# PLANO DE TREINAMENTO E CONSCIENTIZAÇÃO DOS USUÁRIO SOBRE SEGURANÇA DA INFORMAÇÃO

Data: 05/07/2021

Versão 1.0

**HISTÓRICO DE ALTERAÇÕES**

|  |  |  |
| --- | --- | --- |
| **DOCUMENTO** | | |
| **Descrição** | Documentação dos planos de Segurança da Informação | |
| **Objetivo** | Este documento descreve os processos do Plano de Gestão de Riscos de Segurança da Informação | |
| **Responsável** | **Equipe** | **Criado em** |
| GESIN – DITI | 05/07/2021 |
| **Setor** | Gerência de Infraestrutura e Segurança da Informação - GESIN | |

**SUMÁRIO**

[PLANO DE TREINAMENTO E CONSCIENTIZAÇÃO DOS USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO 3](#_heading=h.2et92p0)

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

[CONTROLE DE EXECUÇÃO 4](#_heading=h.3dy6vkm)

[FERRAMENTAS 4](#_heading=h.1t3h5sf)

[DESCRIÇÃO DAS ATIVIDADES: 5](#_heading=h.4d34og8)

[AVALIAR O NÍVEL DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO NO ÓRGÃO (ISO 27001): 6](#_heading=h.2s8eyo1)

[ELABORAR MATERIAL DE CAMPANHA DE SENSIBILIZAÇÃO: 7](#_heading=h.2xcytpi)

[TREINAMENTO INSTITUCIONAL LGPD: 8](#_heading=h.3rdcrjn)

[TREINAMENTO GERENCIAL LGPD: 9](#_heading=h.26in1rg)

[TREINAMENTO DIRECIONAL LGPD: 11](#_heading=h.lnxbz9)

[CONSCIENTIZAÇÃO INSTITUCIONAL: 12](#_heading=h.35nkun2)

# PLANO DE TREINAMENTO E CONSCIENTIZAÇÃO DOS USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO

Proteger informações da população e dados sigilosos da organização é o principal objetivo deste plano. A forma eficaz de se fazer isso é através de um treinamento qualificado de todos os usuários e campanhas constantes de conscientização embasadas sempre na Política de Segurança da Informação Institucional.

Um bom plano de conscientização de segurança deve instruir os funcionários sobre políticas e procedimentos organizacionais para trabalhar com tecnologia da informação e todo acesso físico a locais e ou documentos/objetos sensíveis. Os colaboradores também devem receber informações sobre quem contatar se descobrirem uma ameaça à segurança e aprenderem que os dados são um ativo corporativo valioso.

Este plano visa garantir que todos os envolvidos tenham um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo do plano de conscientização é proteger o ativo de informações da instituição para garantir a continuidade do trabalho, minimizar os danos e reduzir eventuais prejuízos de qualquer sorte.

O treinamento dos usuários para que eles sejam conscientes da segurança os fornecerá as habilidades necessárias para sinalizar comportamentos suspeitos

A metodologia adotada será inicialmente top – down, onde alta gestão com as diretorias, gerências e coordenadores serão capacitados a criar e difundir a Política de Segurança da Informação das suas respectivas instituições.

Em paralelo, se faz necessário um treinamento/seminário de conhecimentos básicos da LGPD a todos os funcionários, normalizando a instituição nos conhecimentos e conscientização dos direitos e deveres relacionados à segurança da informação.

Estabelecimento de métricas de acompanhamento para medir o sucesso do treinamento de conscientização para apresentar à alta administração para justificar novos planos.

Por fim, setores e áreas específicas irão identificar seus colaboradores e assuntos mais sensíveis para solicitar treinamentos direcionais e mais eficazes na disseminação do conhecimento e efetivos nas futuras tomadas de decisão.

# PAPÉIS E RESPONSABILIDADES

|  |  |  |  |
| --- | --- | --- | --- |
| **Papéis** | | | **Responsabilidades** |
| [Nome/Sigla]. | [breve descrição]. | [atribuições de competência]. | |

# 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** |
|  |  |

# DESCRIÇÃO DAS ATIVIDADES:

Cada atividade terá uma descrição breve orientando ao órgão ou instituição como alcançar bons níveis de treinamento de pessoal e conscientização.

**Objetivo:**

Mitigar ao máximo os riscos na segurança da informação através da interação humana.

**Responsável:**

Gestores.

**Entradas:**

* Cursos;
* Treinamentos;
* Seminários;
* Trabalho direcionado de conscientização
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

Definir cada atividade que embasará o cumprimento das atividades.

**Saídas:**

Documentos auxiliares e comprobatórios.

## AVALIAR O NÍVEL DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO NO ÓRGÃO (ISO 27001):

**Objetivo:**

Identificar o nível de maturidade do <...> nos aspectos relacionados à segurança da informação, considerando o disposto na norma ISO 27001.

**Responsável:**

* Gestor institucional

**Entradas:**

* Pesquisa de maturidade de segurança da informação com usuários

**Descrição das Atividades:**

* Elaborar formulário de pesquisa a ser lançado aos usuários de TI
* Disponibilizar formulário ou questionário para os usuários através do portal ou e-mail
* Comunicar usuários sobre o preenchimento
* Compilar respostas e identificar nível de maturidade
* Divulgar no portal institucional o nível de maturidade.

**Saídas:**

* Número que caracteriza o nível de maturidade do <...> em segurança da informação.

## ELABORAR MATERIAL DE CAMPANHA DE SENSIBILIZAÇÃO:

**Objetivo:**

Promover sensibilização e incremento na conscientização dos usuários de TI do <...> nos aspectos que envolvam segurança da informação, visando incrementar o nível de maturidade do <...> de inexistente para definido, bem como reduzir os incidentes de segurança da informação.

**Responsável:**

* Gestor institucional

**Entradas:**

* Modelos de cartilhas e manuais de outros órgãos públicos e empresas privadas.

**Descrição das Atividades:**

* Revisar as normas em vigor: verificar se há necessidade de alteração. A alteração da norma pode decorrer de uma melhoria no processo ou, ainda, de uma adequação ou acréscimo às diretrizes e procedimentos nela previstos. Se houver necessidade de alteração, elaborar proposta. Caso contrário, elaborar informação dando ciência da revisão e das conclusões que apontam para a manutenção do conteúdo.

**Saídas:**

* Cartilha de sensibilização.

## TREINAMENTO INSTITUCIONAL LGPD:

**Objetivo:**

Tem como objetivo informar a todos os funcionários sobre as mudanças ocasionadas pela Lei. Nº 13.709/2018, que regula as atividades de tratamento de dados pessoais. Com base nos elementos Dados pessoais, legislação de dados, proteção de dados, lei geral de proteção de dados pessoais, LGPD nas relações negociais, adequação a LGPD, premissas da LGPD. Apresentação da Política de Segurança da Informação formulada pela própria instituição.

**Responsável:**

* Gestor institucional

**Entradas:**

* Curso ou seminário;
* Política de Segurança da Informação institucional;
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

* Treinamento de nivelamento de toda organização na LGPD e na Política de Segurança da Informação desenvolvida pela instituição.

**Saídas:**

* Certificação individualizada de comparecimento.

## TREINAMENTO GERENCIAL LGPD:

**Objetivo:**

Qualificar os gestores do órgão a LGPD e suas implicações, disseminar o conhecimento no órgão ou instituição e capacitá-los a criar a Política de Segurança da Informação Institucional.

**Responsável:**

* Gestor em conjunto com a alta direção.

**Entradas:**

* Curso completo LGPD
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

|  |  |
| --- | --- |
| **CONTEÚDO DO PROGRAMA SUGERIDO** | |
| **1º Dia** | **2º Dia** |
| Introdução à lei; | Encaminhamento Jurídico; |
| Contexto e necessidade; | Doze medidas imprescindíveis; |
| Bem jurídico tutelado; | Providências de impacto jurídico; |
| Proteção legal da privacidade; | Termo de Consentimento – modelo; |
| Aplicação e alcance / Transferência Internacional de dados pessoais; | Providências Gerais; |
| Novos Conceitos; | Aplicação da Lei – atuação do Ministério Público e Procon; |
| Novos Papéis; | Vigência da Lei; |
| Consentimento – Legítimo interesse; | Relatório de Impacto; |
| Direitos do Titular / Direito ao Esquecimento; | Medidas, salvaguardas e mecanismos de mitigação de risco; |
| Tratamento de dados pessoais – Princípios; | Elaboração Relatório de impacto; |
| Hipóteses de Tratamento de dados pessoais e de dados pessoais sensíveis; | GDPR Avaliação de Impacto; |
| Dispensa de consentimento; | Identificação dos Riscos; |
| Inaplicabilidade; | Classificação de Riscos; |
| Sanções previstas na lei; | Gestão de Riscos; |
| Providências; | Medidas Técnicas e Administrativas de Mitigação de Riscos; |
| ANPD – Configuração/Papel; | Plano de ação; |
| Formação dos Conselhos; | Gestão de Incidentes. |
| Papel da ANPD; |  |
| Aplicação da GDPR; |  |
| Conformidade com a lei; |  |
| Bases técnicas para a proteção de dados pessoais; |  |
| ROADMAP para a adequação técnico-administrativa; |  |
| Processos de negócios; |  |
| Desenho de Processos; |  |
| Gestão de Processos; |  |
| Mapeamento dos dados pessoais; |  |
| Governança; |  |
| ABNT NBR ISO/IEC 27001:2013 – SGSI; |  |
| ABNT NBR ISO/IEC 27701:2019 – SGPI; |  |
| Para Entender Risco; |  |

**Saídas:**

* Certificação individual de participação do curso
* Política de Segurança da Informação

## TREINAMENTO DIRECIONAL LGPD:

**Objetivo:**

Identificado assunto e público-alvo específico, sugerir a gestão responsável treinamento direcional.

Tratar os assuntos específicos e sensíveis a instituição para elevar o nível de conformidade do órgão ou instituição com a LGPD e minimizar eventual risco.

**Responsável:**

* Gerências e seus gestores.

**Entradas:**

* Curso ou seminário específico do assunto;
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

* Assunto específico e setor específico voltado para LGPD.

**Saídas:**

* Certificação individual;

## CONSCIENTIZAÇÃO INSTITUCIONAL:

**Objetivo:**

Criar rotina de comunicação aos usuários das políticas, sistemas, atividades e ações relacionadas a segurança da informação.

**Responsável:**

* Gestores.

**Entradas:**

* Rotinas de comunicados;
* Sistemas de avisos;
* Lista atual com funcionários;
* Lista atual com empresas envolvidas;
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

* Criar uma metodologia cíclica de comunicar toda e qualquer atualização na Política de Segurança da Informação, promover confecção de textos explicativos para sites, sistemas e documentos institucionais, criar mailing com ações e atividades relacionadas a segurança da informação e identificar visualmente termos da política em locais físicos para conhecimento das regras estabelecidas institucionais.

**Saídas:**

* Placas e avisos físicos de segurança;
* Avisos e explicações nos sites e sistemas governamentais;
* Mailing informativo;
* Divulgação das versões atualizadas da Política de Segurança da Informação.