[logotipo da organização]

[nome da organização]

Commented [AES1]: Todos os campos desde documento que aparecem entre colchetes devem ser preenchidos.

PROCEDIMENTO DE GESTÃO DE INCIDENTES

Commented [AES2]: Para saber mais sobre o assunto, leia este artigo:

How to handle incidents according to ISO 27001
https://advisera.com/27001academy/blog/2015/10/26/how-to-handle-incidents-according-to-iso-27001-a-16/

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Commented [AES3]: O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

Sumário

1. Finalidade, escopo e usuários

A finalidade deste documento é garantir a detecção rápida de eventos de segurança e fragilidades e rápida reação e resposta a incidentes de segurança.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), ou seja, a todos os funcionários e a outros ativos usados no escopo do SGSI, bem como a todos os fornecedores e a outras pessoas de fora da organização que têm contato com os sistemas e as informações do SGSI.

Os usuários deste documento são todos funcionários da [nome da organização], bem como as pessoas mencionadas acima.

Commented [AES4]: Inclua o nome da sua organização.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas 7.4, A.5.7, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.4 e A.6.8
- Política de segurança da informação
- Lista de obrigações legais, regulamentares, contratuais e outras

Commented [AES5]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação ISO 27001.

Commented [AES6]: Caso não tenha esta lista, então nestes itens liste todos os requisitos da legislação e contratuais relativos a classificação da informação.

3. Gestão de incidentes

Um incidente de segurança da informação é um ou uma série de eventos não desejados ou não [illegible]

3.1. Recebimento de classificação de incidentes, fragilidades e eventos

Todo funcionário, fornecedor ou terceiro que esteja em contato com as informações, sistemas e/ou áreas sensíveis da [nome da organização] deve informar quaisquer ameaças, fragilidades, incidentes ou eventos que podem levar um possível incidente da seguinte forma:

1. todos os eventos relacionados à tecnologia de informações e comunicação devem ser informados para [cargo]
2. [illegible]

Commented [AES7]: Inclua o nome da sua organização.

Commented [AES8]: Inclua o cargo da pessoa designada como [illegible]

Commented [AES9]: Inclua o cargo da pessoa designada como [illegible]

Incidentes, ameaças, fragilidades e eventos devem ser informados assim que possível, por telefone ou pessoalmente.

Commented [AES10]: Outros sistemas de informação de [illegible]

A pessoa que recebeu a informação deve classificá-la da seguinte forma:

a) ameaça, fragilidade ou evento de segurança – nenhum incidente ocorreu, mas um evento ou [illegible]

b) incidente de menor porte – um incidente que não tem um impacto relevante sobre a
c) incidente de grande porte – um incidente que pode resultar em danos relevantes em função

3.2. Processo de tratamento de fragilidades ou eventos de segurança

A pessoa que recebeu a informação sobre a ameaça, fragilidade ou o evento de segurança analisa as

3.3. Tratamento de incidentes de menor porte

Se um incidente de menor porte for informado, a pessoa que receber a informação deve realizar as seguintes etapas:

1. tomar medidas para conter o incidente
2. analisar a causa do incidente
3.
4.

A pessoa que recebe a informação sobre um incidente de menor porte deve registrá-lo [descreva a forma do registro do mesmo].

Commented [AES11]: Ex.: manual, eletrônico ou automatizado

3.4. Tratamento de incidentes de grande porte

No caso de incidentes graves que possam interromper as atividades por um período de tempo

Commented [AES12]: Se você implementou a continuidade de

3.5. Aprendendo com os incidentes

Commented [AES13]: Exclua este seção se o controle A.5.27

O [cargo] deve analisar todos os incidentes registrados no Registro de incidentes (com a identificação

3.6. Ações disciplinares

Commented [AES14]: Exclua este seção se o controle A.6.4

O [cargo] deve invocar um processo disciplinar para cada violação das regras de segurança.

3.7. Coleta de evidências

Commented [AES15]: Exclua este seção se o controle A.5.28

O [cargo] irá definir as regras para identificar, coletar e preserver a evidência que será aceita como

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	[illegible]	[illegible]	[illegible]
Registro de incidentes	Pasta compartilhada na intranet	[illegible]	[illegible]	[illegible]

Somente o [cargo] pode conceder aos demais funcionários o acesso aos registros.

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

[illegible]

Commented [AES16]: Isso é apenas uma recomendação; [illegible]

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de fragilidades ou incidentes que não foram informados às pessoas autorizadas
- quantidade de incidentes que não foram tratados da forma mais adequada
- [illegible]
- [illegible]
- [illegible]

6. Anexos

- Anexo 1 – Registro de incidentes

[cargo]
[nome]

_____
[assinatura]

Commented [AES17]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.