\*\* VERSÃO DE DEMONSTRAÇÃO \*\*

[logotipo da organização]

[nome da organização]

**PROCEDIMENTO DE GESTÃO DE INCIDENTES**

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

**Histórico de alterações**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versão** | **Criado por** | **Descrição da alteração** |
| 01/10/2013 | 0.1 | Dejan Kosutic | Esboço básico do documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sumário**

[1. Finalidade, escopo e usuários 3](#_Toc368934592)

[2. Documentos de referência 3](#_Toc368934593)

[3. Gestão de incidentes 3](#_Toc368934594)

[3.1. Recebimento de classificação de incidentes, fragilidades e eventos 3](#_Toc368934595)

[3.2. Processo de tratamento de fragilidades ou eventos de segurança 4](#_Toc368934596)

[3.3. Tratamento de incidentes de pequeno porte 4](#_Toc368934597)

[3.4. Tratamento de incidentes de grande porte 4](#_Toc368934598)

[3.5. Aprendendo com os incidentes 4](#_Toc368934599)

[3.6. Ações disciplinares 4](#_Toc368934600)

[3.7. Coleta de evidência 4](#_Toc368934601)

[4. Gestão de registros mantidos de acordo com este documento 5](#_Toc368934602)

[5. Validade e gestão de documentos 5](#_Toc368934603)

[6. Anexo 5](#_Toc368934604)

# 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.

# Documentos de referência

* Norma ISO/IEC 27001, cláusulas clauses A.7.2.3, A.16.1.1, A.6.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
* Política da segurança da informação
* [Lista de requisitos legais, regulamentares, contratuais e outros]

# Gestão de incidentes

Um incidente de segurança da informação é um ou uma série de eventos não desejados ou não esperados com alta probabilidade de comprometer as operações dos negócios e ameaçar a segurança da informação (ISO/IEC 27001 3.6).

## Recebimento de classificação de incidentes, fragilidades e eventos

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

\*\* FIM DA DEMONSTRAÇÃO \*\*

Clique aqui para baixar a versão completa deste documento: <http://www.iso27001standard.com/pt/documentacao/Procedimento-de-gestao-de-incidentes>