POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DA PROCURADORIA-GERAL DO ESTADO DO CEARÁ

CEARÁ
GOVERNO DO ESTADO
PROCURADORIA-GERAL DO ESTADO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DA PROCURADORIA-GERAL DO ESTADO DO CEARÁ

OUTUBRO/2022

CEARÁ
GOVERNO DO ESTADO
PROCURADORIA-GERAL DO ESTADO

PROCURADORIA-GERAL DO ESTADO DO CEARÁ

Procuradora-Geral do Estado do Ceará
Antônia Camily Gomes Cruz

Procurador-Geral Executivo de Contencioso Geral e Administrativo
João Renato Banhos Cordeiro

Procurador-Geral Executiva de Consultoria e Contencioso Tributário
Gerardo Rodrigues de Albuquerque Filho

Procurador-Geral Executivo Assistente
Rafael Machado de Moraes

Equipe de Elaboração
Dieric Guimarães Cavalcante
Kelly Gonçalves Meira Arruda
Renato Monteiro Lima
Syene Rodrigues de Lima Belo Fonseca
Edilson de Oliveira Carneiro - Apoio Técnico

Equipe de Revisão
Adolfo Ciríaco Cunha
Lorena de Sousa Damascena
Giacomina Maria Amélia Borrini de Freitas

Política de Segurança da Informação e Comunicação.		
Elaboração: 05/10/2022	Revisão: 21/10/2022	Aprovação: 24/11/2022
Equipe de elaboração: Dieric Guimarães Cavalcante Kelly Gonçalves Meira Arruda Renato Monteiro Lima Syene Rodrigues de Lima Belo Fonseca Edilson de Oliveira Carneiro	**Equipe de revisão:** Adolfo Ciríaco Cunha Lorena de Sousa Damascena Giacomina Maria Amélia Borrini de Freitas	**Aprovado por:** Antônia Camily Gomes Cruz Giacomina Maria Amélia Borrini de Freitas
Local de guarda: Intranet / File Server / GED		
Objetivo: Instituir as diretrizes para a conduta adequada no manuseio, controle e proteção das informações contra a destruição, modificação, divulgação indevida e acessos não autorizados, sejam estas acidentais ou intencionais.		

CONTROLE DE REVISÕES

Revisão	Data	Responsável	Alteração principal
00	21/10/2022	Coordenadoria de TI	Elaboração inicial

LISTA DE ABREVIATURAS, ACRÔNIMOS E SIGLA

ABNT/NBR	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
CD	Compact Disc (Disco Compacto)
CTI	Coordenadoria de Tecnologia da Informação
DNS	Domain Name System (Sistema de Nomes de Domínio)
DVD	Digital Versatile Disc (Disco Digital Versátil)
HD	Hard Disc (Disco Rígido)
IDS	Intrusion Detection System (Sistema de Detecção de Intrusão)
IPS	Intrusion Prevention System (Sistema de Prevenção de Intrusão)
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
MTP	Media Transfer Protocol (Protocolo de Transferência de Mídia)
PGE-CE	Procuradoria-Geral do Estado do Ceará
PoSIC	Política de Segurança da Informação e Comunicação
SIEM	Security Information and Event Management (Gerenciamento e Correlação de Eventos de Segurança)
SLA	Service Level Agreement (Acordo de Nível de Serviço)
SSD	Solid State Drive (Drive de Estado Sólido)
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network (Rede Virtual Privada)

SUMÁRIO

APRESENTAÇÃO

A Procuradoria Geral do Estado do Ceará (PGE-CE) tem na informação um ativo essencial para o alcance da sua missão e objetivos estratégicos, e consequentemente, que necessita ser adequadamente protegida. Assim, a PGE-CE, por meio desta POLÍTICA, declara formalmente seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda.

A Política de Segurança da Informação e Comunicação (PoSIC) é o documento que orienta e define as diretrizes corporativas para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários, devendo ser lida, entendida, seguida e cumprida por todas as áreas e níveis hierárquicos da instituição.

Esta Política tem por objetivo nortear a implementação de medidas de proteção que deverão ser aplicadas a toda e qualquer informação, independentemente de onde ela se encontre, com vistas ao resguardo da imagem e dos objetivos institucionais desta Procuradoria-Geral.

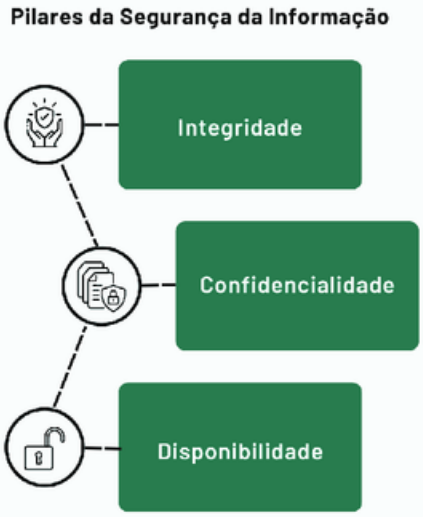
A PoSIC está baseada nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013, reconhecida como um código de práticas para a Gestão da Segurança da Informação, e também está de acordo com as leis vigentes no país, além de atender à orientação do Governo do Estado em aplicar Políticas de Segurança da Informação no Estado, com base no DECRETO Nº 34.100 de 09 de junho de 2021.

INTRODUÇÃO

A informação é um ativo essencial para os negócios de uma instituição e como tal necessita ser adequadamente protegida. Isto 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. Pode ser 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 através do 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. São eles:



Integridade: busca garantir que a informação esteja livre de qualquer alteração não autorizada, mantendo-se íntegra, conforme foi criada.

Confidencialidade: busca garantir que a informação seja acessada apenas por pessoas autorizadas.

Disponibilidade: garantia de que a informação estará disponível sempre que necessário ser acessada.

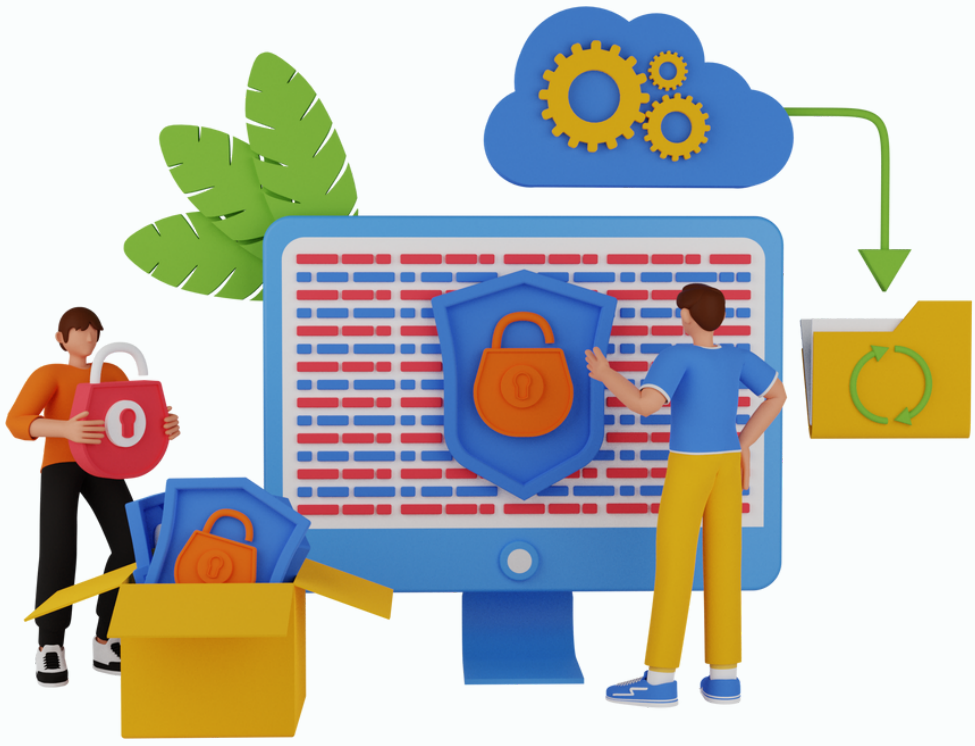
A Segurança da Informação que pode ser alcançada por meios técnicos é limitada, e por isso deve ser apoiada por uma gestão e por procedimentos apropriados.

OBJETIVO

O objetivo desta Política de Segurança é estabelecer diretrizes e normas gerais para a gestão da Segurança da Informação dos ambientes desta Procuradoria-Geral do Estado do Ceará - PGE, definindo as responsabilidades e orientando a conduta dos usuários de maneira a preservar a integridade, confidencialidade e disponibilidade das informações, descrevendo procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.

ABRANGÊNCIA

A Política de Segurança da Informação deverá ser seguida por todas as áreas, e aplicadas às instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação existentes na PGE-CE, como também às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito da PGE-CE ou a quem quer que venha a ter acesso a dados ou informações, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.



5. COMPETÊNCIAS E RESPONSABILIDADES

5.1. COMPETÊNCIAS

Aos dirigentes e gestores, cabem as seguintes competências, relacionadas à Segurança da Informação e Comunicação.

5.1.1. Dirigente Superior da PGE-CE

Ao Dirigente Superior da PGE-CE cabem as seguintes competências:

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. Coordenador de Tecnologia da Informação

Ao Coordenador de Tecnologia da Informação da PGE Ceará cabem as seguintes responsabilidades:

5.1.2.1. Coordenar as ações para implantação das Políticas de Segurança da Informação no âmbito da PGE-CE;
5.1.2.2. Analisar, aprovar, acompanhar e avaliar as principais iniciativas de Segurança da Informação nos ambientes de TIC da PGE-CE;
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 da PGE-CE, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

5.1.2.7. Suspender, a qualquer tempo, o acesso de usuário a recurso computacional quando evidenciado riscos à segurança da informação, informando a 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. Realizar a gestão do acesso do usuário e recurso computacional do órgão/entidade do usuário que se desligar da instituição, ou a qualquer tempo, quando evidenciados riscos à segurança da informação, e informar ao gestor máximo do órgão/entidade, além do gestor de segurança da informação e do assessor de controle interno, se existir;

5.1.2.10. Deliberar sobre as questões que lhe tenham sido encaminhadas.

5.1.3. Gestor Imediato das Áreas e/ou Setores

Cabe ao Gestor imediato das Áreas e/ou Setores:

5.1.3.1. Disseminar permanentemente a Política de Segurança da Informação;

5.1.3.2. Manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação da PGE-CE, tomando as ações necessárias para cumprir tal responsabilidade;

5.1.3.3. Solicitar ao departamento de Tecnologia da Informação, pelos meios oficiais e instituídos, a disponibilidade ou cancelamento dos recursos computacionais e dos sistemas institucionais disponibilizados para os seus subordinados.Solicitar ao departamento de Tecnologia da Informação, pelos meios oficiais e instituídos, a disponibilidade ou cancelamento dos recursos computacionais e dos sistemas institucionais disponibilizados para os seus subordinados.

5.1.3.4. Comunicar e/ou Notificar ao Gestor de Tecnologia da Informação sobre quaisquer indícios, fragilidades ou falhas relacionadas à Segurança da Informação de suas respectivas áreas.

5.2. RESPONSABILIDADES

São deveres dos usuários, sejam eles internos ou externos, cabendo cumprir e assumir as responsabilidades específicas, relacionadas à Segurança da Informação e Comunicação, conforme segue.

5.2.1. Usuários Internos

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

5.2.2.1. Conhecer e seguir a Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC);
5.2.2.2. Responder por toda atividade executada por meio de sua identificação;
5.2.2.3. Responder por toda violação de segurança praticada por si, sem prejuízo da responsabilização da contratada ou de entidade/órgão ao qual está vinculado;
5.2.2.4. Assinar o Termo de Compromisso, formalizando a ciência e o aceite da Política de Segurança e de suas normas;
5.2.2.5. Comunicar e/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 por esta PoSIC, quando estiverem executando atividades no ambiente da PGE-CE;
5.2.2.2. Comunicar e/ou notificar à CTI indício ou falha na Segurança da Informação, bem como qualquer violação a esta 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 de entidade/órgão

ao qual está vinculado;

5.2.2.5. Seguir as recomendações e as boas práticas de utilização dos recursos ofertados pela PGE-CE 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 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 e/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, completeza 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, entre os quais se incluem, não se limitando a estes: 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. Quem 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 possuir acesso às instalações e recursos de informação.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

Para fins de adoção das diretrizes deste documento, a informação classifica-se em:

7.1 **Pública:** é toda informação que pode ser acessada por usuários da instituição, clientes, fornecedores, prestadores de serviço e público em geral, sem restrição.

7.2 **Interna:** é toda informação que só pode ser acessada por colaboradores da PGE Ceará. São informações que já possuem um certo grau de confidencialidade e que pode comprometer o negócio da instituição se divulgada.

7.3 **Confidencial:** é toda informação cujo conhecimento e divulgação, por pessoa não autorizada, possa ser prejudicial ao interesse da instituição;

7.4 **Secreta:** é toda informação que pode ser acessada somente por usuários da instituição explicitamente autorizados, através da indicação feita pelo nome ou por área a que pertence. A divulgação não autorizada desta informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da instituição.

Não é permitido o uso da internet para o fornecimento ou divulgação de informações da PGE-CE que sejam classificadas como interna, confidencial ou secreta.

Cabe a todos os gestores o dever de orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou secretas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso.

É também de 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), além de ser necessária a obediência 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 norteiam esta PoSIC estão descritos no Art. 2º, § 1º, do decreto nº 34.100, de 09 de junho de 2021, conforme segue.

> § 1º A PoSIC deve ser implementada de forma a orientar estrategicamente as ações de segurança da informação e comunicação a serem executadas pelos órgãos e entidades do Poder Executivo do Estado do Ceará, tendo por base os seguintes princípios:
>
> I - Alinhamento estratégico: Os órgãos e entidades estaduais deverão alinhar-se com os princípios, diretrizes, normas, procedimentos e ações de segurança da informação, observando sua missão institucional e o planejamento estratégico, com vistas a viabilizar orçamentos necessários para garantir a implantação mínima e continuada de níveis de controle de segurança da informação, por meio de ações e projetos, de forma a dotar-se de recursos tecnológicos, processos e pessoal qualificado para o devido cumprimento da política de que trata a PoSIC.
>
> II - Diversidade organizacional: A elaboração de diretrizes, normas, procedimentos e controles de Segurança Corporativa do Estado deve levar em consideração a diversidade das atividades das instituições, respeitando a natureza e finalidade de cada órgão/entidade, de forma a garantir a continuidade do seu negócio.
>
> III - Garantia da Segurança das Informações: Deve-se sempre buscar a implantação e utilização de controles que busquem garantir a confidencialidade, disponibilidade e integridade das informações nos órgãos/entidades. Estes controles devem incluir a classificação do grau de confidencialidade, disponibilidade e criticidade, bem como uma política para acesso e manuseio das mesmas.

IV - Propriedade da informação: Toda informação produzida ou armazenada no Estado é de sua propriedade e não de seus colaboradores, exceto os casos onde a Instituição atua como custodiante da informação, devendo seu uso ser destinado, exclusivamente, a atender aos interesses da Instituição.

V - Alinhamento com os aspectos legais ("Compliance"): Devem ser cumpridas 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, bem como evitar, detectar e tratar qualquer desvio ou inconformidade que possa ocorrer.

9. DIRETRIZES REFERENTES ÀS NORMAS E AOS PROCEDIMENTOS

As Normas e Procedimentos especificam o plano tático e operacional e detalham como deverão ser implementados os controles especificados, tornando claros e compreensíveis os detalhes que devem ser seguidos pelos colaboradores.

Devido a sua extensão e particularidades, as Normas e Procedimentos serão definidas em Anexos, ficando neste documento as diretrizes gerais.

Em caso da não existência de uma norma ou procedimento específico para algum item desta política, fica definido como válido o que for declarado no corpo deste documento.

Diretrizes Gerais:

9.1. DA ABRANGÊNCIA:

9.1.1. Estão submetidos às normas desta PoSIC todos os departamentos da PGE-CE que utilizam o serviço de rede de comunicação e sistemas;

9.2. DA CONSCIENTIZAÇÃO:

9.2.1. Deve existir um programa de disseminação desta Política, assegurando que todos que integram a instituição estejam cientes da obrigatoriedade e obediência às normas e recomendações definidas;

9.2.2. Deve ser implementado um programa de conscientização sobre Segurança da Informação de forma que todos sejam informados sobre os potenciais riscos de segurança a que estão expostos os ambientes computacionais, proporcionando assim, maior cooperação para o cumprimento das normas desta Política;

9.2.3. Todo pessoal que integre direta ou indiretamente os recursos humanos da PGE é responsável pela Segurança da Informação, dentro de sua respectiva área de atuação;

9.3. DO CONTROLE DE ACESSO:

9.3.1. Devem existir, documentados e implementados, procedimentos específicos para bloqueio temporário ou definitivo de acesso aos recursos computacionais da PGE quando do 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, sendo necessário para a liberação, a assinatura de um "Termo de Responsabilidade" que comprove sua ciência às condições de uso, seus direitos e deveres quanto ao acesso aos recursos computacionais da PGE-CE;

9.3.3. Todos os usuários, internos e externos, devem ter acesso liberado apenas aos recursos necessários à execução de suas tarefas no ambiente da PGE-CE;

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

9.4.1. Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários em geral, quando da utilização dos recursos computacionais da PGE, ficando os transgressores sujeitos às sanções previstas nesta Política;

9.4.2. O uso de recursos computacionais próprios no âmbito da PGE estará liberado, apenas, mediante autorização prévia do gestor da área ou superior, e somente após verificação quanto à conformidade com as normas de segurança desta Política;

9.5. DA PROPRIEDADE INTELECTUAL:

9.5.1. As informações de propriedade da PGE-CE devem ser de uso restrito para os fins a que se destinam, não podendo, de forma alguma, serem apropriadas por usuários internos ou externos;

9.6. DO TRATAMENTO DAS INFORMAÇÕES

9.6.1. Todas as informações devem ser protegidas contra perda, acessos e usos indevidos, devendo ser adotados procedimentos específicos e adequados ao grau de criticidade da informação, sob a responsabilidade direta do colaborador que a detém em sua guarda;

9.7. DA GESTÃO DE RISCOS:

9.7.1. Os recursos de processamento da informação disponibilizados devem ser suportados de forma a evitar situações de risco à segurança da informação, devendo ser homologados em ambiente de teste e desenvolvimento antes de serem postos em produção;

9.7.2. Esta Política de Segurança da Informação deve ser considerada como subsídio para o processo de aquisição de bens e serviços de Tecnologia da Informação e Comunicação - TIC;

9.7.3. Deve ser implementado um programa de Gerenciamento de Riscos para análise do ambiente computacional da PGE-CE como um todo, com objetivo de identificar e remediar as vulnerabilidades que resultam em riscos para a segurança da informação;

9.8. DO MONITORAMENTO E AUDITORIA:

9.8.1. O cumprimento da Política de Segurança da Informação será acompanhado e auditado sempre que necessário;

9.8.2. A verificação de conformidade da Política de Segurança será documentada em relatório de avaliação de conformidade, o qual será encaminhado ao Dirigente Superior da Instituição.

9.9. DA GESTÃO DE INCIDENTES:

9.9.1. Todos os usuários ao tomarem conhecimento de qualquer incidente de Segurança da Informação devem notificar o fato imediatamente à Coordenadoria de Tecnologia da Informação - CTI para que sejam tomadas as providências cabíveis;

9.9.2. Deve ser estabelecido um plano de Resposta a Incidentes com o objetivo de conter e remediar qualquer incidente de segurança da informação que venha a ocorrer;

9.10. DA GESTÃO DE CONTINUIDADE:

9.10.1. Deve ser implementado um Plano de Continuidade do Negócio e este deve ser testado periodicamente para garantir a continuidade dos serviços críticos nos ambientes computacionais;

9.11. DAS NORMAS E RECOMENDAÇÕES:

9.11.1. Os aspectos de segurança física, lógica e de pessoal serão tratados em documentos independentes, tendo em vista suas peculiaridades, na forma de Anexos, a fim de complementar com maior detalhamento, as normas e recomendações de segurança no trato 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 Resposta a Incidentes;

10. DADOS PESSOAIS

A PGE-CE, em todas as posições que ocupar, desde pronto, declara o seu compromisso com o cumprimento das regras de privacidade e proteção de dados pessoais aplicáveis. Reafirma-se o compromisso previsto no Planejamento Estratégico da Instituição no sentido de instituir um Plano para atendimento à LGPD, o qual será elaborado pelo Comitê Estratégico de Proteção de Dados Pessoais previsto na Portaria nº 139/2022.

11. DIVULGAÇÃO E ACESSO À INSTRUÇÃO NORMATIVA

Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados a todos os servidores, colaboradores, estagiários, aprendizes e prestadores de serviços da PGE quando de sua admissão, e também publicadas na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

12. CASOS OMISSOS

Os casos omissos, não previstos nesta Política e seus documentos complementares, deverão ser submetidos à Coordenação de Tecnologia da Informação, que avaliará a necessidade de encaminhar à Diretoria Superior para deliberação.

13. SANÇÕES

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

13.2. No caso dos servidores, comissionados e estagiários, poderá acarretar na aplicação de advertência, suspensão ou desligamento formal na forma da legislação aplicada;

13.3. No caso de usuários que mantenham contrato com a PGE-CE, a violação ou não cumprimento dessa política poderá resultar em suspensão, rescisão contratual e aplicação de multa à contratada, sem prejuízo de responsabilização pessoal do infrator pelos atos praticados ou para os quais tenha participado ou facilitado.

13.4. Para fins de aplicação das sanções e das punições, será considerada a gravidade da infração, o efeito alcançado e a sua recorrência;

13.5. Em caso de violações que impliquem em atividades ilegais que possam provocar danos à instituição, o infrator será responsabilizado pelos prejuízos na esfera cível, penal e administrativa.

14. REVISÃO

A presente política passa a vigorar a partir da data de sua publicação, devendo ser revisada em um período mínimo de 2 (dois) anos, podendo ser editada ou ajustada sempre que houver a necessidade, valendo sempre o documento mais recentemente publicado.

15. DISPOSIÇÕES FINAIS

15.1. Para a uniformização da informação organizacional, esta PoSIC deverá ser comunicada a todos os gestores, colaboradores e prestadores de serviço da PGE-CE, a fim de que seja cumprida dentro e fora da instituição.

16. REFERÊNCIAS LEGAIS E NORMATIVAS

16.1. A presente Política tem como fundamentos as seguintes referências legais e normativas:

I. Decreto Federal nº 9.637 de 26 de dezembro de 2018 Segurança da Informação, dispõe sobre a governança da segurança da informação;
II. Lei Federal nº 13.709, de 14 de agosto de 2018 (LGPD);
III. Lei Federal nº 12.965, de 23 de abril de 2014;
IV. Lei Federal nº 12.527, de 18 de novembro de 201 1;
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;

CEARÁ

GOVERNO DO ESTADO

PROCURADORIA-GERAL DO ESTADO