LOGO

**LOGO**

**NORMA DE GESTÃO DE INCIDENTES**

|  |  |
| --- | --- |
| Código: | NOR-SGSI-002 |
| Versão: | 1.0 |
| Data da versão: | 01/07/2019 |
| Criado por: | NOME DA PESSOA |
| Aprovado por: | NOME DA PESSOA |
| Nível de confidencialidade: | Uso interno |

**Histórico de alterações**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versão** | **Criado por** | **Descrição da alteração** |
| 01/07/2019 | 1.0 | NOME DA PESSOA | Primeira versão do documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sumário**

[1. Finalidade, escopo e usuários 3](#_Toc416770254)

[2. Documentos de referência 3](#_Toc416770255)

[3. Gestão de incidentes 3](#_Toc416770256)

[3.1. Recebimento de classificação de incidentes, fragilidades e eventos 3](#_Toc416770257)

[3.2. Processo de tratamento de fragilidades ou eventos de segurança 4](#_Toc416770258)

[3.3. Tratamento de incidentes de pequeno porte 4](#_Toc416770259)

[3.4. Tratamento de incidentes de grande porte 4](#_Toc416770260)

[3.5. Aprendendo com os incidentes 4](#_Toc416770261)

[3.6. Ações disciplinares 5](#_Toc416770262)

[3.7. Coleta de evidência 5](#_Toc416770263)

[4. Gestão de rgistros mantidos de acordo com este documento 5](#_Toc416770264)

[5. Validade e gestão de documentos 5](#_Toc416770265)

[6. Anexo 6](#_Toc416770266)

# 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 **Empresa** , bem como as pessoas mencionadas acima.

# Documentos de referência

* Norma ISO/IEC 27001, cláusulas A.7.2.3, A.16.1.1, A.16.1.2, 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 **Empresa**  deve informar quaisquer fragilidades, incidentes ou eventos que podem levar um possível incidente da seguinte forma:

1. todos os eventos relacionadas à tecnologia de informações e comunicação devem ser informados para o **CCI (Centro de Contato e Incidentes**).
2. um analista do **CCI (Centro de Contato e Incidentes**) fará o registro e a análise inicial do fato informado e caso necessário, direcionará para um recurso técnico especialista para uma avaliação aprofundada.
3. a prova de existência da vulnerabilidade é responsabilidade única e exclusiva da equipe de resposta a incidentes.
4. todos os demais eventos devem ser informados para o **Gestor de Facilities**.
5. a **Empresa**  disponibilizará canais de comunicação específicos para receber as comunicações de incidentes de segurança da informação.

Incidentes, fragilidades e eventos devem ser informados imediatamente, através dos canais estabelecidos pela **Empresa .**

A analista do **CCI (Centro de Contato e Incidentes)** que recebeu a informação deve classificá-la da seguinte forma:

1. **fragilidade ou evento de segurança** - nenhum incidente ocorreu, mas um evento ou uma propriedade de um sistema, de um processo ou de uma organização pode acionar a ocorrência de um incidente no futuro próximo ou distante
2. **incidente de menor porte** - um incidente que não tem um impacto relevante sobre a confidencialidade ou integridade da informação e não pode resultar em não disponibilidade a longo prazo
3. **incidente de grande porte** - um incidente que pode resultar em danos relevantes em função da perda da confidencialidade ou da integridade das informações ou que pode resultar em interrupção da disponibilidade das informações e/ou de processos por um período de tempo inaceitável

## Processo de tratamento de fragilidades ou eventos de segurança

O analista do **CCI (Centro de Contato e Incidentes)** que recebeu a informação sobre a fragilidade ou o evento de segurança analisa as informações, estabelece a causa e, se necessário, sugere ações preventivas e corretivas.

## Tratamento de incidentes de pequeno porte

Se um incidente de pequeno 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. tomar ações corretivas para eliminar a causa do incidente
4. informar as pessoas envolvidas no incidente e o **CSO (Chief Security Officer)** sobre o processo de tratamento do incidente

A pessoa que recebe a informação sobre um incidente de pequeno porte deve registrá-lo imediatamente no sistema de Service Desk.

## Tratamento de incidentes de grande porte

Em casos de incidentes de grande porte, um plano de continuidade de negócios específico para o ativo ou serviço afetado é acionado.

## Aprendendo com os incidentes

O **CSO (Chief Security Officer)** deve analisar todos os incidentes registrados no Registro de incidentes (com a identificação de tipo, a afinidade e o custo do incidente) e, se necessário, deve sugerir ações preventivas ou corretivas.

## Ações disciplinares

O **CSO (Chief Security Officer)** deve invocar um processo disciplinar para cada violação das regras de segurança.

Se um incidente requerer a coleta de evidências para ações legais, o **CSO (Chief Security Officer)** coordenará o processo de coleta de evidências em um formato aceitável.

## Coleta de evidência

O **CSO (Chief Security Officer)** irá definir as regras para identificar, coletar e preserver a evidência que será aceita como evidência em processos judiciais e outros processos.

# Gestão de registros mantidos de acordo com este documento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Nome do registro*** | ***Local de armazenamento*** | ***Responsável pelo armazenamento*** | ***Controles para proteção do registro*** | ***Tempo de retenção*** |
| Registro Geral de incidentes | Local de armazenamento dos documentos (Servidor?) | Analista do CCI (Centro de Controle e Incidentes) | Somente o Analista do CCI (Centro de Controle e Incidentes) tem o direito de editar esses registros | 3 anos |
| Regras para identificar, coletar e preservar evidências | Pasta compartilhada na intranet (Onde disponibilizaremos a documentação para os usuários da empresa). | **CSO (Chief Security Officer)** | Somente o **CSO (Chief Security Officer)** tem o direito de editar e publicar as regras |  |

# Validade e gestão de documentos

Este documento é válido a partir de 01/07/2019.

O proprietário do documento é o **CSO (Chief Security Officer)**, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez a cada seis meses.

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
* quantidade de incidentes que não foram registrados no Registro de incidentes
* quantidade de incidentes para os quais as evidencias necessárias para ação legal foi insuficiente
* quantidade de violações de regras de segurança para as quais o processo disciplinar não foi invocado

# Anexo

* Documento Registro Geral de incidentes