**PLANO DE PROTEÇÃO DE DADOS PESSOAIS BASEADA NA LGPD**

Data: 04/11/2021

Versão 2.0

**HISTÓRICO DE ALTERAÇÕES**

| **DOCUMENTO** |
| --- |
| **Descrição** | Documentação referente ao Plano de Proteção de Dados Pessoais Baseada na LGPD, descreve as ações a serem tomadas para a conformidade com a Lei Geral de Proteção de Dados Pessoais. |
| **Objetivo** | Estabelecer medidas para a salvaguarda dos dados e conformidade da Sigla do órgão com a LGPD. |
| **Responsável** | **Equipe** | **Criado em** |
| GESIN – DITI | 00/00/2021 |
| **Setor** | Gerência de Infraestrutura e Segurança da Informação - GESIN |

**SUMÁRIO**

[PLANO DE PROTEÇÃO DE DADOS PESSOAIS BASEADA NA LGPD 1](#_heading=h.4lvqt0ypcqgx)

[HISTÓRICO DE ALTERAÇÕES 2](#_heading=h.gjdgxs)

[PLANO DE PROTEÇÃO DE DADOS PESSOAIS BASEADA NA LGPD 3](#_heading=h.t3qspumhaqr2)

[PAPÉIS E RESPONSABILIDADES 4](#_heading=h.b8e1fvdn3eus)

[CONTROLE DE EXECUÇÃO 4](#_heading=h.kzk40dhrk9hz)

[REQUISIÇÃO A TERCEIROS DE CONFORMIDADE COM A LGPD: 5](#_heading=h.5ao89lh6e8cf)

AVALIAÇÃO DE MATURIDADE DE SEGURANÇA E PRIVACIDADE EM ADEQUAÇÃO À LGPD 6

COMUNICAÇÃO INTERNA SOBRE ALTERAÇÕES NA LGPD E POSIN 7

REGISTRO DE EVENTOS 8

INVENTÁRIO DE DADOS 9

MODELOS PARA REQUISIÇÃO DE CONFORMIDADE COM A LGPD A TERCEIROS 11

**PLANO DE PROTEÇÃO DE DADOS PESSOAIS BASEADA NA LGPD**

 O plano de proteção de dados pessoais baseado na LGPD, é parte integrante da POSIN (Política de Segurança da Informação) Nome do órgão do Governo do Estado de Santa Catarina. Estabelece diretrizes, normas, procedimentos, mecanismos, competências, responsabilidades, direcionamentos e valores a serem adotados para a Segurança da Informação, adequados às responsabilidades, funcionalidades e peculiaridades Nome do órgão do Governo do Estado de SC.

Os objetivos das ações a serem implementadas são a salvaguarda dos dados, das informações e materiais sensíveis, críticos e sigilosos, dos sistemas computacionais, suas instalações e das áreas de trabalho, além da preservação. Este plano leva em consideração cinco pontos cruciais da LGPD para a adequação e conformidade Nome do órgão com a Lei.

1. **Consentimento:** Autorização expressa em TODA captação de dados, porém de forma SEPARADA;
2. **Finalidade:** Porque e para que quer usar o dado, legítimo interesse. Está vedado a captação de QUALQUER DADO para enviar a terceiros;
3. **Transparência:** O que está acontecendo com os dados e estes termos estarem disponíveis para acesso, ter contratos para tudo;
4. **Não discriminação**: Não pode o usuário sofrer qualquer prejuízo pelo seu dado coletado;
5. **Opção fácil e clara:** Para descadastrar ou excluir o dado do requerente SEM JUSTIFICATIVA;

**PAPÉIS E RESPONSABILIDADES**

| **Papéis** | **Responsabilidades** |
| --- | --- |
| [Nome/Sigla].Nome DPODiretores e GerentesEncarregados | [breve descrição]DPO Sigla do órgãoDiretores e Gerentes Sigla do órgãoEncarregados | [atribuições de competência].Fiscalizar a realização e o cumprimento do planoCoordenar a execução do planoExecução do plano |

**CONTROLE DE EXECUÇÃO**

| **Controle** | **Método de execução** | **Frequência** |
| --- | --- | --- |
| [Nome/Sigla]. | [A ser feito]. | [Período Mensal/Anual etc]. |

**FERRAMENTAS**

| **POSIN/SEA** | **Política de Segurança da Informação da SEA** |
| --- | --- |
|  |  |

**REQUISIÇÃO DE CONFORMIDADE COM A LGPD A TERCEIROS:**

 **Objetivo:**

* Obter garantia de que terceiros que tenham qualquer tipo de interação com Sigla do órgão, desde que se utilizem de dados pessoais, estejam em conformidade com a LGPD.

 **Responsável:**

* Gestores e encarregados por interações com terceiros.

 **Entradas:**

* Aviso legal de conformidade.

 **Descrição das Atividades:**

* Elencar interações com terceiros que envolvam dados pessoais.
* Disponibilizar no início da interação o aviso legal.
* Obter a garantia através de um aviso legal em que o terceiro, com exceção do titular dos dados, garanta o compromisso e conformidade com a LGPD.
* Armazenar a garantia juntamente com a saída da interação.

 **Saídas:**

* Aviso legal com assinatura digital/física do terceiro.

**AVALIAÇÃO DE MATURIDADE DE SEGURANÇA E PRIVACIDADE EM ADEQUAÇÃO À LGPD:**

**Objetivo:**

* Avaliar o grau de maturidade em segurança da informação e privacidade do Sigla do órgão, no que concerne às obrigações contidas na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
* Estruturar e aplicar medidas de segurança da informação, inclusive levantamento sobre necessidades específicas referentes ao tema; e
* Promover ações de conscientização de lideranças, servidores, terceirizados, estagiários e demais colaboradores, com a finalidade de promover a segurança no cotidiano do trabalho.

 **Responsável:**

* Gestores.
* DPO.

 **Entradas:**

* Questionário avaliativo sobre segurança e privacidade. [Acesso ao questionário](http://limesurvey.sgd.nuvem.gov.br/index.php/798411?lang=pt-BR).

 **Descrição das Atividades:**

* Acessar o questionário avaliativo e responder as perguntas com base no seu departamento.
* A etapa deverá ser realizada a cada nova atualização que for gerada no questionário e reavaliado semestralmente
* O resultado da avaliação deverá ser guardado pelos responsáveis como prova de cumprimento desta atividade, e para fins comparativos do resultado entre períodos. Podendo o mesmo ser solicitado a qualquer momento pelo DPO para fins de verificação de conformidade à referida lei e incitação ao desenvolvimento de melhorias no que tange a segurança da informação da Sigla do órgão.

 **Saídas:**

* Resultado do questionário deve ser salvo após avaliação.

**COMUNICAÇÃO INTERNA SOBRE ALTERAÇÕES NA POSIN:**

**Objetivo:**

* Fazer com que todos colaboradores Nome do órgão tenham conhecimento e estejam cientes das alterações na POSIN.

 **Responsável:**

* DPO.
* GETIN

**Entradas:**

* Envio de email e outros meios de comunicação interna do órgão, comunicando as alterações; e
* Incluindo resumo prévio do que foi alterado na POSIN.

 **Descrição das Atividades:**

* O DPO deve se manter atualizado sobre alterações na Política de Segurança da Informação do órgão.
* Será obrigação da GETIN comunicar o DPO sobre alterações/atualizações realizadas na POSIN.
* Quando ocorrido algum tipo de atualização, o DPO junto aos responsáveis pela comunicação, deverão realizar o comunicado da mesma para todos os colaboradores.
* A comunicação deverá ser realizada de modo individualizado por email e/ou mensagens de aplicativos, e para suprir casos em que o colaborador não possua acesso aos mesmos, poderá ser realizado por meios alternativos.

**Saídas:**

* Não se aplica.

**REGISTRO DE EVENTOS:**

**Objetivo:**

* Possuir em registro tudo o que tiver sido feito referente a LGPD (consentimento dos funcionários sobre o termo de sigilo e confidencialidade, comprovação individual dos funcionários sobre treinamento LGPD, relatório da avaliação de maturidade de segurança e privacidade com a LGPD, tudo e qualquer ação pertinente a proteção de dados pessoais).

 **Responsável:**

* DPO

**Entradas:**

* Consentimento dos funcionários sobre o termo de sigilo e confidencialidade;
* Comprovação individual dos funcionários sobre treinamento LGPD;
* Relatório da avaliação de maturidade de segurança e privacidade com a LGPD;
* Tudo e qualquer feito pertinente à proteção de dados pessoais e segurança da informação.

 **Descrição das Atividades:**

* O DPO assim como os gerentes dos departamentos, devem guardar em relatório todo tipo de feito realizado em prol da segurança dos dados pessoais e LGPD.

**Saídas:**

* Registro de eventos.

**INVENTÁRIO DE DADOS:**

**Objetivo:**

* Assegurar o Art. 37 da LGPD. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.
* Salvaguarda do órgão em acordo com a Lei.

 **Responsável:**

* DPO

**Entradas:**

* Modelo disponibilizado pelo Governo Federal (https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/templates-e-ferramentas/template\_inventario\_dados\_pessoais.xlsx)
* Descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade como:
	+ atores envolvidos (agentes de tratamento e o encarregado);
	+ finalidade (o que a instituição faz com o dado pessoal);
	+ hipótese (arts. 7º e 11 da LGPD);
	+ previsão legal;
	+ dados pessoais tratados pela instituição;
	+ categoria dos titulares dos dados pessoais;
	+ tempo de retenção dos dados pessoais;
	+ instituições com as quais os dados pessoais são compartilhados;
	+ transferência internacional de dados (art. 33 LGPD); e
	+ medidas de segurança atualmente adotadas.

 **Descrição das Atividades:**

* O DPO juntamente com o GETIN e gerentes dos departamentos, devem realizar o inventário de dados para seus sistemas.
* Preencher o modelo de inventário de dados e atualizá-lo conforme a demanda.

**Saídas:**

Inventário de Dados Pessoais.

**MODELOS PARA REQUISIÇÃO DE CONFORMIDADE COM A LGPD A TERCEIROS**

**Modelo aviso legal (disclaimer):**

Ao prosseguir desta etapa, resguardo a Secretaria de Estado da Administração, que estou ciente, em conformidade e acordo com a Lei 13.709/2018 que regula o tratamento de dados pessoais no Brasil.

**Modelo captura de consentimento (cláusula):**

<Nome do terceiro>, portador do cnpj <código cnpj>, resguardo a Secretaria de Estado da Administração, o mesmo <nome do terceiro> garante estar em conformidade com a Lei 13.709/2018 que regula o tratamento de dados pessoais no Brasil.