RESOLUÇÃO Nº 349, de 04 de março de 2013.

Institui a Política de Segurança da Informação e Comunicação no âmbito do Tribunal de Justiça de Pernambuco.

A CORTE ESPECIAL DO TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO , 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 que o artigo 13, da Resolução n. 90, de 29 de setembro de 2009, do Conselho Nacional de Justiça, determina que os tribunais brasileiros devem elaborar e aplicar Política de Segurança da Informação, por meio de um Comitê Gestor, alinhada com as diretrizes nacionais;

CONSIDERANDO a Resolução n. 99, de 24 de novembro de 2009, do Conselho Nacional de Justiça, que institui o planejamento estratégico de TIC no âmbito do Judiciário e prevê como objetivo estratégico a promoção da Segurança da Informação;

CONSIDERANDO o Planejamento Estratégico Decenal do Tribunal de Justiça do Estado de Pernambuco (TJPE), cujo objetivo estratégico prevê a adoção de medidas de Segurança da Informação, ressaltando explicitamente a necessidade através da publicação de uma Política específica;

CONSIDERANDO a necessidade do acompanhamento das metas estabelecidas no Planejamento Estratégico de TIC, seu aprimoramento contínuo no âmbito do TJPE e o seu objetivo estratégico de promover a Segurança da Informação;

CONSIDERANDO as diretrizes nacionais para a Gestão de Segurança da Informação no âmbito do Judiciário, que define como estratégia a criação de uma Estrutura Normativa da Segurança da Informação, que contemple a Política de Segurança, bem como Normas de Segurança da Informação, que regulamentem: (i) o controle de acesso aos sistemas de informação; (ii) a utilização de recursos de TIC; (iii) o acesso à internet e às redes sociais; (iv) a utilização de correio eletrônico (e-mail); (iv) a política de cópias de segurança (backup); e (v) os procedimentos de Segurança da Informação através de campanha para a divulgação da estrutura normativa e conscientização dos usuários,

RESOLVE:

Art. 1 º Instituir a Política de Segurança da Informação (PSI) do Tribunal de Justiça do Estado de Pernambuco (TJPE).

CAPÍTULO I

VISÃO GERAL E GLOSSÁRIO

Art. 2 º A Política de Segurança da Informação (PSI) do TJPE e de seus órgãos acessórios 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 do TJPE, ou pessoais em seu proveito, deve ser pautado pelos princípios da ética, segurança e legalidade.

Art. 3º A Secretaria 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 judiciários ou terceiros interessados que tiverem contato com informações e demais recursos de TIC.

CAPÍTULO II

ESTRUTURA NORMATIVA, APROVAÇÃO E REVISÃO

Art. 4 º A Estrutura Normativa da Segurança da Informação do TJPE 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 Tribunal Pleno do TJPE, 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 realizados. Os procedimentos e suas revisões serão aprovados pelo Núcleo de Segurança da Informação (NSI), vinculado à SETIC, com periodicidade de revisão anual ou conforme a necessidade.

Art. 5 º 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 do TJPE e seus órgãos subordinados.

CAPÍTULO III

REQUISITOS DE CAPITAL HUMANO, SUAS OBRIGAÇÕES E RESPONSABILIDADES

Art. 6 º Para os efeitos desta Política entende-se por classes de agentes do Judiciário: magistrados, servidores efetivos, servidores cedidos, servidores comissionados, estagiários, voluntários e terceirizados que possuam um vínculo formal com o TJPE.

Art. 7 º Cabe aos agentes do Judiciário:

firmar, obrigatoriamente, Termo de Responsabilidade e Confidencialidade sobre as informações;
participar das campanhas, eventos ou atualizações promovidas sobre Segurança da Informação no âmbito do TJPE;
estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes do TJPE ou do órgão subordinado que executar suas tarefas;
cumprir o disposto nos documentos da Estrutura Normativa de Segurança da Informação do TJPE, sem exceção;
utilizar, modificar ou reproduzir dados e informações do TJPE exclusivamente para o desempenho de suas funções, da mesma forma que a utilização dos dispositivos de TIC em nome do TJPE;
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 do TJPE, 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 do Tribunal 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 à Ouvidoria quaisquer eventos ou incidentes potenciais ou reais que causem riscos à segurança das informações do TJPE, ou ainda sua mera suspeita.

Art. 8 º Cabe às chefias:

conhecer, divulgar, cumprir e estimular o cumprimento da PSI, normas e procedimentos correlatos;
atribuir 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 à Secretaria de Gestão de Pessoas (SGP) as mudanças de lotação, afastamentos, retornos ou desligamentos ocorridos em suas equipes;
a responsabilidade por gerir os recursos de TIC e postura dos agentes judiciários que compõem sua área ou equipe em relação à Segurança da Informação.

Art. 9 º Cabe à Corte Especial do TJPE a provar e publicar a PSI, suas revisões e documentos acessórios, encaminhados pelo Comitê Gestor de Tecnologia da Informação e Comunicação.

Art. 10. 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 à Corte Especial, quando providências a serem autorizadas por este colegiado forem requeridas;
propor medidas relacionadas à melhoria da Segurança da Informação do TJPE;
propor o planejamento e a alocação de recursos no que tange à Segurança da Informação do TJPE;
aprovar a relação de responsáveis pelas informações pertencentes ou sob a guarda do TJPE;
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 pelo TJPE aos agentes do judiciário.

Art. 11. Cabe à Secretaria 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 SGP 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. 12. Cabe à Secretaria de Gestão de Pessoas (SGP):

manter atualizados, no sistema informatizado de gestão de pessoas, todos os dados referentes a: desligamentos, afastamentos, retornos e modificações no quadro funcional do TJPE 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 do Judiciário e proceder à guarda segura e adequada dos documentos assinados, conforme estabelecido pela tabela de temporalidade vigente.

Art. 13. Cabe à Secretaria Judiciária (SEJU):

manter atualizados, no sistema informatizado de gestão de pessoas, todos os dados referentes a: desligamentos, afastamentos, retornos e modificações no quadro de magistrados do Poder Judiciário, e de quaisquer credenciais que precisem ser emitidas, revogadas ou 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 magistrados e proceder à guarda segura e adequada dos documentos assinados, conforme estabelecido pela tabela de temporalidade vigente.

Art. 14. Cabe ao Núcleo de Segurança da Informação (NSI), vinculado à SETIC:

promover campanhas com o objetivo de conscientizar os agentes judiciários 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 conteúdos 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 judiciários 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 judiciários no ambiente institucional e aplicar as medidas de segurança cabíveis para a preservação da infraestrutura de TIC do TJPE.

CAPÍTULO IV

CLASSIFICAÇÃO DA INFORMAÇÃO, CONTROLE E CREDENCIAIS DE ACESSO

Art. 15. 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. 16. Os agentes judiciários tem o dever de cumprir com o nível de segurança exigido pela classificação das informações, sob pena de interposição de Processo Administrativo, que poderá restar em sanção severa, conforme a gravidade do ato e os prejuízos sofridos.

Art. 17. Não é permitido o acesso ou uso de qualquer recurso de TIC ou ativo da informação sem as credenciais de acesso correspondentes.

Art. 18. O agente judiciário 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. 19. 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.

CAPÍTULO V

AQUISIÇÃO, UTILIZAÇÃO, CONTROLE E DESCARTE DE RECURSOS DE TIC

Art. 20. Todas as informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao agente judiciário ou das quais tiver acesso no exercício de suas atividades, são de propriedade e/ou direito de uso exclusivo do TJPE.

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

Art. 21. Os recursos de TIC de propriedade do TJPE somente poderão ser utilizados pelos magistrados e servidores.

Parágrafo único. Outras classes de agentes do judiciário e o público externo somente poderão fazer uso dos recursos se forem previamente autorizados, por mecanismo formal, pela Presidência do TJPE, levando em consideração quaisquer responsabilidades legais na concessão.

Art. 22. A utilização de qualquer recurso da infraestrutura de tecnologia deve ser restrito à execução de atividades inerentes e previamente previstas para o desempenho de suas funções ou concessões formalmente divulgadas pelo TJPE, seguindo a política de conceder apenas as permissões indispensáveis para realização das suas atividades.

Art. 23. Todos os equipamentos, dispositivos e demais recursos que fizerem uso da infraestrutura de TIC do TJPE deverão estar sujeitos à PSI e às demais normas de Segurança da Informação do TJPE e deverão possuir softwares de proteção instalados, a exemplo, mas não se limitando, de antivírus, anti-spyware e firewall sempre ativos e atualizados.

Art. 24. São direitos do TJPE, através da SETIC, registrar, bloquear, permitir, suspender e limitar o uso dos recursos e dispositivos que compõem sua infraestrutura de TIC.

Art. 25. O TJPE, 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 O TJPE 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* , o TJPE 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. 26. Não é permitido aos agentes judiciários tirarem fotos, capturarem imagens, som ou vídeo do ambiente compreendido no perímetro físico sob gerenciamento do TJPE ou divulgar esses materiais sem uma autorização prévia da instituição.

Art. 27. É vedado aos agentes do judiciário acessar ou armazenar, a partir de dispositivos ou recursos de TIC do TJPE 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 do TJPE, 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 do TJPE, 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;

conteúdos ou serviços de TIC de ordem pessoal dos agentes judiciários 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 do TJPE 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 estatutária, conforme sua gravidade e prejuízo ao TJPE.

Art. 28. O TJPE aconselha aos agentes judiciários 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. 29. Apenas é permitido aos agentes judiciários 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. 30. 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 pelo TJPE. As exceções devem ser previamente aprovadas pelos responsáveis pelo serviço e realizadas em data e horário de menos impacto possível.

Art. 31. 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. 32. A mera disponibilidade ou operação contínua e involuntária de recursos de TIC para acesso remoto às informações ou recursos do TJPE não configura sobrejornada, horas extras, sobreaviso ou qualquer consequência que configure atividade laboral ou estatutária que mereça remuneração além dos vencimentos já firmados.

Art. 33. O acesso remoto aos recursos de TIC do TJPE deve ser previamente homologado pela SETIC, que indicará as configurações adequadas e controles de segurança necessários para que haja o uso seguro pelos agentes judiciários.

Art. 34. Sempre que o agente judiciário 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. 35. É permitido o uso de dispositivos pessoais de TIC pelos agentes judiciários nos ambientes do TJPE, desde que não haja restrição conforme seu perfil profissional e que não traga prejuízos para o TJPE.

§ 1º Os agentes judiciários serão integralmente responsáveis pelos conteúdos armazenados em seus dispositivos pessoais e pelos atos através deles praticados, sem ressalvas ou exceções.

§ 2º Os agentes judiciários 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 ao TJPE, sob pena de perderem o benefício e sofrerem outras sanções disciplinares, mediante competente Processo Administrativo.

Art. 36. Todos os relacionamentos e contratações em que haja o compartilhamento de informações ou ativos de TIC do TJPE ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos devem ser precedidos por Termos de Confidencialidade e cláusulas contratuais que tratem especificamente da Segurança da Informação.

Art. 37. O descarte de informações e ativos de TIC do TJPE 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. 38. Os agentes judiciários 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 judiciário.

CAPÍTULO VI

DESENVOLVIMENTO, AQUISIÇÃO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

Art. 39. Os Sistemas de Informação adquiridos, mantidos ou desenvolvidos pelo TJPE deverão atender aos princípios e requisitos de Segurança da Informação, estabelecidos pela presente Resolução e demais normas em vigor.

Art. 40. 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. 41. 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 do TJPE.

Parágrafo único. O descumprimento desta disposição acarretará em Procedimento Administrativo disciplinar e justificará a aplicação de penas previstas em lei, conforme a gravidade do ato e prejuízos sofridos pelo TJPE.

CAPÍTULO VII

ANÁLISE DE CONFORMIDADE E AUDITORIAS

Art. 42. Ao TJPE 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.

CAPÍTULO VIII

RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 43. 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. 44. A SETIC tem o dever de guardar as provas produzidas pelos recursos e dispositivos de TIC pelo tempo previsto na tabela de temporalidade do TJPE, sobretudo em casos de incidente de Segurança de Informação.

CAPÍTULO IX

GERENCIAMENTO DE RISCOS

Art. 45. 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. 46. É de responsabilidade do CGTIC a administração dos riscos identificados.

CAPÍTULO X

PLANO DE CONTINUIDADE DO NEGÓCIO E RECUPERAÇÃO DE DESASTRES

Art. 47. 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 do TJPE por eles suportados.

Art. 48. É de responsabilidade do CGTIC aprovar a estratégia de continuidade do plano e fornecer subsídios para a sua implementação.

Art. 49. 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.

CAPÍTULO XI

VIOLAÇÕES DA PSI E SANÇÕES

Art. 50 Todos os agentes judiciários 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 pelo TJPE, sem prejuízo de comunicação administrativa conforme o caso e urgência, formalmente.

Art. 51 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. 52 Todos os documentos da Estrutura Normativa de Segurança da Informação do TJPE estão disponibilizados em [www.tjpe.jus.br/seguranca].

Art. 53 Casos omissos ou esclarecimentos da PSI, normas e procedimentos correlatos são de exclusiva responsabilidade do CGTIC e passíveis de aprovação pela Presidência do TJPE, conforme o caso.

Art. 54 Esta Resolução entra em vigor na data de sua publicação.

Desembargador JOVALDO NUNES GOMES

Presidente

(Resolução unanimemente aprovada na Sessão Ordinária da Corte Especial do dia 04.03.2013)