cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. 1.7. Lembremos também que a já citada LGPD traz um entendimento de uma nova cultura de privacidade e proteção de dados no país, o que demanda a conscientização de toda a sociedade acerca da importância dos dados pessoais e os seus reflexos em direitos fundamentais. Nesse sentido, a SOP emitiu e publicou em Diário Oficial do Estado de 03 de fevereiro de 2026, a Portaria nº 0041/2026, que instituiu o Comitê Setorial de Proteção de Dados Pessoais e Encarregado pelo Tratamento de Dados Pessoais da SOP, na forma dos Art. 9º e 10º da lei Estadual nº 18.699, de 7 de março de 2024; 1.8. Vale ainda destacar que a PoSIC/SOP denota o cumprimento das recomendações exaradas pelo Tribunal de Contas do Estado, aferidas por meio do Questionário de Auto Avaliação do Controle Interno – Procedimentos de Controle, da Prestação de Contas Anual, bem como a avaliação da SOP pelo Programa Nacional de Gestão Pública e Desburocratização – GesPública, focado em elevar a qualidade da administração pública por meio de modelos gerenciais de excelência e desburocratização. 2. APRESENTAÇÃO DA POLÍTICA 2.1. A Superintendência de Obras Públicas (SOP), apresenta sua Política de Segurança da Informação e Comunicação dos Ambientes de TIC, que visa estabelecer princípios, diretrizes e responsabilidades para a Gestão da Segurança da Informação e Proteção de Dados Pessoais, voltadas ao cumprimento do seu papel como responsável pela elaboração de projetos arquitetônicos e complementares, bem como pela supervisão e fiscalização da execução de todas as obras civis públicas de Edificações e de Rodovias, solicitadas pelas diversas Secretarias e Entidades Públicas que não possuem finalidades construtivas, fortalecendo a gestão pública e o desenvolvimento econômico e social. 2.2. A Política de Segurança da Informação e Comunicação da SOP, definida neste documento, alinha-se à diretriz de Governo de "Rever e aplicar Políticas da Segurança da Informação e Comunicação do Estado", elaborada no Planejamento Estratégico da Função Tecnologia da Informação do Governo do Estado do Ceará. 2.3. Dessa forma, nesta política passam a figurar 03 (três) elementos principais: a) Princípios, que são os fundamentos da Política de Segurança da Informação e Comunicação; b) Diretrizes, que são as regras de alto nível que representam os princípios básicos que o Governo do Estado do Ceará resolveu incorporar a sua gestão e servirão como base para que as normas e os procedimentos sejam criados e detalhados; e c) Normas e Procedimentos, que especificam no plano tático os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes e servir como base para os procedimentos no plano operacional, constantes da Instrução Normativa a ser expedida. 3. OBJETIVO 3.1. Estabelecer princípios e diretrizes gerais para a gestão da segurança da informação e comunicação dos ambientes de TIC da SOP, de maneira a preservar a integridade, confidencialidade e disponibilidade das informações, posteriormente através de Instrução Normativa descrevendo as normas e procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados. 4. ABRANGÊNCIA 4.1. A Política de Segurança da Informação e Comunicação deverá ser aplicada a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação existentes na SOP, inclusive em ambientes remotos, em nuvem ou terceirizados, como também às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito da Superintendência de Obras Públicas – SOP, ou a quem venha a ter acesso a dados ou informações, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação. 4.2. Diretrizes Gerais da Política de Segurança da Informação e Comunicação da SOP a) Diretrizes do Princípio 1 - Alinhamento Estratégico ● Conflitos de negócios: Na existência de conflito entre os controles de segurança e uma necessidade de negócio específica, o novo cenário de controle deve ser analisado pelo Comitê de Gestão de Segurança da Informação da SOP, conforme preconiza o Decreto Estadual nº 34.100 que regulamenta a PoSIC/SOP; ● Gestão de Riscos: Os ativos, sistemas, processos, produtos e serviços desenvolvidos, adquiridos, implementados ou disponibilizados da SOP devem ser submetidos a um processo formal de análise, avaliação e tratamento de riscos, visando atingir o grau de segurança adequado para o Governo do Estado; ● Gestão de Continuidade: A SOP deve estabelecer um conjunto de estratégias e planos de ação documentados, testados e revisados periodicamente, de maneira a garantir que os seus serviços essenciais sejam devidamente identificados, preservados e entregues, mesmo diante da ocorrência de um desastre até o retorno à situação normal de funcionamento da Instituição; ● Auditoria e Conformidade: A prática da Política de Segurança da Informação e Comunicação da SOP, poderá ser auditada por meio do Comitê Gestor de Segurança da Informação do Governo do Estado, de forma a avaliar a conformidade das ações de seus colaboradores em relação ao estabelecido pela PoSIC/SOP e pela legislação aplicável; ● Monitoramento: O acesso e utilização de ambientes físicos, bem como o uso dos equipamentos e sistemas tecnológicos da SOP, poderão ser monitorados pelo Comitê Gestor de Segurança da Informação do Governo do Estado, de forma que ações indesejáveis ou não autorizadas sejam detectadas proativamente; ● Fortalecer o alinhamento estratégico: A Política de Segurança da Informação e Comunicação dos Ambientes de TIC é agenda estratégica para o Governo do Estado do Ceará, devendo contemplar diretrizes e metas relacionadas ao tema no planejamento estratégico de cada órgão/entidade para fortalecer o alinhamento entre o planejamento de TIC e o planejamento estratégico da SOP, bem como o do Governo do Estado; ● Objetivos estratégicos mínimos: O planejamento estratégico da SOP/2025-2028, que será revisado e adaptado ao próximo Plano Plurianual (PPA), deverá conter no mínimo os objetivos estratégicos de: "Assegurar estruturas e práticas de segurança da informação e comunicação" e "Fortalecer o alinhamento entre o planejamento de TIC, as estratégias da SOP e do Governo do Estado"; ● Responsabilidades dos gestores de TIC e de Ativos TIC: Os gestores de TIC e de ativos de TIC são responsáveis por acompanhar e seguir as Políticas de Segurança da Informação e Comunicação dos Ambientes de TIC do órgão/entidade e do Governo do Estado do Ceará; ● Responsabilidades da alta gestão: A alta gestão formada pelos dirigentes máximos é responsável por acompanhar e seguir a PoSIC da SOP, tendo como referência: Prover os recursos necessários à PoSIC; Promover o desenvolvimento de Políticas de Segurança da Informação e Comunicações dos Ambientes de TIC; Estimular a adoção de práticas de governança de segurança da informação e comunicações; ● Implementar práticas de gerenciamento de riscos e continuidade de negócios. 4.3. Objetivos Estratégicos relacionados às Diretrizes do Princípio 1 - Alinhamento Estratégico: a) Objetivo Estratégico: Desenvolver e implantar uma Política de Segurança da Informação e Comunicação na SOP. ● Ações Prioritárias ● Adotar mecanismos para promover a elaboração, revisão, atualização, divulgação, conscientização e validação dos princípios, diretrizes, normas e procedimentos da Política de Segurança da Informação e Comunicação nos órgãos/entidades estaduais; ● Elaborar plano estratégico de segurança da informação e comunicação para viabilizar todos os recursos necessários para o cumprimento das Políticas de Segurança da Informação e Comunicação; ● Selecionar mecanismos de segurança da informação e comunicação considerando fatores de riscos, tecnologias e custos; ● Criar grupo responsável pela elaboração, implantação, acompanhamento, auditoria e revisão da Política de Segurança da Informação e Comunicação; ● Criar o Comitê de Gestão de Segurança da Informação para coordenar a política de segurança da informação e comunicação da SOP; e ● Estabelecer mecanismos que possibilitem o processo de coleta, recuperação, análise e correspondência de dados para investigação de questões cíveis, criminais e administrativas, para proteger os usuários e recursos de TIC. b) Objetivo Estratégico: Comunicar oficialmente e orientar os usuários na Política de Segurança da Informação e Comunicação dos Ambientes de TIC adotada pela SOP, para garantir a conscientização e a prática. ● Ações Prioritárias: ● Definir mecanismos para garantir a disseminação da cultura de segurança da informação e comunicação na SOP; ● Estabelecer medidas para que a política de segurança da informação e Comunicação dos Ambientes de TIC seja cumprida de forma que as diretrizes, normas e procedimentos de segurança sejam aplicados por todos os usuários; e ● Prover mecanismos de orientação nos procedimentos de segurança e uso correto dos recursos de TIC para todos os usuários. c) Diretrizes do Princípio 2 - Diversidade Organizacional ● Alinhamento da política de segurança da informação e comunicação: A política de segurança da informação e comunicação da SOP deve estar alinhada com a política de segurança da informação e Comunicação dos Ambientes de TIC do Governo do Estado do Ceara; ● Natureza e finalidade das atividades: Deve ser respeitada a natureza e finalidade das atividades de cada órgão/entidade, quanto à elaboração de Políticas, Normas, Procedimentos e controles de segurança corporativa; ● Leis e regimentos: A Política de Segurança da Informação e comunicação deve respeitar as leis e regimentos inerentes à SOP. 4.4. Objetivos Estratégicos relacionados as Diretrizes do Princípio 2 - Diversidade Organizacional: a) Objetivo Estratégico: Desenvolver e implementar plano de contingência e respostas a incidentes, considerando a diversidade das atividades das Instituições, respeitando a natureza e finalidade de cada órgão/entidade de forma a assegurar a continuidade do negócio, bem como o seu reestabelecimento em situação de anormalidade. ● Ações Prioritárias ● Definir os processos e recursos críticos realizando análise de impacto de riscos para elaboração do plano de continuidade do negócio; ● Estabelecer processos de proteção contra falhas e danos que comprometam as atribuições do Governo do Estado do Ceará; ● Definir mecanismos formais e periodicamente testados para garantir a continuidade das atividades críticas e o retorno à situação de normalidade; e ● Definir processo e criar procedimentos para gestão de incidentes. b) Diretrizes do Princípio 3 - Garantia da Segurança das Informações ● Responsabilidade e Comprometimento: Todos os colaboradores da SOP, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda dos ativos físicos, tecnológicos e informações de que sejam usuários, dos ambientes físicos e computacionais a que tenham acesso, independente das medidas de segurança implementadas; ● Segurança das Comunicações: Garantir a segurança das comunicações entre a SOP e entidades que compõem o Governo do Estado; ● Controle de Acessos: Os acessos aos ambientes físicos e computacionais devem ser controlados, registrados e monitorados, com base na necessidade de conhecer ações desenvolvidas e do privilégio de acesso mínimo para o desempenho das atividades profissionais; ● Notificação, Registro e Tratamento de Incidentes: Todos os colaboradores da SOP, em qualquer vínculo, função ou nível hierárquico têm a obrigação de reportar imediatamente, por meio dos processos definidos na autarquia, quaisquer incidentes de segurança que tomarem conhecimento, de modo que possam ser registrados, avaliados e tratados; ● Treinamento e Conscientização: Todos os colaboradores devem conhecer a Política de Segurança da Informação e Comunicação da SOP e serem orientados regularmente por meio de campanhas de conscientização e treinamentos, de acordo com suas funções, garantindo assim maior efetividade e eficácia das ações de segurança da Informação e comunicação; ● Revisão e análise crítica: Os conjuntos de documentos que compõem a PoSIC/SOP devem passar por revisões e análises críticas periódicas em no máximo 4 (quatro) anos, ou sempre que ocorrer fato ou evento relevante que motive sua revisão antecipada; ● Proteção Física: Toda proteção física deve ser compatível com o risco identificado. ● Ameaças Externas: Deve ser estabelecida também a proteção contra ameaças externas e do meio ambiente, como proteção contra incêndios e enchentes ou outras formas de desastres naturais; ● Cópias de Segurança: Gerar no mínimo cópias de segurança dos dados classificados como críticos e sua respectiva restauração em tempo aceitável, a fim de não prejudicar o bom andamento das atividades da SOP com uso preferencial do ambiente de nuvem. ● Suporte jurídico: A implantação de uma Política de Segurança da Informação e Comunicação deve contar com suporte jurídico ou de profissionais qualificados sobre os aspectos legais e seus requisitos. 4.5. Objetivos Estratégicos relacionados às Diretrizes do Princípio 3 - Garantia da Segurança das Informações: a) Objetivo Estratégico: Definir procedimentos de rotina para a execução de cópias de segurança e disponibilização dos recursos de reserva. b) Ações Prioritárias ● Implantar rotina de backup (cópias), armazenamento, testes de integridade e recuperação de dados (restore) preferencialmente utilizando o ambiente de nuvem; ● Implantar normas e responsabilidades sobre o controle das mídias de software. c) Objetivo Estratégico: Garantir de forma segura o acesso e manuseio das informações no âmbito da SOP. d) Ações Prioritárias ● Definir normas e procedimentos de acesso a dados, informações e conhecimentos por pessoas da SOP, por outros órgãos/entidades e terceiros. e) Objetivo Estratégico: Assegurar que os sistemas de informações em operação e em implantação, possuam