Instituto de Saúde dos Servidores do Estado do Ceará – ISSEC

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Abril 2024

Superintendente
Katherine Saunders Gondim

Gerente de TIC
Francisco José Magalhães de Pinho

Equipe de Elaboração
Denis Marden Lima Negreiros

Equipe de Revisão
Neyla Maria de King Freire

Política de Segurança da Informação e Comunicação.		
Elaboração:	Revisão:	Aprovação:
Equipe de elaboração: ● Francisco José Magalhães de Pinho ● Denis Marden Lima Negreiros	Equipe de revisão: ● Neyla Maria de King Freire	Aprovado por: ● Francisco José Magalhães de Pinho ● Neyla Maria de King Freire
Local de guarda: Google Drive		
Objetivo: Estabelecer diretrizes para a conduta adequada no manuseio, controle e proteção das informações, visando evitar a destruição, modificação, divulgação indevida e acessos não autorizados, sejam estes acidentais ou intencionais.		

1. APRESENTAÇÃO

O Instituto de Saúde dos Servidores do Estado do Ceará - ISSEC é uma entidade autárquica, com personalidade jurídica de direito público, autonomia administrativa, técnica, financeira e patrimonial vinculada à Secretaria de Planejamento e Gestão – SEPLAG, regendo-se por Regulamento próprio, pelas normas internas e a legislação pertinente em vigor.

São seus beneficiários :Os servidores públicos civis e militares estaduais,ativos e inativos,e seus respectivos dependentes e pensionistas, dos Poderes Executivo, Legislativo e Judiciário, do Ministério Público Estadual, dos Tribunais de Contas do Estado e dos Municípios, dos Órgãos e Entidades da Administração Pública Estadual Direta, Autárquica e Fundacional.

A estes beneficiários são ofertados os serviços de saúde: médico,hospitalar,odontológico,laboratorial,fonoaudiológico,psicológico,fisioterápico e de assistência às pessoas com deficiência mental e auditiva através de Rede Credenciada, dentro de seu limite orçamentário, observando os atendimentos clínicos e cirúrgicos,o fornecimento de órteses, próteses, materiais especiais, os anexos e as tabelas de materiais, medicamentos e procedimentos, constantes do edital de chamamento público, publicado em jornal de grande circulação e Diário Oficial do Estado.

2. INTRODUÇÃO

A informação é um ativo essencial para os negócios de uma instituição governamental e, como tal, necessita ser adequadamente protegida. Isso é especialmente importante em ambientes corporativos cada vez mais interconectados. Como resultado desse processo de interconexão, a informação está cada vez mais exposta a um grande número de ameaças.

A informação pode existir em diversas formas, seja impressa, escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio pelo qual a informação é compartilhada ou armazenada, é recomendado que esteja sempre protegida adequadamente.

A segurança da informação se baseia em três pilares principais, que sustentam as práticas e políticas de proteção de dados nas organizações, servindo como parâmetros para guiar os processos. Esses pilares são:

Integridade: visa garantir que a informação permaneça livre de alterações não autorizadas, mantendo-se íntegra conforme foi originalmente criada;

Confidencialidade: tem como objetivo assegurar que a informação seja acessada somente por pessoas autorizadas;

Disponibilidade: garante que a informação estará sempre disponível quando necessário para ser acessada.

A segurança da informação, embora possa ser reforçada por meios técnicos, é limitada nessa abordagem e, portanto, deve ser complementada por uma gestão eficaz e por procedimentos adequados.

3. OBJETIVO

Esta Política de Segurança tem como objetivo estabelecer diretrizes e normas gerais para a gestão da Segurança da Informação no Instituto de Saúde dos Servidores do Estado do Ceará – ISSEC. Ela define as responsabilidades e orienta a conduta dos usuários para preservar a integridade, confidencialidade e disponibilidade das informações. Além disso, descreve procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.

4. ABRANGÊNCIA

A Política de Segurança da Informação do ISSEC se aplica a todas as áreas e abrange as instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação da instituição. Ela também se estende às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que atuam no ISSEC ou que tenham acesso a dados ou informações. Cada indivíduo é responsável e estará comprometido com a aplicação desta política.

5. COMPETÊNCIAS E RESPONSABILIDADES

5.1. COMPETÊNCIAS

Os dirigentes e gestores têm as seguintes responsabilidades em relação à Segurança da Informação e Comunicação.

5.1.1. Do Diretor de Planejamento e Gestão

5.1.1.1. Disseminar permanentemente a Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC);

5.1.1.2. Garantir o cumprimento da PoSIC, inclusive disponibilizando recursos necessários para tanto;

5.1.1.3. Aprovar e sancionar, por meio de publicação de portaria interna, o teor da PoSIC e seus normativos;

5.1.1.4. Delegar poderes de supervisão à execução da PoSIC;

5.1.1.5. Promover a elaboração, a atualização, a validação e a divulgação das diretrizes e objetivos estratégicos da PoSIC.

5.1.2. Do Gerente de Tecnologia da Informação

Ao Gerente de Tecnologia da Informação do ISSEC cabem as seguintes responsabilidades:

5.1.2.1. Coordenar as ações para implantação das Políticas de Segurança da Informação no âmbito do ISSEC;

5.1.2.2. Analisar, aprovar, acompanhar e avaliar as principais iniciativas de Segurança da Informação nos ambientes de TIC do ISSEC;

5.1.2.3. Promover a elaboração e implantação de planos de contingência e recuperação de desastres de TIC;

5.1.2.4. Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;

5.1.2.5. Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

5.1.2.6. Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança da informação do ISSEC, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

5.1.2.7. Suspender, a qualquer momento, o acesso de um usuário a recursos computacionais quando houver evidência de riscos à segurança da informação, comunicando à alta gestão e demais interessados;

5.1.2.8. Homologar e autorizar o uso e acesso de ativos, sistemas e dispositivos de processamento de informações em suas instalações;

5.1.2.9. Gerenciar o acesso de usuários e recursos computacionais do órgão/entidade quando um usuário se desligar da instituição, ou a qualquer momento, quando houver evidência de riscos à segurança da informação, e informar ao gestor máximo do órgão/entidade, e ao assessor de controle interno, se existir;

5.1.3. Do Gestor imediato das Áreas ou Setores

Ao Gestor imediato das Áreas ou Setores cabe:

5.1.3.1. Disseminar permanentemente a Política de Segurança da Informação do Issec;

5.1.3.2. Manter os processos sob sua responsabilidade em conformidade com as políticas, normas e procedimentos específicos de segurança da informação do ISSEC, adotando as medidas necessárias para cumprir tal responsabilidade;

5.1.3.3. Solicitar ao departamento de Tecnologia da Informação, por meio dos canais oficiais, a disponibilização ou cancelamento dos recursos computacionais e dos sistemas institucionais para seus subordinados;

5.1.3.4. Comunicar ou notificar o Gestor de Tecnologia da Informação sobre quaisquer indícios, fragilidades ou falhas relacionadas à Segurança da Informação de suas respectivas áreas.

5.2. RESPONSABILIDADE

Os usuários, sejam internos ou externos, devem cumprir e assumir as responsabilidades específicas relacionadas à Segurança da Informação e Comunicação, conforme detalhado a seguir:

5.2.1. Usuários Internos

Aos usuários internos dos recursos de TIC computacionais e sistemas de informação do ISSEC cabem as seguintes responsabilidades:

5.2.1.1. Conhecer e seguir a Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC);

5.2.1.2. Responder por toda atividade executada por meio de sua identificação;

5.2.1.3. Responder por toda violação de segurança praticada por si, sem prejuízo da responsabilização da contratada ou da entidade/órgão ao qual está vinculado;

5.2.1.4. Assinar o Termo de Compromisso, formalizando a ciência e o aceite da Política de Segurança e de suas normas;

5.2.1.5. Comunicar ou notificar à chefia imediata e ao Gestor de Tecnologia da Informação sobre qualquer indício ou falha relacionada à Segurança da Informação.

5.2.2. Usuários Externos

Aos Usuários externos dos Recursos de TIC cabem as seguintes responsabilidades:

5.2.2.1. Cumprir os preceitos estipulados pela Política de Segurança da Informação e Comunicação (PoSIC) quando estiverem executando atividades no ambiente do ISSEC;

5.2.2.2. Comunicar ou notificar à GETIC qualquer indício ou falha na Segurança da Informação, bem como qualquer violação à PoSIC;

5.2.2.3. Responder por toda atividade executada por meio de sua identificação;

5.2.2.4. Responder por toda violação de segurança praticada por si, sem prejuízo da responsabilização da contratada ou da entidade/órgão ao qual está vinculado;

5.2.2.5. Seguir as recomendações e as boas práticas de utilização dos recursos oferecidos pelo ISSEC para a execução de suas atividades;

5.2.2.6. Assinar o Termo de Compromisso, formalizando a ciência e o aceite da Política de Segurança e de suas normas.

6. TERMOS E DEFINIÇÕES

Para os fins desta Política, entende-se por:

6.1. Ameaça: qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio.

6.2. Ativos: qualquer coisa que represente valor para a instituição.

6.3. Ativos de Informação: qualquer informação que tenha valor para a instituição.

6.4. Backup: cópia de dados em meio separado do original, de forma a protegê-los de qualquer eventualidade.

6.5. BYOD (Bring your own device): consiste na utilização de aparelhos próprios dos funcionários no desempenho das atividades empresariais.

6.6. Usuários internos e externos: gestores, comissionados, estagiários, fornecedores, terceirizados ou quaisquer outras pessoas que sejam usuários de equipamentos ou informações.

6.7. Computação em Nuvem: modelo computacional que permite acesso por demanda, independente da localização geográfica, a um conjunto compartilhado de recursos computacionais.

6.8. Confidencialidade: garantia de que a informação é acessível somente por pessoas devidamente autorizadas a ter acesso à mesma.

6.9. Criticidade: importância da informação para a continuidade das operações.

6.10. Custodiante: pessoa ou órgão com atribuição fornecida pelo proprietário da informação de guardar e proteger adequadamente esta informação.

6.11. Integridade: salvaguarda da exatidão, completude da informação e dos métodos de processamento.

6.12. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

6.13. Dispositivos Móveis: equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, incluindo, mas não se limitando a: notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos e cartões de memória.

6.14. Hoax: mensagem de conteúdo alarmista e não verdadeiro (boato).

6.15. Incidente de Segurança: evento não planejado que pode acarretar prejuízos à empresa ou mesmo violar as regras de segurança.

6.16. Informação: conjunto organizado de dados, que constitui uma mensagem.

6.17. Plano de Continuidade de Negócios: procedimentos e informações necessárias para que os órgãos ou entidades mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidente.

6.18. Plano de Gerenciamento de Incidentes: plano de ação definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

6.19. Plano de Recuperação de Desastres: procedimentos e informações necessárias para que o órgão ou entidade operacionalize o retorno das atividades críticas à sua normalidade.

6.20. Política de Privacidade e Proteção de Dados Pessoais: documento que fornece informações sobre como as organizações obtêm, utilizam, armazenam, descartam e protegem os dados pessoais coletados.

6.21. Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

6.22. Redes Sociais: estruturas disponíveis na internet, compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

6.23. Responsável pela Informação: gerador da informação ou seu principal usuário, que define o nível de classificação da informação.

6.24. Usuário: pessoa que acessa ou utiliza de forma legítima e autorizada as informações.

6.25. Terceiros: pessoas que prestam serviços e podem ter acesso às instalações e recursos de informação.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

Para a implementação efetiva das diretrizes apresentadas neste documento, é essencial classificar as informações conforme as seguintes categorias:

7.1. **Pública:** refere-se a qualquer informação que pode ser acessada por usuários da instituição, sejam clientes, fornecedores, prestadores de serviço e o público em geral, sem qualquer restrição;

7.2. **Interna:** essa categoria inclui todas as informações que só podem ser acessadas pelos colaboradores do ISSEC. Essas, caracterizam-se por possuírem um certo grau de confidencialidade e que podem comprometer o negócio da instituição se forem divulgadas;

7.3. **Confidencial:** trata-se de categoria que abrange todas as informações cujo conhecimento e divulgação por pessoas não autorizadas, podem ser prejudiciais aos interesses da instituição.;

7.4. **Secreta:** é uma categoria especial de informações, que só podem ser acessadas por usuários da instituição que foram explicitamente autorizados, seja por nome ou pela área a que pertencem. A divulgação não autorizada dessas informações pode causar sérios danos ao negócio ou comprometer a estratégia de negócio da instituição.

Não é permitido o uso da internet para fornecer ou divulgar informações do ISSEC que sejam classificadas como internas, confidenciais ou secretas.

Todos os gestores têm o dever de orientar seus subordinados a não circularem informações ou mídias consideradas confidenciais ou secretas. Isso inclui não deixar relatórios nas impressoras e mídias em locais de fácil acesso.

É responsabilidade dos gestores de cada área estabelecer critérios relativos ao nível de confidencialidade da informação gerada por sua área, de acordo com sua classificação (pública, interna, confidencial ou secreta).

Leis de Acesso à Informação: É necessário obedecer aos critérios de classificação das informações quando do atendimento da Lei de Acesso à Informação (Lei 12.527/11) e da Lei Estadual nº 15.175/12, que regulamenta a Lei de Acesso à Informação no âmbito do Estado do Ceará.

8. PRINCÍPIOS E DIRETRIZES

Os princípios e diretrizes que orientam essa Política, estão descritos no Artigo 2º, Seção 1º, do Decreto nº 34.100, datado de 09 de junho de 2021, conforme segue:

Artigo 1º - implementação da PoSIC: A Política de Segurança da Informação e Comunicação (PoSIC) é uma estratégia crucial que deve ser implementada pelos órgãos e entidades do Poder Executivo do Estado do Ceará. Esta política orienta as ações de segurança da informação e comunicação, garantindo a proteção e integridade dos dados. A implementação é baseada nos seguintes princípios:

I - Alinhamento Estratégico: princípio que enfatiza a importância do alinhamento entre os órgãos e entidades estaduais e as diretrizes de segurança da informação. O objetivo é garantir que todas as ações e procedimentos estejam em conformidade com a missão institucional e o planejamento estratégico. Isso inclui a alocação de orçamentos para a implantação de controles de segurança da informação e a capacitação de pessoal;

II - Diversidade Organizacional: reconhece a diversidade das atividades das instituições e respeita a natureza e finalidade de cada órgão/entidade. As diretrizes e controles de Segurança Corporativa do Estado são elaborados levando em consideração essa diversidade, garantindo a continuidade dos negócios;

III - Garantia da Segurança das Informações: esse princípio destaca a necessidade de implementar e utilizar controles que garantam a confidencialidade, disponibilidade e integridade das informações. Isso inclui a classificação do grau de confidencialidade e

criticidade das informações, bem como a definição de políticas para acesso e manuseio das mesmas;

IV - Propriedade da Informação: afirma que todas as informações produzidas ou armazenadas no Estado são de propriedade do Estado e não de seus colaboradores. O uso dessas informações deve ser destinado exclusivamente a atender aos interesses da Instituição;

V - Alinhamento com os Aspectos Legais (Compliance): princípio que enfatiza a importância de cumprir as normas legais e regulamentares de abrangência estadual e federal, as políticas e as diretrizes estabelecidas para o negócio e para as atividades do estado. Além disso, é necessário evitar, detectar e tratar qualquer desvio ou inconformidade que possa ocorrer.

9. DIRETRIZES REFERENTES ÀS NORMAS E AOS PROCEDIMENTOS

As Normas e Procedimentos são documentos cruciais que delineiam o plano tático e operacional de uma instituição. Eles especificam os controles que devem ser implementados e detalham os procedimentos necessários para garantir a conformidade e eficiência operacional. Esses documentos são projetados para serem claros e compreensíveis, assegurando que todos os colaboradores possam segui-los sem ambiguidades.

Devido à complexidade e às características específicas de cada setor, as Normas e Procedimentos são frequentemente segmentados em Anexos. Isso permite uma organização mais clara e facilita a atualização de partes específicas sem a necessidade de revisar o documento inteiro. No documento principal, são estabelecidas as diretrizes gerais, que servem como um guia abrangente para a governança organizacional.

No caso de uma situação não estar explicitamente coberta por uma norma ou procedimento específico, prevalece o que está estipulado no corpo principal do documento. Isso garante que haja sempre um ponto de referência claro, mesmo quando circunstâncias inesperadas ou excepcionais surgirem, assegurando a continuidade e a integridade dos processos organizacionais. É importante que esta cláusula seja bem comunicada a todos os colaboradores, para que haja entendimento unificado em casos de lacunas nos Anexos.

9.1. **DA ABRANGÊNCIA:**

9.1.1. Todos os departamentos do ISSEC, que fazem uso do serviço de rede de comunicação e sistemas, estão obrigatoriamente sujeitos às diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações (PoSIC).

9.2. **DA CONSCIENTIZAÇÃO**:

9.2.1. É imperativo que exista um programa eficaz de disseminação dessa Política, garantindo que todos os membros da instituição estejam plenamente cientes da obrigatoriedade e da necessidade de obediência às normas e recomendações estabelecidas;

9.2.2. É essencial a implementação de um programa de conscientização robusto sobre Segurança da Informação. Este programa deve garantir que todos os membros estejam informados sobre os potenciais riscos de segurança aos quais os ambientes computacionais estão expostos, promovendo assim, uma maior cooperação para o cumprimento das normas desta Política;

9.2.3. É importante ressaltar que todo o pessoal, que integre direta ou indiretamente os recursos humanos do ISSEC, é responsável pela Segurança da Informação, dentro de sua respectiva área de atuação. Esta responsabilidade é fundamental para a manutenção da integridade e segurança das informações da instituição.

9.3. **DO CONTROLE DE ACESSO:**

9.3.1. É imperativo que existam procedimentos específicos, devidamente documentados e implementados, para o bloqueio temporário ou definitivo de acesso aos recursos computacionais do ISSEC no caso de afastamento ou desligamento de usuários credenciados;

9.3.2. A identificação do usuário é pessoal e intransferível, tornando-o responsável pelas atividades desenvolvidas através dela. Para a liberação do acesso, é necessário que o usuário assine um “Termo de Responsabilidade” que ateste sua compreensão das condições de uso, bem como seus direitos e deveres em relação ao acesso aos recursos computacionais do ISSEC;

9.3.3. Todos os usuários, sejam eles internos ou externos, devem ter acesso liberado apenas aos recursos que são necessários para a execução de suas tarefas no

ambiente do ISSEC. Esta medida visa garantir a segurança e a eficiência do uso dos recursos computacionais.

9.4. **DO USO E ACESSO À INTERNET E RECURSOS COMPUTACIONAIS:**

9.4.1. Apenas atividades que são lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários em geral ao utilizar os recursos computacionais do ISSEC. Qualquer transgressão a esta norma sujeitará o infrator às sanções previstas nesta Política;

9.4.2. O uso de recursos computacionais próprios, dentro do âmbito do ISSEC, será permitido somente mediante autorização prévia do gestor da área ou superior. Além disso, tal uso somente será liberado após uma verificação cuidadosa para garantir a conformidade com as normas de segurança estabelecidas nesta Política.

9.5. **DA PROPRIEDADE INTELECTUAL**:

9.5.1. As informações que são propriedade do ISSEC, devem ser utilizadas exclusivamente para os propósitos aos quais foram destinados. Sob nenhuma circunstância, essas informações podem ser apropriadas por usuários internos ou externos.

9.6. **DO TRATAMENTO DAS INFORMAÇÕES:**

9.6.1. É imperativo que todas as informações sejam protegidas contra perda, acessos e usos indevidos. Para isso, devem ser adotados procedimentos específicos e adequados, correspondentes ao grau de criticidade da informação. A responsabilidade direta pela proteção dessas informações recai sobre o colaborador que as detém em sua guarda.

9.7. **DA GESTÃO DE RISCOS:**

9.7.1. Os recursos de processamento da informação disponibilizados devem ser suportados de maneira a prevenir situações de risco à segurança da informação. Estes recursos devem ser homologados em um ambiente de teste e desenvolvimento antes de serem implementados em um ambiente de produção;

9.7.2. Esta Política de Segurança da Informação deve ser considerada como um recurso fundamental para o processo de aquisição de bens e serviços de Tecnologia da Informação e Comunicação (TIC);

9.7.3. É recomendável que seja implementado um programa de Gerenciamento de Riscos para a análise do ambiente computacional do ISSEC como um todo. O

objetivo deste programa é identificar e remediar as vulnerabilidades que resultam em riscos para a segurança da informação.

9.8. **DO MONITORAMENTO E AUDITORIA:**

9.8.1. A aderência à Política de Segurança da Informação será monitorada e auditada sempre que se fizer necessário, garantindo a sua efetiva implementação e manutenção;

9.8.2. A conformidade com a Política de Segurança será documentada em um relatório de avaliação de conformidade. Este relatório, que serve como um registro formal da aderência às normas estabelecidas, será encaminhado ao Dirigente Superior da Instituição para revisão e aprovação.

9.9. **DA GESTÃO DE INCIDENTES:**

9.9.1. Todos os usuários, ao tomarem conhecimento de qualquer incidente de Segurança da Informação, têm a obrigação de notificar imediatamente o ocorrido à Gerência de Tecnologia da Informação (GETIC). Esta medida é crucial para que as providências cabíveis sejam tomadas de maneira tempestiva;

9.9.2. É recomendável que seja estabelecido um plano de Resposta a Incidentes. O objetivo deste plano é conter e remediar qualquer incidente de segurança da informação que possa ocorrer, garantindo assim a continuidade das operações e a integridade das informações.

9.10. **DA GESTÃO DE CONTINUIDADE:**

9.10.1. É recomendável que seja implementado um Plano de Continuidade do Negócio. Este plano deve ser testado periodicamente para assegurar a continuidade dos serviços críticos nos ambientes computacionais. Esta medida é crucial para garantir a resiliência e a eficácia operacional da instituição..

9.11. **DAS NORMAS E RECOMENDAÇÕES:**

Os aspectos de segurança física, lógica e de pessoal serão abordados em documentos independentes, considerando suas peculiaridades. Estes serão apresentados na forma de Anexos, com o objetivo de complementar, com maior detalhamento, as normas e recomendações de segurança no manuseio das informações:

I. NR01 - Controle de Acesso;

II. NR02 - Uso de Senhas;

III. NR03 - Gestão de Ativos;
IV. NR04 - Backup e Restauração de Dados;
V. NR05 - Uso de Softwares;
VI. NR06 - Uso da Internet;
VII. NR07 - Uso do Correio Eletrônico;
VIII. NR08 - Combate a Softwares Maliciosos;
IX. NR09 - Uso de Dispositivos Móveis;
X. NR10 - Acesso Remoto;
XI. NR11 - Descarte de Mídias;
XII. NR12 - Aquisição, Desenvolvimento e Manutenção de Sistemas.
XIII. NR13 - Controle de Respostas a Incidentes.

10. DADOS PESSOAIS

O ISSEC, em todas as posições que assumir, declara prontamente o seu compromisso inabalável com o cumprimento das regras aplicáveis de privacidade e proteção de dados pessoais. Reitera-se o compromisso, conforme previsto no Planejamento Estratégico da Autarquia, de instituir um Plano de Atendimento à Lei Geral de Proteção de Dados (LGPD). Este plano deverá ser elaborado pelo Comitê Estratégico de Proteção de Dados Pessoais, conforme estabelecido na Portaria nº 139/2022.

11. DIVULGAÇÃO E ACESSO À INSTRUÇÃO NORMATIVA

Os documentos que compõem a estrutura normativa de gestão de segurança da informação, devem ser divulgados a todos os servidores, colaboradores, estagiários, aprendizes e prestadores de serviços do ISSEC no momento de sua admissão. Além disso, esses documentos devem ser publicados na Intranet corporativa, de forma que seu conteúdo possa ser consultado a qualquer momento.

12. CASOS OMISSOS

Quaisquer casos omissos, não contemplados nesta Política e em seus documentos complementares, devem ser submetidos à Gerência de Tecnologia da Informação. Esta

Gerência avaliará a necessidade de encaminhar tais casos à Diretoria Superior para uma deliberação apropriada.

13. SANÇÕES

13.1. Em situações de violação ou não cumprimento desta política, poderá ser instaurada uma sindicância para a averiguação dos fatos, quando houver indícios de ocorrência de infração, sem prejuízo da responsabilização penal, administrativa e civil do suposto infrator, respeitando os princípios da ampla defesa e do contraditório;

13.2. No caso dos servidores, comissionados e estagiários, a violação desta política poderá resultar na aplicação de medidas disciplinares, como advertência, suspensão ou desligamento formal, conforme a legislação aplicável;

13.3. Para os usuários que mantêm contrato com o ISSEC, a violação ou não cumprimento desta política poderá resultar em suspensão, rescisão contratual e aplicação de multa à parte contratada, sem prejuízo da responsabilização pessoal do infrator pelos atos praticados ou para os quais tenham contribuído ou facilitado;

13.4. Para fins de aplicação das sanções e punições, será considerada a gravidade da infração, o impacto causado e a frequência de ocorrência;

13.5. Em casos de violações que envolvam atividades ilegais capazes de causar danos à instituição, o infrator será responsabilizado pelos prejuízos nas esferas cível, penal e administrativa.

14. REVISÃO

14.1. Esta política entra em vigor a partir da data de sua publicação e deverá ser revisada em um intervalo mínimo de dois anos, podendo ser modificada ou ajustada sempre que se fizer necessário. Em todas as circunstâncias, prevalecerá o documento mais recentemente publicado.

15. DISPOSIÇÕES FINAIS

15.1. Para assegurar a uniformidade da informação organizacional, esta Política de Segurança da Informação e Comunicação (PoSIC) deve ser comunicada a

todos os gestores, colaboradores e prestadores de serviço do ISSEC. O objetivo é garantir que a política seja cumprida tanto dentro quanto fora da instituição.

16. REFERÊNCIAS LEGAIS E NORMATIVAS

Esta Política é fundamentada nas seguintes referências legais e normativas:

I. Decreto Federal nº 9.637, de 26 de dezembro de 2018, que dispõe sobre a governança da segurança da informação;
II. Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD);
III. Lei Federal nº 12.965, de 23 de abril de 2014;
IV. Lei Federal nº 12.527, de 18 de novembro de 2011;
V. Lei Estadual nº 15.175, de 28 de junho de 2012;
VI. NBR/ISO/IEC 27001:2006 - Segurança da Informação;
VII. NBR/ISO/IEC 27002:2013 - Segurança da Informação;
VIII. NBR/ISO/IEC 27005:2008 - Tecnologia da Informação.