1. **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - POSIN**

Data: 16/07/2021

Versão 1.0

* 1. **HISTÓRICO DE ALTERAÇÕES**

| **DOCUMENTO** |
| --- |
| **Descrição** | Este é o documento chave da Política de Segurança da Informação - POSIN |
| **Objetivo** | * Tornar a segurança da informação como um dos elementos fundamentais no planejamento estratégico da Secretaria de Estado da Administração;
* Definir os padrões mínimos obrigatórios para o devido uso e proteção das informações criadas, recebidas, armazenadas, processadas, transmitidas ou impressas na Secretaria de Estado da Administração;
* Estabelecer as competências e atribuições dos atores envolvidos nesta política;
* Elencar os processos necessários para atingir um padrão aceitável de Segurança da Informação, conforme as legislações existentes e os padrões que o mercado estabelece;
* Difundir os aspectos relacionados à Segurança da Informação na Secretaria de Estado da Administração.
 |
| **Responsável** | **Equipe** | **Criado em** |
| GESIN – DITI | 16/07/2021 |
| **Setor** | Gerência de Infraestrutura e Segurança da Informação - GESIN |

**SUMÁRIO**

[​ POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - POSIN 1](#_heading=h.gjdgxs)

[​ HISTÓRICO DE ALTERAÇÕES 2](#_heading=h.30j0zll)

[​ 1 – APRESENTAÇÃO 3](#_heading=h.1fob9te)

[​ 2 – DOS OBJETIVOS 3](#_heading=h.3znysh7)

[​ 3 – DECLARAÇÃO DE COMPROMETIMENTO DA ALTA GESTÃO 4](#_heading=h.2et92p0)

[​ 4 – ABRANGÊNCIA E DIVULGAÇÃO 4](#_heading=h.tyjcwt)

[​ 5 – DOCUMENTOS QUE COMPÕEM A POSIN 4](#_heading=h.3dy6vkm)

[​ 5.1 – COMITÊ DE SEGURANÇA DA INFORMAÇÃO: 4](#_heading=h.1t3h5sf)

[5.2 – PLANO DE CONTINUIDADE DE NEGÓCIO (PCN): 5](#_heading=h.4d34og8)

[​ 5.3 – PLANO DE GESTÃO DE ATIVOS DE INFORMAÇÃO: 5](#_heading=h.2s8eyo1)

[5.4 – PLANO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO: 5](#_heading=h.17dp8vu)

[5.5 – PLANO DE SEGURANÇA PARA FORNECEDORES: 5](#_heading=h.3rdcrjn)

[5.6 – PLANO DE CONTROLE DE ACESSO À INFORMAÇÃO: 5](#_heading=h.26in1rg)

[5.7 – PLANO DE CONSENTIMENTOS DE DADOS: 6](#_heading=h.lnxbz9)

[​ 5.8 – PLANO DE PROTEÇÃO DE DADOS PESSOAIS BASEADA NA LGPD: 6](#_heading=h.35nkun2)

[​ 5.9 – PLANO DE TREINAMENTO E CONSCIENTIZAÇÃO DOS USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO: 6](#_heading=h.1ksv4uv)

1. **1 – APRESENTAÇÃO**

Este documento descreve a Política de Segurança da Informação da SEA – Secretaria de Estado da Administração de SC

Esta política consiste na adoção de medidas para proteção da informação das diversas ameaças visando preservar a integridade, confidencialidade, disponibilidade e autenticidade dos ativos de informação.

As diretrizes descritas neste documento servem para orientar as ações para iniciar, implementar, manter e melhorar a gestão da segurança da informação e comunicação de maneira a promover a criação de alicerces para a proteção da informação.

A Política de Segurança da Informação e Comunicação é uma declaração formal acerca do compromisso com a proteção, controle e monitoramento das informações processadas, armazenadas, transmitidas ou custodiadas, de sua propriedade e/ou sob sua guarda.

As diretrizes apresentadas nesta Política foram baseadas nas recomendações das publicações da família de normas NBR ISO/IEC 27000.

1. **2 – DOS OBJETIVOS**

Além de buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade são objetivos da Política de Segurança da Informação da SEA:

1. Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional.
2. Designar, definir ou alterar papéis e responsabilidades do grupo responsável pela Segurança da Informação e Comunicações.
3. Apoiar a implantação das iniciativas relativas à Segurança da Informação e Comunicações.
4. Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados
5. **3 – DECLARAÇÃO DE COMPROMETIMENTO DA ALTA GESTÃO**

A alta gestão do órgão reconhece a importância dos ativos de informação da organização e de seus clientes, fornecedores e parceiros, que estão sob sua responsabilidade. Esta apoia o Sistema de Gestão de Segurança da Informação em suas atividades, visando a garantia dos princípios de confidencialidade, integridade e disponibilidade e compromete-se a implantar, manter, divulgar e fiscalizar esta política dentro da organização.

1. **4 – ABRANGÊNCIA E DIVULGAÇÃO**

Esta POSIN e suas eventuais normas complementares aplicam-se em toda a organização, abrangendo os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, tenha acesso aos ativos de informação da SEA em qualquer meio ou suporte.

Os princípios e diretrizes gerais desta POSIN também se aplicam às entidades vinculadas a SEA e a quaisquer relacionamentos com outros órgãos e entidades públicos ou privados.

Este documento, dentre outras diretrizes, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do órgão poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

Esta Política de Segurança da Informação será implementada no SEA por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do tipo de vínculo, nível hierárquico ou função.

Todos os dirigentes, empregados, servidores, colaboradores, estagiários, prestadores de serviços e visitantes da empresa.

1. **5 – DOCUMENTOS QUE COMPÕEM A POSIN**
2. **5.1 – COMITÊ DE SEGURANÇA DA INFORMAÇÃO:**
* O comitê é responsável pela gestão da segurança da informação nos aspectos físicos e lógicos.

**5.2 – PLANO DE CONTINUIDADE DE NEGÓCIO (PCN):**

* A responsabilidade pela continuidade dos negócios, bem como pelo desenvolvimento do PCN é do Comitê de Segurança da Informação.
* O PCN deve descrever os controles preventivos e corretivos para situações de contingência.
1. **5.3 – PLANO DE GESTÃO DE ATIVOS DE INFORMAÇÃO:**
* Os ativos de informação devem ser classificados de acordo com aspectos legais e requisitos de negócio.
* A responsabilidade pelo sistema de classificação de ativos é do Comitê de segurança da informação.
* A responsabilidade pela classificação dos ativos de informação em cada setor é do respectivo gestor.

**5.4 – PLANO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO:**

* A análise de risco deve abranger aspectos físicos e lógicos da segurança da informação.
* A análise de risco deve resultar em um plano de ação para a redução dos riscos encontrados.

**5.5 – PLANO DE GESTÃO DE CONTRATOS:**

* A política de Segurança da Informação para fornecedores deve ser parte integrante dos contratos.
* Realizar auditorias de segurança da informação em seus fornecedores, quando as informações fornecidas forem de classificação restrita.

**5.6 – PLANO DE CONTROLE DE ACESSO À INFORMAÇÃO:**

* Segurança Física: Descrever os controles e monitoramento dos ambientes físicos.
* Segurança Lógica: Descrever controles de acesso à internet, controle de acesso à rede interna, armazenamento e manuseio de informações, utilização de e-mail, instalação e utilização de sistemas corporativos, uso de senhas.

**5.7 – PLANO DE CONSENTIMENTOS DE DADOS:**

* Obter consentimento das partes envolvidas para dar segurança legal.
* Captação de dados de terceiros e seu armazenamento, uso de dados e privacidade.
* Consentimento de sigilo e confidencialidade.
1. **5.8 – PLANO DE PROTEÇÃO DE DADOS PESSOAIS BASEADA NA LGPD:**
* Declaração de terceiros a conformidadecom a LGPD
* Questionário para a conformidade
1. **5.9 – PLANO DE TREINAMENTO E CONSCIENTIZAÇÃO DOS USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO:**
* Elaborar conteúdo para divulgar a Política de Segurança da Informação e avaliar o nível de maturidade;
* Identificar necessidades de treinamento e capacitação dos usuários;
* Mostrar e sensibilizar sobre a importância da manutenção das ações de Segurança da Informação.
* Todos os usuários devem assinar um termo de ciência em relação à Política de Segurança da Informação.