprimento das atividades profissionais, dentro do padrão de conduta ética estabelecida pela Estrutura Normativa de Segurança da Informação da DPPE e às demais leis em vigor, respeitando os requisitos de sigilo profissional.

Art. 19º Os recursos de TIC de propriedade da DPPE somente poderão ser utilizados pelos membros e servidores.

Parágrafo único. Outras classes de agentes da Defensoria e o público externo somente poderão fazer uso dos recursos se forem previamente autorizados, pelo membro da Defensoria Pública, levando em consideração quaisquer responsabilidades legais na concessão.

Art. 20º A utilização de qualquer recurso da infraestrutura de tecnologia deve ser restrita à execução de atividades inerentes e previamente previstas para o desempenho de suas funções ou concessões formalmente divulgadas pela DPPE, seguindo a política de conceder apenas as permissões indispensáveis para realização das suas atividades.

Art. 21º Todos os equipamentos, dispositivos e demais recursos que fizerem uso da infraestrutura de TIC da DPPE deverão estar sujeitos à PSI e às demais normas de Segurança da Informação da DPPE e deverão possuir softwares de proteção instalados, a exemplo, mas não se limitando, de antivírus, anti-spyware e firewall sempre ativos e atualizados.

Art. 22º São direitos da DPPE, através da SETIC, registrar, bloquear, permitir, suspender e limitar o uso dos recursos e dispositivos que compõem sua infraestrutura de TIC.

Art. 23º A DPPE, por meio da SETIC, monitora todos os recursos, ambientes, dispositivos e ativos ligados à Tecnologia de Informação e Comunicação, tais como, mas não se restringindo, o e-mail institucional, acesso à internet, estrutura de comunicação telefônica, espaços físicos e utilização dos dispositivos de TIC

institucionais, com a finalidade de proteger seus ativos, sua reputação e conhecimento.

§ 1º A DPPE também registra todos os dados obtidos pelo monitoramento realizado para eventual análise forense, apuração a violações à Estrutura Normativa de Segurança de Informação, podendo investigar fatos que comprometam seus ativos.

§ 2º Da mesma forma que indicado no *caput* , a DPPE possui a prerrogativa de registrar, inspecionar, apreender, isolar ou neutralizar dispositivos ou recursos de TIC de propriedade de terceiros que pretendam adentrar em seu perímetro lógico ou físico, ou até mesmo impedir que estes o façam, com a utilização das medidas de contenção que entender cabíveis para preservar a incolumidade de sua estrutura de TIC e pelo tempo que for necessário, observando os princípios de transparência, proporcionalidade e razoabilidade.

Art. 24º É vedado aos agentes da Defensoria acessar ou armazenar, a partir de dispositivos ou recursos de TIC da DPPE ou pessoais em seu proveito, conteúdo que caracterize atividade ilegal, que não condiga com as atividades a serem cumpridas ou que possa causar prejuízo ao bom funcionamento da infraestrutura de TIC da DPPE, a exemplo, mas não se limitando, de:

- Arquivos de mídia, softwares e demais materiais protegidos por propriedade intelectual sem a devida licença ou autorização; material pornográfico ou que possua intenção de satisfazer a lascívia; conteúdo ou ambientes que ponham em risco a incolumidade da segurança dos dispositivos e ativos de TIC da DPPE, tais quais sítios de internet suspeitos de conterem scripts maliciosos ou consistirem em prática de fraude, instalação de softwares maliciosos, desconhecidos ou não homologados pelo NSI, vinculado à SETIC;
- Conteúdo ou serviços de TIC de ordem pessoal dos agentes da Defensoria ou de terceiros, tais quais, repositórios de arquivos na internet, serviço de e-mail, mídias sociais não liberadas, rádios online e recursos de entretenimento em geral; qualquer outro que constitua crime, ato ilícito ou contrarie a Ordem Pública, os bons costumes, as normas em vigor da DPPE ou seus objetivos e função social.

Parágrafo único. O descumprimento à vedação do presente artigo, ainda que por tentativa de burla, acarretará em Procedimento Administrativo disciplinar próprio, podendo incorrer nas penas previstas em lei orgânica, conforme sua gravidade e prejuízo aa DPPE.

Art. 25º A DPPE aconselha aos agentes da Defensoria que utilizarem as Mídias Sociais a evitar expor rotinas de trabalho e demais detalhes privados e íntimos sobre si, família, amigos próximos. Sugere-se, ainda, que utilizem somente conteúdos autorizados, com a citação da fonte, para evitar punições por crimes contra direitos autorais ou que violem direitos de marca, não faltando com educação, polidez e urbanidade quando forem interagir com os demais usuários.

Art. 26º Apenas é permitido aos agentes da Defensoria a utilização de conteúdos originais, legais e legítimos, sempre existindo licença ou autorização para o uso de materiais protegidos por direitos de propriedade intelectual.

Art. 27º As alterações em qualquer recurso de TIC que possam impactar no funcionamento dos serviços críticos deverão ser regidas por um processo de gerenciamento de mudanças, de forma a garantir o máximo de disponibilidade dos recursos disponibilizados pela DPPE. As exceções devem ser previamente aprovadas pelos responsáveis pelo serviço e realizadas em data e horário de menor impacto possível.

Art. 28º As trocas de mensagens eletrônicas institucionais somente devem ser realizadas para fins laborais, utilizando sistemas fornecidos ou homologados pela SETIC, mantendo vocabulário formal e condizente com a reputação esperada, evitando subjetividades e intimidades em seus conteúdos.

Art. 29º A mera disponibilidade ou operação contínua e involuntária de recursos de TIC para acesso remoto às informações ou recursos da DPPE não configura sobre jornada, horas extras, sobreaviso ou qualquer consequência que configure atividade laboral ou estatutária que mereça remuneração além dos vencimentos já firmados.

Art. 30º O acesso remoto aos recursos de TIC da DPPE deve ser previamente homologado pela SETIC, que indicará as configurações adequadas e controles de segurança necessários para que haja o uso seguro pelos agentes da Defensoria.

Art. 31º Sempre que o agente da Defensoria necessitar portar informações em mobilidade deverá fazê-lo pelo menor tempo possível e com controle de restrição na mídia ou dispositivo que as contiverem, seja pelo uso de trava, senha, criptografia ou tecnologia subserviente. Após o uso da informação ou trânsito com sucesso, esta deverá ser excluída da mídia que a carregou. Caso não seja possível, deve ser aplicado procedimento adequado para impedir novo uso futuro.

Art. 32º É permitido o uso de dispositivos pessoais de TIC pelos agentes da Defensoria nos ambientes da DPPE, desde que não haja restrição conforme seu perfil profissional e que não traga prejuízos para a DPPE.

§ 1º Os agentes da Defensoria serão integralmente responsáveis pelo conteúdo armazenado em seus dispositivos pessoais e pelos atos através deles praticados, sem ressalvas ou exceções.

§ 2º Os agentes da Defensoria poderão utilizar seus dispositivos pessoais de TIC durante o expediente profissional, isto é, desde que não atrapalhe a própria concentração ou dos demais a seu redor nas atividades que devem desempenhar, não prejudique o atendimento ao público ou atrase as tarefas que lhe cabem, não violem a Estrutura Normativa de Segurança da Informação ou gerem riscos aa DPPE, sob pena de perderem o benefício e sofrerem outras sanções disciplinares, mediante competente Processo Administrativo.

Art. 33º Todos os relacionamentos e contratações em que haja o compartilhamento de informações ou ativos de TIC da DPPE ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos devem ser precedidos por **Termo de Responsabilidade e Confidencialidade** e cláusulas contratuais que tratem especificamente da Segurança da Informação.

Art. 34º O descarte de informações e ativos de TIC da DPPE devem ser realizados de forma segura, com a destruição, sanitização ou inutilização da mídia ou dispositivo que contém as informações, de modo que fique incapacitada de ser recuperada, adquirida ou reutilizada por terceiros.

Art. 35º Os agentes da Defensoria devem adotar postura de mesa limpa nos locais onde realizam suas tarefas, dando prioridade à organização, limpeza e asseio ao ambiente, além de não permitir situações não seguras de ocorrerem, a exemplo, mas não se limitando, de deixar à mostra documentos com informações não públicas, chaves na fechadura das gavetas, mídias não adequadamente guardadas, estação de trabalho desbloqueada na ausência do agente da Defensoria.

7. CAPÍTULO VI - DESENVOLVIMENTO, AQUISIÇÃO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO.

Art. 36º Os Sistemas de Informação adquiridos, mantidos ou desenvolvidos pela DPPE deverão atender aos princípios e requisitos de Segurança da Informação, estabelecidos pela presente Resolução e demais normas em vigor.

Art. 37º As atividades de desenvolvimento, teste e homologação dos Sistemas de Informação não devem afetar o funcionamento dos sistemas em operação. Para isso, um plano consistente deve ser elaborado pela SETIC.

Art. 38º Os dados classificados como sigilosos, mantidos pelos Sistemas de Informação, não deverão estar replicados ou acessíveis em outro ambiente, sem a competente autorização do NSI, vinculado à SETIC, sob o risco de vazamento de informações pessoais ou confidenciais sob a guarda da DPPE.

Parágrafo único. O descumprimento desta disposição poderá acarretar em Procedimento Administrativo disciplinar e justificará a aplicação de penas previstas em lei, conforme a gravidade do ato e prejuízos sofridos pela DPPE.

8. CAPÍTULO VII - ANÁLISE DE CONFORMIDADE E AUDITORIAS.

Art. 39º A DPPE é facultada a realização de análises de conformidade ou auditorias periódicas na segurança da infraestrutura de TIC, seus ativos, processos e pessoas com o objetivo de detectar vulnerabilidades e demonstrar evidências do cumprimento da política e boas práticas de Segurança da Informação.

9. CAPÍTULO VIII - RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.

Art. 40º É de responsabilidade da SETIC a implantação de uma equipe de resposta a incidentes de Segurança da Informação, de forma que as fragilidades e eventos de segurança associados aos ativos de informação sejam comunicados ao CGTIC, permitindo a tomada de ação corretiva em tempo hábil e com a orientação de preservar ou restabelecer operantes os recursos de TIC oferecidos.

Art. 41º A SETIC tem o dever de guardar as provas produzidas pelos recursos e dispositivos de TIC pelo tempo previsto na tabela de temporalidade da DPPE, sobretudo em casos de incidente de Segurança de Informação.

10. CAPÍTULO IX - GERENCIAMENTO DE RISCOS.

Art. 42º É de responsabilidade da SETIC mapear e documentar as ameaças e vulnerabilidades que redundam em risco ao negócio e à infraestrutura de tecnologia que o suporta, assim como buscar a solução adequada para cada caso.

Art. 43º É de responsabilidade do CGTIC a administração dos riscos identificados.

11. CAPÍTULO X - PLANO DE CONTINUIDADE DO NEGÓCIO E RECUPERAÇÃO DE DESASTRES.

Art. 44º É de responsabilidade do CGTIC coordenar a elaboração, execução, teste e renovação de plano que tenha como objetivo minimizar o impacto na disponibilidade dos recursos críticos de TIC e, consequentemente, nos processos da DPPE por eles suportados.

Art. 45º É de responsabilidade do CGTIC aprovar a estratégia de continuidade do plano e fornecer subsídios para a sua implementação.

Art. 46º Independentemente da existência de um plano de continuidade dos negócios ou de recuperação a desastres, o CGTIC deve estabelecer normas e procedimentos para backup, com frequência de realização diária, mantendo sempre a base de dados tão atualizada quanto possível.

12. CAPÍTULO XI - VIOLAÇÕES DA PSI E SANÇÕES.

Art. 47º Todos os agentes da Defensoria devem noticiar à Ouvidoria os incidentes de Segurança da Informação que presenciarem ou tomarem conhecimento, ainda que por mera suspeita, para que a providência adequada seja adotada no menor tempo possível e minimizando os danos sofridos pela DPPE, sem prejuízo de comunicação administrativa conforme o caso e urgência, formalmente.

Art. 48º Violações da presente PSI, normas e procedimentos correlatos são passíveis de penalidades administrativas, sem prejuízo de ações legais cabíveis. Estas violações serão avaliadas tanto quanto à responsabilidade pessoal como quanto à institucional.

Art. 49º Todos os documentos da Estrutura Normativa de Segurança da Informação da DPPE devem ser disponibilizados no site oficial da Defensoria Pública do Estado de Pernambuco.

Art. 50º Casos omissos ou esclarecimentos da PSI, normas e procedimentos correlatos são de exclusiva responsabilidade do CGTIC e passíveis de aprovação pelo Grupo de Trabalho de Tecnologia (Portaria n° 523/20).

Art. 51º Esta Resolução entra em vigor na data de sua publicação.

Recife, 24 de abril de 2021.

JOSÉ FABRÍCIO SILVA DE LIMA

Defensor Público-Geral do Estado