# Introdução

##### A **Demarco** é uma empresa de consultoria que oferece soluções em tecnologia atua em diferentes segmentos, como:

* regularidade contratual e jurídica;
* segurança operacional em serviços de transporte;
* gestão de pessoas;
* gestão de terceiros;
* educação e treinamento corporativo;
* negociações sindicais;

##### Devido as características predominantes de trabalho da **Demarco** e da importância dos serviços prestados a seus clientes, existem diversos riscos que ameaçam a segurança dos dados e informações tratados.

##### Com isso em mente, a **Demarco** entende que é essencial que a confidencialidade, integridade e disponibilidade sejam enraizadas em sua cultura corporativa, para assegurar que o negócio se mantenha saudável, funcional e em plena expansão.

# Propósito

##### Esta Política de Segurança da Informação tem como principal objetivo:

#### Aumentar o nível de maturidade dos requisitos de Segurança da Informação conforme melhores práticas do mercado.

#### Estabelecer os requisitos para o SGSI, através de diretrizes, normas, padrões e responsabilidades internas pela Segurança da Informação.

#### Implementar, manter e melhorar controles que possam reduzir riscos à Segurança das Informações e recursos da **Demarco**.

#### Assegurar a existência de processo de revisão de acessos aos sistemas e recursos da **Demarco**.

#### Assegurar a existência de padrão de desenvolvimento seguro para as equipes de desenvolvimento.

#### Assegurar a realização de avaliações periódicas de vulnerabilidades.

#### Assegurar que seja realizada a conscientização de Segurança da Informação para os colaboradores.

#### Assegurar que a **Demarco** tenha uma gestão efetiva de incidentes de Segurança da Informação, estando sempre preparada para tratar, prevenir ou minimizar o impacto de eventuais incidentes que possam ocorrer.

#### Assegurar a existência e manutenção de diretrizes para a continuidade de negócios e recuperação de desastres.

# Escopo

##### Esta política é aplicável a todos os colaboradores, ex-colaboradores, parceiros e fornecedores que venham a ter acesso às informações ou recursos tecnológicos da **Demarco**.

# Glossário

#### **Confidencialidade:** garantia de que informações, dados ou recursos tecnológicos da **Demarco** não sejam disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

#### **Controle:** medida de segurança adotada pela **Demarco** para o tratamento de um risco específico.

#### **Disponibilidade:** propriedade dos ativos da informação da **Demarco** de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

#### **Segurança da Informação:** apreservação das propriedades de confidencialidade, integridade e disponibilidade das informações da **Demarco**.

#### **Incidente de Segurança da Informação:** um evento ou conjunto de eventos indesejados de segurança da informação, com possibilidade significativa de afetar as atividades ou ameaçar as informações da **Demarco**.

#### **Integridade:** garantia de que informações e dados da **Demarco** são exatos e completos.

#### **Risco de Segurança da Informação:** Possibilidade de ocorrência de um evento que possa impactar, positiva ou negativamente, a implementação das estratégias ou a realização dos objetivos da organização, sendo mensurado em termos de impacto e de probabilidade.

#### **Vulnerabilidade**: fraqueza de um ativo ou controle que pode ser explorada por uma ameaça, com recurso ou método de ataque.

#### **Comite de Segurança da Informação e Privacidade (CSIP):** Comitê responsável pela implementação e manutenção dos requisitos de Segurança da Informação e Privacidade da **Demarco**.

# Diretrizes

## É diretriz desta política a implementação, manutenção e melhoria de SGSI que:

#### Assegure a existência de objetivos de Segurança da Informação aderentes a realidade de negócio da **Demarco**.

#### Estabeleça e implemente políticas, normas e procedimentos que forem necessários para o direcionamento dos requisitos e controles de Segurança da Informação da **Demarco**. Estes instrumentos devem estar sempre atualizados para refletir a situação atual do negócio.

#### Estabeleça responsabilidades pela execução das atividades necessárias para a Segurança da Informação.

#### Garantir que todas as partes envolvidas tenham acesso facilitado e conheçam as políticas, normas e procedimentos de Segurança da Informação.

#### Assegure que os colaboradores sejam conscientizados e treinados nas políticas, normas e procedimentos de Segurança da Informação que forem necessários, em um programa de conscientização periódica.

#### Assegure que o SGSI atenda aos requisitos legais, normativos e contratuais que forem aplicáveis.

#### Estabeleça e mantenha processo de gestão de riscos de Segurança da Informação, bem como planejamento de ações para a redução destes riscos.

#### Estabeleça e mantenha processos para a gestão de acessos dos colaboradores aos sistemas utilizados.

#### Estabeleça e mantenha padrões com níveis apropriados para o desenvolvimento seguro dos sistemas.

#### Estabeleça e mantenha padrões com níveis mínimos de segurança para os dispositivos e recursos utilizados.

#### Estabeleça e mantenha a gestão de seus incidentes de Segurança da Informação e Privacidade.

#### Estabeleça e mantenha processos para a realização de cópias de segurança de seus dados, informações e sistemas.

#### Assegure a realização de auditorias internas periódicas para acompanhamento da maturidade do SGSI.

## A Diretoria deve estar integralmente comprometida com esta política e suas diretrizes, além de garantir que os recursos que forem necessários para a sua manutenção sejam disponibilizados, conforme a realidade do negócio e seus riscos de Segurança da Informação.

# Papéis e Responsabilidades

## Diretoria de Governança

#### Assegurar a disponibilidade de pessoal capacitado para a gestão e operação do SGSI.

#### Disponibilizar recursos necessários para a aplicação das políticas, bem como as demais normas de Segurança da Informação.

#### Avaliar e tomar decisões sobre sanções.

#### Revisar os resultados do SGSI e tomar as decisões sobre o tratamento dos riscos de Segurança da Informação.

## Comitê de Segurança da Informação e Privacidade

#### Revisar políticas e normas de Segurança da Informação e Privacidade.

#### Tomar as ações cabíveis para se fazer cumprir as diretrizes desta política e demais normas.

#### Acompanhamento periódico de gestão de riscos de Segurança da Informação e Privacidade.

#### Revisar as avaliações de riscos e seus resultados.

#### Validar a apresentação de resultados para a diretoria.

## Áreas de Privacidade e de Infraestrutura e Segurança da Informação

#### Conduzir a gestão e operação do SGSI, tendo como base esta política e demais normas e procedimentos.

#### Elaborar e propor ao Comitê de Segurança da Informação as normas e procedimentos de segurança da informação, necessários para se fazer cumprir o SGSI.

#### Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco.

#### Elaborar relatórios periódicos de suas atividades.

#### Apresentar a diretoria resultados da gestão do SGSI para a tomada de decisões.

## Colaboradores, ex-colaboradores, parceiros e fornecedores

#### Ler, compreender e cumprir integralmente as diretrizes desta política, e demais normas e procedimentos de segurança aplicáveis.

#### Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre as políticas e demais normas e procedimentos ao Comitê de Segurança da Informação.

#### Comunicar à área de qualquer evento que viole as políticas, e demais normas e procedimentos ou que possa colocar em risco a Segurança das Informações ou dos recursos tecnológicos da **Demarco**.

#### Assinar o Termo de Leitura e Ciência, formalizando a ciência e o aceite integral das diretrizes das políticas e das demais normas e procedimentos de segurança da **Demarco**, assumindo responsabilidade pelo seu cumprimento.

#### Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções.

#### Participar de conscientizações e treinamentos de Segurança da Informação que forem necessários.

# Sanções

## A mera tentativa de violação das políticas, normas e procedimentos da Demarco pelos colaboradores e ex-colaboradores, seja ela concretizada ou não, poderá ocasionar nas seguintes sanções, de acordo com a gravidade do incidente:

#### Advertência escrita.

#### Suspensão.

#### Demissão por justa causa.

#### Notificação extrajudicial.

## A aplicação de sanções será realizada conforme análise da Diretoria, munida de informações sobre o incidente ocorrido e de suas evidências.

## No caso de violações por parceiros e fornecedores, deve ser realizada análise do incidente e aplicada sanção de acordo com a gravidade do ocorrido, tendo como base os termos estabelecidos em contrato.

## A Demarco reserva-se ao direito de recorrer a medidas judiciais para reparação de danos por eventuais prejuízos suportados, independente de dolo ou culpa.

# Gestão de versões

## As políticas e normas da Demarco devem ser revisadas anualmente ou sempre que pertinente.

## A Diretoria é diretamente responsável pela revisão e aprovação das políticas e normas de Segurança da Informação.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 28/04/2023 | CSIP | Criação da política |
| 0.2 | 09/05/2023 | CSIP | Alteração dos papéis e responsabilidades |
| 0.3 | 15/08/2023 | CSIP | Ajuste de nomenclaturas |
| 0.4 | 17/07/2024 | CSIP | Revisão e ajustes |