REF.15616

DECRETO 22.249, DE 25 DE JULHO DE 2023

Institui a Política Estadual de Segurança da Informação e Comunicação do Estado do Piauí - POSIC, e dá outras providências.

O GOVERNADOR DO ESTADO DO PIAUÍ, no uso das atribuições que lhe conferem os incisos I, V e XIII do artigo 102 da Constituição Estadual,

CONSIDERANDO o disposto na Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados);

CONSIDERANDO o Decreto Estadual nº 21.979, de 13 de abril de 2023, que institui a Política de Transformação Digital do âmbito do Poder Executivo do Estado, o portal único de serviços, regulamenta as Leis Federais nº 14.129, de 29 de março de 2021, e nº 13.460, de 26 de junho de 2017;

CONSIDERANDO a Lei Federal nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos;

CONSIDERANDO a Lei Federal nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

CONSIDERANDO o disposto na Lei Federal nº 12.257, de 18 de novembro de 2011, Lei de Acesso a Informação;

CONSIDERANDO o Decreto Federal nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação;

CONSIDERANDO o Ofício nº 970/2023/ATI-PI/DIR GERAL, de 14 de julho de 2023, da Agência de Tecnologia da Informação - ATI-PI, registrado no SEI nº 00117.000874/2023-54,

D E C R E T A:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º A Política Estadual de Segurança da Informação e Comunicação - POSIC, atendendo ao Sistema de Gestão da Segurança da Informação - SGSI, fundamentado na Norma NBR ISO/IEC 27001, contém um conjunto diversificado de informações, tais como diretrizes e recomendações, regras, infrações, penalidades, responsabilidade do usuário, abrangência da política de segurança, entre outros, aplicados a todas as pessoas que utilizam as informações, sistemas, infraestruturas e dependências de propriedade ou de responsabilidade do Estado do Piauí.

Art. 2º A Segurança da Informação é o conjunto de propriedades que proporcionam disponibilidade, integridade, confidencialidade, autenticidade, responsabilidade, confiabilidade e não repúdio aplicado sobre os sistemas de informação.

§ 1º Para alcançar objetivos deste Decreto, deverá ocorrer a criação de controles que abordem acordos de confidencialidade, uso de contas e senhas, uso de rede, acesso à Internet, mensagens eletrônicas, acesso remoto, instalação e remoção de **software**, cópias de segurança e alienação do equipamento.

§ 2º Os órgãos e entidades estaduais deverão desenvolver suas políticas de segurança da informação e comunicação, alinhadas com o Planejamento Estratégico de suas áreas e com foco nas estratégias de Governo apresentadas nesta POSIC.

§ 3º O acompanhamento permanente da aplicação dessa política compete ao órgão central de Tecnologia de Informação e Comunicação - TIC, considerando também o caráter dinâmico da segurança da informação no âmbito nacional e internacional.

Art. 3º A POSIC deve servir como guia para todos os órgãos e entidades estaduais do Poder Executivo Estadual implementarem e manterem a gestão de Segurança da Informação e Comunicação - SIC nos seus ambientes de TIC.

CAPÍTULO II
DOS OBJETIVOS E DO ESCOPO

Art. 4º A Política de Segurança da Informação e Comunicação - POSIC tem por objetivo definir e implantar, no âmbito do Estado do Piauí, os princípios, diretrizes e instrumentos da Política Estadual de Segurança da Informação, preconizando a elaboração, coordenação e execução da Política Estadual de Informática e de Tecnologia da Informação.

§ 1º A POSIC considera ainda o disposto na Lei nº 13.709, de 14 de agosto de 2018, que institui a Lei Geral de Proteção de Dados - LGPD, e as instruções relacionadas à segurança da informação dispostas na legislação federal pertinente.

§ 2º Todos os instrumentos normativos gerados a partir desta Lei são parte integrante da POSIC e emanam dos princípios e diretrizes nela estabelecido.

Art. 5º A Política de Segurança da Informação e Comunicação do Estado do Piauí busca atingir os seguintes objetivos abaixo descritos:
I - promover a análise, operação, monitoramento e implementação da política de segurança, mantendo e melhorando o gerenciamento da Segurança da Informação e Proteção de Dados;
II - definir os princípios e diretrizes gerais que visam à preservação da Segurança da Informação, primando pela confidencialidade, integridade, disponibilidade, autenticidade, bem como legalidade dos processos que amparam a operacionalização e gestão das atividades dos órgãos e entidades estaduais;
III - auxiliar no estabelecimento das responsabilidades de atuação dos servidores, colaboradores, consultores externos, estagiários e prestadores de serviços, independentemente do vínculo que possuam com a Administração, que desempenham atividades no âmbito do Governo do Estado do Piauí ou de qualquer pessoa que tenha acesso a dados ou informações.

Art. 6º A POSIC-PI abrange os domínios de segurança e defesa cibernética, a segurança física e a proteção de dados organizacionais, tendo por escopo as ações destinadas à preservação da disponibilidade, integridade, confidencialidade e autenticidade das informações e dados, bem como a proteção de dados pessoais e a privacidade, incluindo o estabelecimento de:
I - diretrizes no que se refere a comportamentos, procedimentos e normas de segurança da informação, comunicação e proteção de dados;
II - estrutura de gestão de segurança da informação, comunicação e proteção de dados adequada às diretrizes institucionais, considerando um conjunto de papéis, responsabilidades e instrumentos normativos e organizacionais;
III - orientações gerais de segurança da informação, comunicação e proteção de dados em harmonia com a legislação vigente, as boas práticas e a gestão eficiente dos riscos associados.

Art. 7º As diretrizes e orientações previstas nesta Política, nas demais normas específicas associadas e suas eventuais metodologias, manuais, procedimentos e documentos correlatos são aplicadas a todos os servidores, demais colaboradores do Governo do Estado do Piauí e a terceiros que tenham acesso às informações e dados e aos recursos de Tecnologia da Informação e Comunicação.

CAPÍTULO III
DOS PAPÉIS E DAS RESPONSABILIDADES GERAIS

Art. 8º Para assegurar o alcance dos objetivos elencados no Capítulo II deste Decreto, deverão ser identificados os papéis do processo de segurança da informação nas organizações, assim como esclarecer suas responsabilidades.

§ 1º Para os efeitos deste Decreto, entende-se por:
I - papéis: funções inerentes ao servidor ou prestador de serviço de um órgão governamental;
II - responsabilidades: conjunto de atribuições ligadas ao cargo do servidor ou prestador de serviço que está ligado ao processo de segurança da informação.

§ 2º Os papéis e responsabilidades dos envolvidos no processo de segurança da informação deverão ser atendidos na forma dos arts. 9º, 10 e do Capítulo IV deste Decreto.

Art. 9º A Política Estadual de Segurança da Informação e Proteção de Dados envolve os seguintes papéis e responsabilidades:
I - SUBCOMITÊ DE SIC: alta administração formada por grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão;
II - ENCARREGADO DE PROTEÇÃO DE DADOS: assessores técnicos, pessoa física ou jurídica, com conhecimento técnico em proteção de dados e privacidade, de acordo com a Lei Federal nº 13.709, de 2018, com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas aos incidentes de proteção de dados e privacidade;
III - GESTOR DE SIC: Diretoria Técnica responsável pelas ações de segurança da informação e comunicações no âmbito do órgão;
IV - ÁREA DE TIC: Gerência/Coordenação de Tecnologia da Informação, formada por uma unidade organizacional responsável pela gestão e operação dos recursos de TIC na organização e custodiante da informação;
V - GESTORES: Secretários, Diretores Gerais, Presidentes, Superintendentes, Diretores e demais cargos de chefia, considerando-se todos aqueles que exercem funções de gerência no âmbito da organização, administrando pessoas e processos;
VI - USUÁRIO INTERNO: servidores públicos, terceirizados, demais funcionários e colaboradores internos, considerando-se todos os servidores, gestores, técnicos, estagiários, bolsistas de programas educacionais, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais do Governo do Estado do Piauí;
VII - USUÁRIO EXTERNO: prestadores de serviços e demais colaboradores externos, contratados direta ou indiretamente pela Administração e demais colaboradores externos e particulares que tenham relações jurídicas com contratos, requerimentos administrativos, entre outros, que fazem uso de recursos informacionais e computacionais.

Art. 10. São responsabilidades gerais e comuns a todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos de informação e comunicação do Governo do Estado do Piauí:
I - zelar pela segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso;
II - seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos corporativos de informação e comunicação, utilizando-os sempre de forma ética, legal e consciente;
III - manter-se atualizado em relação a esta POSIC-PI e às suas normas complementares e procedimentos relacionados, buscando informação junto ao Gestor de Segurança da Informação e Comunicações sempre que não estiver absolutamente seguro quanto à obtenção, tratamento, uso e/ou descarte de informações.

CAPÍTULO IV
DAS RESPONSABILIDADES ESPECÍFICAS

Seção I
Dos Usuários Internos e Externos

Art. 11. Todo prejuízo ou dano decorrente da não obediência às diretrizes e normas referenciadas nesta Política de Segurança da Informação e Comunicações e nas normas e procedimentos específicos dela decorrentes é de inteira responsabilidade do usuário interno ou externo que o der causa.

Art. 12. Os usuários externos devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos vigentes de segurança da informação e comunicações.

Art. 13. Gestor do órgão ou entidade poderá, de forma justificada e motivada, revogar credenciais de acesso concedidas aos usuários em virtude do descumprimento desta POSIC-PI ou das normas complementares e procedimentos específicos dela decorrentes.

Parágrafo único. Ninguém pode se escusar do conhecimento das regras contidas nesta POSIC-PI, sendo que a alegação de seu desconhecimento não exime o usuário de suas responsabilidades por atos praticados em sua desconformidade.

Seção II
Dos Gestores de Pessoas e Processos

Art. 14. Os gestores dos órgãos e entidades estaduais devem manter postura exemplar em relação à segurança da informação e comunicações, diante, sobretudo, dos usuários sob sua gestão.

Art. 15. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de Segurança da Informação e Comunicações do Estado do Piauí, tomando as ações necessárias para cumprir tal responsabilidade.

Seção III
Da Área de Tecnologia da Informação e Comunicação

Art. 16. No tocante à gestão de segurança da informação e comunicações, serão responsabilidades específicas da área de Tecnologia da Informação e Comunicação:

I - zelar pela eficácia dos controles de SIC utilizados e informar aos gestores e demais interessados os riscos residuais, como vulnerabilidades não identificadas, riscos emergentes, erros de configuração, falhas de implementação ou manutenção ou ameaças internas;

II - negociar e acordar com os gestores níveis de serviço relacionados a SIC, incluindo os procedimentos de resposta a incidentes;

III - configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de Segurança da Informação e Comunicações; IV - gerar e manter trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes, devendo ser implantados controles de integridade para as trilhas geradas ou mantidas em meio eletrônico, de modo a torná-las juridicamente válidas como evidências;

V - garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

VI - zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e eliminar a existência de pessoas que possam excluir logs e trilhas de auditoria das suas próprias ações;

VII - administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para o Estado do Piauí;

VIII - implantar controles que gerem registros auditáveis para retirada e transporte de mídias que contenham informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

IX - informar previamente o Gestor de SIC sobre o fim do prazo de retenção de informações, para que este tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custodiante;

X - assegurar-se, nas movimentações internas dos ativos de TIC, de que as informações de determinado usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;

XI - gerir a capacidade de armazenamento, processamento e transmissão de dados de forma a garantir os níveis de segurança requeridos;

XII - atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta;

XIII - proteger continuamente todos os ativos de informação contra ameaças de segurança, buscando assegurar que novos ativos apenas sejam integrados ao ambiente de produção após cumprirem os requisitos de segurança da informação definidos;

XIV - zelar pela não introdução de vulnerabilidades ou fragilidades indesejadas nos ativos de informação ou nos ambientes informacionais do Estado do Piauí durante sua operação ou durante eventos de mudança de ambiente, tais como de desenvolvimento para teste, homologação ou produção;

XV - definir regras para instalação de softwares e hardwares no ambiente corporativo e demais ambientes vinculados, incluindo aqueles dedicados ao uso pelo público externo;

XVI - definir metodologia e realizar auditorias periódicas de configurações técnicas e análise de riscos;

XVII - responsabilizar-se pelo uso, manuseio, guarda de assinatura de certificados digitais corporativos;

XVIII - garantir, da forma mais rápida possível, com recebimento de solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento do órgão, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos do instituto;

XIX - garantir que todos os servidores, estações de trabalho e demais dispositivos com acesso à rede operem com o relógio sincronizado com os servidores de tempo oficiais do Governo;

XX - monitorar o ambiente de TIC, gerando indicadores e históricos de uso da capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos, períodos de indisponibilidade no acesso à internet e aos sistemas críticos, incidentes de segurança e atividade de todos os usuários durante os acessos às redes externas, inclusive internet.

Seção IV
Gestor de Segurança da Informação e Comunicação

Art. 17. Compete ao Gestor de Segurança da Informação e do órgão:

I - promover cultura de segurança da informação e comunicação no âmbito de suas atribuições dentro do órgão governamental;

II - acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança da informação;

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

IV - coordenar o Subcomitê de Segurança da Informação e Comunicação e a Equipe Técnica de Tratamento de Incidentes em Redes Computacionais (ETIR);

V - realizar e acompanhar estudos de novas tecnologias no que tange aos aspectos relacionados à segurança da informação;
VI - manter contato com a Agência de Tecnologia da Informação e Comunicação do Estado do Piauí ou outra entidade que venha substituí-la, nos termos da Lei nº 8.017, de 10 de abril de 2023;
VII - propor normas internas relativas à segurança da informação e comunicação.

Seção V
Encarregado de Proteção de Dados

Art. 18. São responsabilidades específicas do Encarregado de Proteção de Dados coordenar as atividades de tratamento de dados e resposta a incidentes em proteção de dados e privacidade e cooperar com outras equipes e participar em fóruns e redes nacionais e internacionais.

Art. 19. São atribuições do Encarregado de Proteção de Dados:
I - atender as demandas dos titulares dos dados dos quais o órgão ao qual o encarregado de dados é a controladora e realizar atividades como, dentre outras:
a) recebimento e registro das solicitações, reclamações e comunicações dos titulares;
b) prestação de esclarecimentos;
c) adoção de providências dentro dos prazos legais e definidos nas políticas da empresa, envolvendo, sempre que necessário, ao fiel e efetivo atendimento dos pedidos, outras áreas da empresa.
II - receber e registrar as comunicações da ANPD - Autoridade Nacional de Proteção de Dados, e de agências de proteção de dados internacionais, quando o órgão ao qual o encarregado de dados estiver abrangido por lei de aplicação extraterritorial, e adotar providências;
III - garantir que as reuniões presenciais ou online com representantes das agências de proteção de dados sejam realizadas sempre por, no mínimo, dois profissionais, para aumentar a segurança, a transparência e a qualidade das interações relacionadas à proteção de dados e evitar possíveis conflitos de interesse ou falhas na comunicação;
IV - registrar em ata as reuniões realizadas com Agência Nacional de Proteção de Dados – ANPD;
V - orientar os empregados e os contratados a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
VI - desempenhar suas atribuições em articulação com o Encarregado de Proteção de Dados do Estado;
VII - receber os registros de incidente de segurança da informação que contenham evidências de que o incidente diz respeito ou relaciona-se à proteção dos dados pessoais;
VIII - elaborar o RIPD - Relatório de Impacto à Proteção de Dados Pessoais e documentos equivalentes eventualmente exigidos por leis internacionais aplicáveis ao órgão ao qual o encarregado de dados está vinculado, envolvendo as áreas necessárias para apoio à composição dos documentos, e transmiti-los às respectivas agências solicitantes, em atendimento à demanda formal;
IX - receber e registrar as orientações das agências de proteção de dados e encaminhá-las às áreas que deverão tomar conhecimento;
X - executar as demais atribuições definidas pelo gestor, por normas complementares do Estado do Piauí ou agências de proteção de dados;
XI - contribuir com investigações, internas ou externas, relacionadas, dentre outras coisas, ao acesso não autorizado, uso inadvertido de dados pessoais;
XII - contribuir com o mapeamento do ciclo de vida dos dados pessoais;
XIII - gerenciar incidentes de segurança em redes computacionais;
XIV - investigar e avaliar danos decorrentes de quebras de segurança;
XV - registrar todos os incidentes de proteção de dados e privacidade, com a finalidade de assegurar registro histórico de incidentes;
XVI - realizar tratamento da informação de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

Seção VI
Subcomitê de Segurança da Informação e Comunicação

Art. 20. Compete ao Subcomitê de Segurança da Informação e Comunicação dos órgãos governamentais:
I - assessorar o órgão na implementação das ações de Segurança da Informação;
II - constituir grupos de trabalho para de tratar temas e propor soluções específicas sobre Segurança da Informação e Comunicação;
III - propor alterações e revisar periodicamente a Política de Segurança da Informação e Comunicações do Estado do Piauí, em conformidade com a legislação existente sobre o tema;
IV - propor, aprovar, alterar e revisar normas complementares e procedimentos internos de Segurança da Informação e Comunicação, em conformidade com a legislação existente sobre o tema;
V - propor investimentos relacionados à Segurança da Informação e Comunicação;

VI - propor procedimentos administrativos e definir medidas corretivas e punitivas cabíveis nos casos de descumprimento da Política de Segurança da Informação e Comunicações ou de suas normas e procedimentos complementares;
VII - coordenar a Equipe Técnica de Tratamento de Incidentes em Redes Computacionais (ETIR).

Art. 21. O Subcomitê de Segurança da Informação e Comunicação é uma estrutura permanente formalmente instituída e subordinada ao Comitê Gestor dos Recursos de Tecnologia da Informação e Comunicação (COGESTI) do Estado do Piauí, cuja estrutura e composição será regulamenta por meio de portaria específica.

CAPÍTULO V
DO TRATAMENTO DA INFORMAÇÃO

Art. 22. As diretrizes específicas e os procedimentos próprios de tratamento da informação corporativa serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:
I - documentos corporativos imprescindíveis às atividades dos usuários deverão ser salvos em dispositivos de rede, não ficando cobertos pelo serviço de backup (cópias de segurança) os arquivos gravados localmente, nos computadores dos usuários, sujeitos a perda e a não recuperação;
II - arquivos pessoais e/ou não pertinentes às atividades laborais do servidor, tais como fotos, músicas e vídeos, não deverão ser copiados ou movidos para os dispositivos de rede, por conta de possível sobrecarga da capacidade de armazenamento e conter vulnerabilidades e riscos de segurança, devendo, caso identificados, ser excluídos de forma imediata e definitiva sem necessidade de comunicação prévia ao usuário;
III - normas de classificação de informações, acesso à informação, uso e descarte de ativos de informação, dentre outros temas afins, serão fixadas em estrita aderência às leis e normas atinentes à Administração Pública Estadual, conforme as competências regimentais.

Seção I
Do Acesso à Intranet, Internet e Uso de Mensagem

Art. 23. Diretrizes específicas e procedimentos de acesso à intranet, internet e uso de mensagem serão regulamentados em norma complementar considerando as diretrizes gerais definidas nos arts. 24 a 27 deste Decreto.

Art. 24. As comunicações por meio eletrônico, o armazenamento de mensagens, ou qualquer informação produzida no ambiente corporativo são de propriedade e de responsabilidade do Estado do Piauí, devendo o seu conteúdo ter tratamento adequado à preservação das propriedades de autenticidade, confidencialidade, disponibilidade, integridade e legalidade das informações.

Art. 25. Os serviços corporativos de correio eletrônico, mídias sociais, mensagens instantâneas, intranet e internet devem ter seu uso orientado para o interesse do Estado do Piauí.

Art. 26. O uso dos serviços de Internet e de mensagem deve estar em conformidade com perfis funcionais definidos em norma e procedimento complementar.

Art. 27. O usuário se compromete a respeitar toda a conduta de uso de mensagens eletrônicas e de acesso à internet e intranet.

Seção II
Do Serviço de Backup e Restore

Art. 28. Os procedimentos próprios ao serviço de **backup** (cópia de segurança) e **restore** (restauração de cópia de segurança) serão regulamentados em norma complementar, considerando as seguintes diretrizes gerais:
I - o **backup** dos sistemas governamentais deve ser controlado pelo órgão executor e concedido somente a pessoas identificadas e autorizadas;
II - as cópias de segurança devem ser testadas e avaliadas;
III - os órgãos executores devem manter relatórios de logs dos **backups** realizados.

Seção III
Da auditoria e conformidade

Art. 29. Para garantir a aplicação das diretrizes mencionadas nesta POSIC-PI, além de fixar normas e procedimentos complementares sobre o tema, o órgão deverá seguir as seguintes diretrizes de controle:

I - proceder ao exame sistemático do grau de atendimento dos requisitos relativos à segurança da informação e comunicações com as legislações e normas vigentes;
II - efetuar a análise de conformidade em segurança da informação e comunicações deve ser efetuada criticamente, em intervalos regulares.

Art. 30. As normas e procedimentos complementares de Auditoria e Conformidade devem ser especificados de acordo com requisitos legais, observando-se a prevenção contra uso indevido de recursos de processamento da informação, monitoramento de uso e política de acesso.

Seção IV
Da Gestão do Risco

Art. 31. A diretriz geral do processo de Gestão de Riscos de Segurança da Informação e Comunicações deverá considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão, direta e indireta, além de estarem alinhadas a esta Política de Segurança da Informação e Comunicações.

Art. 32. O Governo do Estado do Piauí estabelecerá o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC.

Parágrafo único. O pocesso de que trata o **caput** deverá abordar:
I - a definição do contexto para identificação dos riscos;
II - a análise e avaliação dos riscos; o tratamento, aceitação e comunicação às partes interessadas;
III - a realização contínua do monitoramento e da análise crítica dos riscos.

Seção V
Da Gestão de Continuidade

Art. 33. O Programa de Gestão de Continuidade de Negócios dos órgãos estaduais deverá ser composto, no mínimo, pelos seguintes Planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas:
I - 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;
II - Plano de Continuidade de TIC: documentação dos procedimentos e informações necessárias para que o órgão mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas de TIC, num nível previamente definido, em casos de incidentes;
III - Plano de Recuperação de TIC: documentação dos procedimentos e informações necessárias para que o órgão operacionalize o retorno das atividades críticas de TIC à normalidade.

Art. 34. Os planos acima definidos deverão ser testados e revisados periodicamente, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Seção VI
Do Canal de Ouvidoria

Art. 35. Será estabelecido canal de ouvidoria a ser divulgado aos gestores, servidores públicos, colaboradores, prestadores de serviços e parceiros do Estado do Piauí para reportar a ocorrência de incidentes de segurança da informação, comunicação e privacidade, podendo ser realizado de forma identificada ou por denúncia anônima, em sítio oficial.

Seção VII
Da Capacitação

Art. 36. Deverão ser treinados e capacitados os servidores e colaboradores do Estado do Piauí, desde a fase de admissão, nos procedimentos e no uso correto das informações e ativos sob sua responsabilidade, a fim de minimizar possíveis riscos de segurança.

Art. 37. O Estado do Piauí deve capacitar seus servidores em matéria de Segurança da Informação, Comunicações, Proteção de Dados e Privacidade.

Seção VIII
Do Controle de Acesso

Art. 38. Devem ser observadas as seguintes diretrizes:
I - o controle de acesso deve ser implementado, garantindo que apenas pessoas identificadas e autorizadas tenham permissão para entrar, podendo ser flexibilizada a aplicação dessa regra, conforme as particularidades de determinados locais , como escolas e hospitais em áreas remotas, levando em consideração a segurança e a praticidade;
II - as autorizações de acesso devem ser concedidas com base na necessidade do conhecimento da informação, condição inerente ao efetivo exercício de cargo, função ou atividade;
III - o acesso a informações e recursos de Tecnologia da Informação será provido via perfis de trabalho, ou por solicitação especial ao Gestor de Segurança da Informação e Comunicação de cada entidade;
IV - o usuário é responsável pela própria e devida autenticação nos sistemas computacionais disponibilizados pelo Governo, não podendo fornecer e/ou compartilhar seu usuário, senha e/ou acesso a outros usuários;
V - o acesso de colaboradores à informação e aos recursos de processamento da informação não deve ser permitido até que os controles sejam implementados e o contrato que define os termos para a conexão ou acesso seja assinado.

§ 1º No caso de ambientes computacionais, é imprescindível que se exija a identificação e autorização adequadas para garantir a segurança das informações e dos sistemas.

§ 2º Esta Política deve ser observada no que concerne à assinatura do contrato a que se refere o inciso V deste artigo ou na contratação externa para processamento da informação.

Seção IX
Do Desenvolvimento Seguro de Sistemas

Art. 39. Os processos de desenvolvimento de Sistemas de Informação devem observar as melhores práticas e padrões de desenvolvimento seguro, como a definição de requisitos de segurança, seleção de controles adequados, implementação de boas práticas de desenvolvimento seguro, realização de testes e revisões de segurança, e manutenção contínua da segurança, em conformidade com a ISO/IEC 27034, desde a fase do planejamento, visando à Privacidade e Gestão de Riscos de Segurança da Informação e Comunicação, sendo considerados os seguintes aspectos:
I - avaliação de riscos: identificação e avaliação dos riscos de segurança da informação associados ao desenvolvimento e uso dos sistemas, considerando as ameaças, vulnerabilidades e impactos potenciais;
II - os princípios de privacidade por design para incorporar desde o início dos processos de desenvolvimento de sistemas os princípios de privacidade, garantindo a proteção adequada dos dados pessoais;
III - controles de acesso: implementação de mecanismos adequados de autenticação, autorização e controle de acesso aos sistemas, garantindo que apenas usuários autorizados possam interagir com as informações;
IV - criptografia: utilização de técnicas de criptografia para proteger dados sensíveis durante o armazenamento, transmissão e processamento;
V - testes de segurança: realização de testes regulares de segurança, como testes de penetração, para identificar vulnerabilidades e garantir a robustez dos sistemas.

Seção X
Da Privacidade e Proteção de Dados

Art. 40. É dever do Estado do Piauí respeitar a privacidade dos titulares de dados e garantir a autenticidade, confidencialidade, disponibilidade, integridade e legalidade dos dados pessoais em todo o seu ciclo de vida, que vai desde a coleta, retenção, tratamento, compartilhamento e a eliminação, em qualquer tipo de dado pessoal.

Art. 41. Os órgãos e as entidades estaduais devem:
I - assegurar o **compliance** dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação da proteção de dados pessoais;
II - desenvolver e implementar procedimentos para a preservação da privacidade e proteção de dados, e que esses procedimentos sejam comunicados a todas as partes interessadas relevantes envolvidas no tratamento dos dados pessoais.
III - implementar medidas técnicas e organizacionais adequadas para proteger dados.

CCAPÍTULO VI
DO TRATAMENTO DE INCIDENTES

Art. 42. É dever dos gestores, servidores públicos, colaboradores, prestadores de serviços e parceiros do Estado do Piauí reportar imediatamente eventos ou incidentes de segurança da informação à Equipe de Tratamento de Resposta a Incidentes em Redes Computacionais (ETIR), devendo os incidentes de segurança ser registrados, avaliados e tratados.

CCAPÍTULO VII
DAS PENALIDADES

Art. 43. Os recursos de TIC são de propriedade do Estado do Piauí e fornecidos para uso corporativo, para os fins a que se destinam, e no interesse da Administração Pública.

Art. 44. É considerada imprópria a utilização destes recursos, assim como das informações de propriedade do Estado do Piauí, para fins não profissionais ou não autorizados.

Parágrafo único. Ao tomarem conhecimento desta prática, servidores e colaboradores devem informá-la ao superior imediato, para que sejam aplicadas as ações disciplinares cabíveis.

Art. 45. Os casos omissos desta política serão tratados pelo Comitê de Segurança da Informação e Comunicações.

CCAPÍTULO VIII
DAS ATUALIZAÇÕES DA POSIC-PI

Art. 46. A Política de Segurança da Informação e Comunicação – POSIC deverá ser revisada em função de alterações na legislação pertinente, tanto estadual quanto federal, de alterações nos normativos internos, quando considerada necessária ou no prazo máximo de 02 (dois) anos, a contar da data de sua publicação.

Art. 47. Os órgãos poderão expedir normas complementares associadas à POSIC-PI, no âmbito de sua competência regimental, visando detalhar particularidades e procedimentos relativos à sua implementação no âmbito do Estado do Piauí.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 48. Para a uniformização da informação organizacional, esta Política de Segurança da Informação e Comunicação – POSIC deverá ser comunicada a todos os servidores, colaboradores, prestadores de serviço e gestores do Estado do Piauí, para o fiel cumprimento deste Decreto.

Art. 49. O não cumprimento dos preceitos e requisitos preconizados nesta política, nas normas complementares e nos procedimentos de Segurança da Informação e Comunicações constitui violação às regras internas do Governo do Estado do Piauí e sujeitará o usuário às medidas administrativas e legais cabíveis.

Art. 50. As dúvidas sobre esta Política e seus documentos associados devem ser submetidas à Agência de Tecnologia da Informação do Estado do Piauí ou entidade que venha a substituí-la, nos termos da Lei nº 8.017, de 10 de abril de 2023.

Art. 51. Este Decreto entra em vigor na data de sua publicação.

PALÁCIO DO KARNAK, em Teresina (PI), 25 de julho de 2023.

(assinado eletronicamente)
RRAFAEL TAJRA FONTELES
Governador do Estado do Piauí

(assinado eletronicamente)
MMARCELO NUNES NOLLETO
Secretário de Governo