# Propósito

A Norma de Classificação da Informação **NOR-SGSI-001** complementa a Política de Segurança da Informação, definindo as diretrizes para a classificação, rotulagem, manuseio, guarda e descarte seguro de informações, sejam elas em formato digital ou físico.

# Escopo

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

# Conceitos

#### **Comite de Segurança da Informação e Privacidade (CSIP):** Comite responsável pela implementação e manutenção dos requisitos de Segurança da Informação e Privacidade da **Demarco, incluindo a execução do propósito da presente norma, assumindo o papel de Administrador dos Dados.**

#### **Administrador dos Dados:** Responsável por gerenciar o modelo de d**ados** corporativo, contribuindo para assegurar a qualidade das informações, a integração dos sistemas, a retenção e a disseminação do conhecimento dos negócios. Cabe a ele, guiado por certos princípios e através de atividades de planejamento, organização e controle dos dados corporativos, gerenciar os dados como recursos de uso comum da organização, promovendo-lhes os valores de autenticidade, autoridade, precisão, acessibilidade, seguridade e inteligibilidade.

#### **Correio Eletrônico (ou e-mail)**: Serviço de comunicação que consiste na troca de mensagens por meio de redes de computadores.

#### **Criptografia:** Técnica utilizada para proteger a Informação contra acesso indevido e garantir sua integridade. A criptografia baseia-se em dois processos, a encriptação –para que a informação legível seja transformada em Informação cifrada através de algoritmos matemáticos, e a decriptação – processo inverso a encriptação, torna a informação acessível somente a um destinatário autorizado.

#### **Dado pessoal:** Informação relacionada à pessoa natural identificada ou identificável.

#### **Dado pessoal sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

#### **Gestor da informação**: Colaborador ou pessoa responsável pela gestão da classificação e rotulagem de documentos na Demarco.

# Diretrizes

## Classificação e rotulagem da Informação

Para efeitos de classificação da Informação, a **Demarco** utiliza as seguintes categorias:

|  |  |  |
| --- | --- | --- |
| **CLASSIFICAÇÃO** | **DESCRIÇÃO** | **ROTULAGEM** |
| Pública | Informação de conhecimento público, que pode ser divulgada a qualquer pessoa sem que prejudique a **Demarco**. | É obrigatória a rotulagem da Informação. A classificação deve estar em local visível no documento. |
| Interno | Informação de uso interno das áreas da **Demarco**, não podendo ser compartilhada ao público em geral. | Não é obrigatória a rotulagem da informação, pois ela será a padrão. |
| Restrita | Informação que possui conteúdo sigiloso ou que identifique pessoas naturais. Seu uso é restrito a áreas específicas da **Demarco** para o desempenho das atividades profissionais e é protegido por requisitos legais e contratuais. | É obrigatória a rotulagem da Informação. A classificação deve estar em local visível no documento. |
| Confidencial | Informação que possui alto nível de criticidade ou que trate dados pessoais sensíveis, podendo prejudicar a **Demarco** em caso de acesso não autorizado. Seu uso é altamente restrito e deve estar disponível somente a pessoas autorizadas. | É obrigatória a rotulagem da Informação. A classificação deve estar em local visível no documento. |

## Segue rol exemplificativo para orientar a classificação:

## As informações, dispositivos e arquivos recebidos de terceiros, clientes, parceiros, fornecedores e demais partes externas da Demarco serão classificados como “Interno”.

1. Todos os documentos contendo informações relacionadas a dados pessoais dos colaboradores da **Demarco**, tais como número de identificação, endereços residenciais e números de seguro social, devem ser classificadas como "Confidencial".
2. Qualquer documento que contenha informações sobre processos judiciais, extrajudiciais, administrativos ou pareceres jurídicos deve ser classificado como "Confidencial".
3. Documentos que contenham informações sobre contratos com clientes ou parceiros comerciais devem ser classificados como "Restrito", especialmente se envolverem termos comerciais sigilosos.
4. Informações sobre interações com clientes envolvendo o escopo do contrato devem ser classificadas como "Restrito".
5. Todos os documentos financeiros que contenham informações bancárias, números de cartões de crédito ou informações financeiras devem ser classificados como "Confidencial".

## Manuseio da Informação

O manuseio da informação deverá obedecer às regras a seguir:

| **AÇÃO** | **CLASSIFICAÇÃO** | | |
| --- | --- | --- | --- |
| **Pública** | **Interna** | **Confidencial / Restrita** |
| Acesso | Sem restrições | Todas as áreas | Áreas ou pessoas específicas que possuem a necessidade de acesso a Informação |
| Cópia | Sem restrições | Sem restrições, desde que seja mantida no ambiente interno | Mediante a permissão do Gestor da Informação |
| Transmissão de arquivo através de redes públicas | Permitido | Permitido, desde que seja mantida no ambiente interno. | Utilizar meio de comunicação criptografada |
| Compartilhamento interno de arquivos e informações | Sem restrições | Meios de comunicação e armazenamento disponibilizados pela **Demarco** | Meios de comunicação criptografado disponibilizado pela **Demarco** |
| Compartilhamento externo de arquivos e informações | Sem restrições | Manuseio interno: Não é necessária a rotulagem. Registro padrão.  Manuseio externo: será necessária alteração da classificação. | Meio de comunicação criptografado disponibilizado pela **Demarco.** |
| Envio a terceiros via internet | Sem restrições | Manuseio interno: Não é necessária a rotulagem. Registro padrão.  Manuseio externo: será necessária alteração da classificação. | Classificado e rotulado, utilizando recurso de criptografia |
| Correio interno e externo | Envelope comum | Público: Envelope comum.  Confidencial/Restrito: Envelope carimbado com o nível de classificação e por meio rastreável. | Envelope carimbado com o nível de classificação e por meio rastreável |
| Correio eletrônico | Sem restrições | Manuseio interno: Não é necessária a rotulagem. Registro padrão.  Manuseio externo: será necessária alteração da classificação. | Classificado e rotulado, utilizando recurso de criptografia |
| Armazenamento físico | Sem restrições | Armazenar em local seguro | Armazenar em local seguro, de acesso limitado, restrito e monitorado |
| Armazenamento lógico | Sem restrições | Somente nos recursos e ferramentas disponibilizadas pela **Demarco** | Somente na ferramenta especificada pela **Demarco** como meio para armazenamento da informação |
| Descarte de documento físico | Lixo comum | Lixo comum. Recomendável uso de fragmentadora | Lixo controlado. Uso obrigatório de fragmentadora. Descarte somente mediante autorização do Gestor da Informação |
| Descarte de documento/arquivo lógico | Sem restrições Lixo comum | Meio comum de exclusão digital | Em caso de exclusão permanente, avaliar com a área de tecnologia o meio com melhor eficácia. Descarte somente mediante autorização do Administrador da Informação |
| Descarte de dispositivo tecnológico | Desmagnetização ou uso de software de sanitização | Desmagnetização ou uso de software de sanitização | Desmagnetização, criptografia one way, uso de software de sanitização ou destruição. Mediante aprovação da área de TI |

Toda regra desrespeitada será considerada uma não conformidade e será tratada como um Incidente de Segurança da Informação, cabendo uma análise da infração pelo **CSIP**.

# Papéis e Responsabilidades

## COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Analisar e tomar decisões a respeito de desvios aos requisitos desta norma.
2. **Promover a execução do propósito da presente norma, assumindo o papel de Administrador dos Dados.**

**5.2. ADMINISTRADOR DOS DADOS**

#### Gerenciar o modelo de **dados** corporativo, contribuindo para assegurar a qualidade das informações, a integração dos sistemas, a retenção e a disseminação do conhecimento dos negócios.

#### Gerenciar os dados como recursos de uso comum da organização, promovendo-lhes os valores de autenticidade, autoridade, precisão, acessibilidade, seguridade e inteligibilidade.

## 5.3. INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

1. Implementar a ferramenta operacional para execução das regras e políticas estabelecidas nesta norma.
2. Orientar e esclarecer dúvidas dos colaboradores sobre o uso de funcionalidades para o manuseio correto de Informações em recursos tecnológicos.

## GESTOR DA INFORMAÇÃO

1. Definir a classificação das Informações sob sua responsabilidade com base nas categorias de classificação constantes nesta norma.
2. Assegurar que as Informações sejam corretamente rotuladas.
3. Controlar as Informações geradas em sua área de negócio e atuação.
4. Revisar periodicamente a classificação das Informações sob sua guarda.
5. Seguir e fazer com que os requisitos da norma sejam cumpridos.
6. Comunicar ao **CSIP** qualquer desvio aos requisitos desta norma.

## COLABORADOR

1. Apoiar o Gestor da Informação na rotulagem.
2. Reportar ao Gestor atribuições incorretas de rotulagem das Informações.
3. Seguir os requisitos estabelecidos para o tratamento das Informações.
4. Comunicar ao **CSIP** qualquer desvio aos requisitos da norma.

# Sanções

Sanções serão aplicadas conforme previsto na Política de Segurança da Informação.

# Gestão de versões

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 06/07/2023 | CSIP | Criação da norma |
| 0.2 | 23/08/2023 | CSIP | Revisão e atualização |
|  |  |  |  |