# Propósito

A Norma de Gestão de Incidentes de Segurança e Privacidade **NOR-SGSI-011** complementa a Política de Segurança da Informação e Política de Proteção de Dados, definindo as diretrizes para a identificação, registro, avaliação, classificação, comunicação, tratamento e encerramento de incidentes de segurança da informação e privacidade na **Demarco**.

# Escopo

Esta norma é aplicável ao escopo definido na Política de Segurança da Informação e Política de Proteção de Dados.

# Glossário

* **Evento de segurança da informação e privacidade:** Ocorrências identificadas por meio de ferramentas de monitoramento ou situações identificadas pelo usuário final que podem indicar possível incidente de segurança da informação.
* **Incidente de segurança da informação e privacidade:** Um evento ou conjunto de eventos indesejados de segurança da informação, com possibilidade significativa de afetar as atividades ou ameaçar as informações da **Demarco**.
* **Logs:** Registro de atividades e eventos dentro de um sistema computacional.
* **Logs de atividade de usuário:** Registro de atividades realizadas por um usuário dentro de um sistema.
* **Logs de status do sistema:** Registro de eventos sistêmicos, que não foram realizados por um usuário.

# Diretrizes

Incidentes de Segurança da Informação e privacidade são situações nas quais é evidente a violação de diretrizes da **Demarco** ou o comprometimento da Confidencialidade, Integridade ou Disponibilidade de nossos ativos de informação. Estes incidentes podem ter diferentes consequências, a depender da situação ocorrida e do tipo de ativo comprometido. Caso um incidente envolva dados pessoais, ele passa a ser considerado um Incidente de Privacidade e sua tratativa pode variar. Para assegurar uma gestão adequada dos Incidentes de Segurança da Informação e Privacidade, devem ser observadas as seguintes diretrizes:

## Identificação de Incidentes de SI e Privacidade

1. Todos os colaboradores precisam ser minimamente conscientizados para que possam identificar incidentes de segurança da informação e privacidade. Estes incidentes devem ser reportados contendo o máximo de detalhes possível através da Central de Privacidade e Segurança da Informação;
2. Incidentes que forem identificados por terceiros devem ser reportados através do suporte.lgpd@demarco.com.br.

Para facilitar a identificação de incidentes, segue a tabela contendo exemplos:

|  |  |
| --- | --- |
| **PRINCÍPIO COMPROMETIDO** | **DESCRIÇÃO** |
| Diretrizes de Segurança da Informação e Privacidade | Compartilhar credenciais de acesso;  Usar software não autorizado. |
| Confidencialidade | Acesso por colaborador ou terceiro de forma não autorizada a um sistema, dados ou informações;  Envio de e-mail contendo arquivos ou informações a destinatário incorreto;  Divulgação indevida de informações confidenciais. |
| Integridade | Alteração indevida ou não autorizada de dados e informações;  Corrupção lógica de um conjunto de dados ou arquivos. |
| Disponibilidade | Destruição ou perda de ativo de informação;  Indisponibilidade temporária de informação, sistema ou recurso tecnológico. |

## Registro, Avaliação e Classificação de Incidentes de SI e Privacidade

1. Incidentes de SI e Privacidade registrados devem ser complementados durante sua triagem para que contenha no mínimo as seguintes informações.

* Nome do Solicitante;
* Área/Departamento;
* Data e hora da identificação;
* Descrição do incidente;
* Classificação do incidente quanto a seu nível de criticidade;
* Sistema, serviço, processo ou ativo afetado;
* Categoria do incidente;
* Se o incidente envolveu dados pessoais;
* Indicação dos colaboradores que atuarão no time de resposta.

1. Os incidentes de SI e privacidade deverão ser avaliados e classificados de acordo com os seguintes critérios de criticidade:

|  |  |
| --- | --- |
| **CLASSIFICAÇÃO** | **DESCRIÇÃO** |
| **BAIXO** | * Representa baixo impacto para o negócio a nível operacional e financeiro; * Não oferece risco ao sigilo das informações e dados pessoais. |
| **MÉDIO** | * Afeta parcialmente a capacidade operacional e financeira do negócio; * O sigilo das informações de negócio é mantido, mas pode haver risco de comprometimento; * Pode ter impacto na integridade, confidencialidade ou disponibilidade de um pequeno conjunto de dados pessoais. |
| **ALTO** | * Representa alto impacto para o negócio a nível operacional e financeiro; * O sigilo das informações de negócio foi comprometido; * Impactou a integridade, confidencialidade ou disponibilidade de grande conjunto de dados pessoais ou quantidade considerável de dados pessoais sensíveis ou de crianças e adolescentes. |
| **SEVERO** | * Representa impacto catastrófico ao negócio, podendo afetar todo o funcionamento da **Demarco**; * O sigilo das informações de negócio foi comprometido e é de grande impacto para o negócio a nível contratual ou regulatório; * Impactou a integridade, confidencialidade ou disponibilidade de grande conjunto de dados pessoais sensíveis ou de crianças e adolescentes. |

1. Após a avaliação do registro de incidente, deverão ser designados os colaboradores que farão parte da equipe de resposta do incidente. O CSIP tem autonomia para compor equipe multidisciplinar para o tratamento de incidentes.

## Comunicação

1. De acordo com a classificação do incidente, diferentes partes precisam ser comunicadas para a tomada de ações:

|  |  |
| --- | --- |
| **CLASSIFICAÇÃO** | **DEVE SER COMUNICADO A** |
| **BAIXO** | * N/A |
| **MÉDIO** | * CSIP |
| **ALTO** | * CSIP * JURIDICO CONSULTORIAS |
| **SEVERO** | * CSIP * JURIDICO CONSULTORIAS * PRESIDÊNCIA |

1. Colaboradores que venham a ter o conhecimento de incidentes de segurança da informação e privacidade de nível alto ou severo estão estritamente proibidos de compartilhar com qualquer outra parte a existência e detalhes do incidente, a menos que tenham permissão expressa para tal.
2. Incidentes de Segurança da Informação e privacidade de nível alto ou severo não devem ser discutidos em:

* Ambientes ou locais que as informações possam ser ouvidas por pessoas não autorizadas;
* Através de softwares e aplicações não homologadas.

1. A comunicação oficial em nome da **Demarco** sobre incidentes de segurança da informação e privacidade é restrita ao **CSIP** e à Presidência.

## Tratamento de incidentes de Segurança da Informação e Privacidade

1. Um ou mais plano(s) de resposta a incidentes devem ser utilizados para realizar o tratamento e mitigação do incidente ocorrido. Estes planos devem considerar situações comuns de incidentes e trazer uma sequência de ações que devem ser realizadas para o tratamento apropriado do incidente. Os planos devem ser criados e mantidos atualizados, conforme apropriado.
2. Quando a sequência de ações de um plano não abranger completamente as ações necessárias para o tratamento de um incidente, deve ser utilizado o plano que mais se aproxima das ações necessárias.
3. As ações tomadas pela equipe de resposta a incidentes devem ser documentadas contendo o detalhamento necessário no registro do incidente.
4. Registros físicos ou digitais que possam ser utilizados como evidência de causa ou resolução do incidente devem ser preservados e documentados no registro do incidente. Para registros que forem físicos, estes devem ser digitalizados quando possível. Mediante a impossibilidade da digitalização, ele deverá ser encaminhado ao CSIP para que seja preservado.

## Encerramento do incidente

1. Após o tratamento do incidente, caberá ao CSIP avaliar se o incidente pode ser considerado como encerrado.
2. Quando apropriado, registros de incidentes que já foram encerrados devem ser analisados para:

* Aplicar melhorias em planos de resposta existentes;
* Permitir a construção de novos planos de resposta a incidente e documentos orientativos;
* Melhorar ou implementar novos controles de segurança da informação e privacidade;

1. Convém avaliar a necessidade de abertura de um RACM, de acordo com os requisitos da **NOR-SGSI-0010 Norma de Ações Corretivas e de Melhorias,** para a tomada de ações corretivas e de melhoria dos controles de segurança da informação e privacidade.

## Indicadores de gestão

1. Trimestralmente deve ser realizada a compilação de indicadores de incidentes de segurança da informação e privacidade em um relatório que deverá ser apresentado à Presidência. O relatório deve conter no mínimo:

* Quantidade de incidentes no período/por classificação;
* Quantidade de Incidentes concluídos e em aberto;
* Tempo médio para tratamento de incidentes;
* Quantidade de incidentes envolvendo dados pessoais;
* Resumo de incidentes de classificação alto e severo do período.

# Papéis e Responsabilidades

## COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Avaliar relatórios de gestão de incidentes;
2. Realizar ou aprovar comunicados oficiais relacionados a incidentes a clientes e terceiros;
3. Avaliar e classificar incidentes registrados;
4. Avaliar partes necessárias que devem ser envolvidas para o tratamento de incidentes;
5. Assegurar que todas as etapas e evidências do tratamento do incidente sejam documentadas;
6. Aprovar o encerramento de um incidente;
7. Avaliar necessidade de tomada de uma ação corretiva e melhoria;
8. Compilar dados de incidentes em relatório e apresentar **à Presidência**.

## GESTORES E COLABORADORES

1. Apoiar as atividades de respostas a incidentes, quando for necessário;
2. Relatar incidentes e violações identificadas em canal específico;
3. Seguir as diretrizes relativas à comunicação desta norma.

# Gestão de versões

A revisão, aprovação e alteração desta norma segue os requisitos estabelecidos na Política de Segurança da Informação e Política de Proteção de Dados.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 03/10/2023 | CSIP | Criação da política |
| 0.2 | 15/01/2024 | CSIP | Ajustes e validação |
| 0.3 | 09/07/2024 | CSIP | Revisão e ajustes |