# Propósito

##### A Política de Gestão de Riscos de Segurança da Informação, POL-SGSI-002, tem como objetivo determinar como será realizada a gestão de riscos de segurança da informação.

# A quem se destina

##### A presente política destina-se à Diretoria de Governança e ao Comitê de Segurança da Informação e Privacidade da Demarco.

# Glossário

#### **Ameaças:** indício de acontecimento desfavorável que possa afetar algum processo ou objetivo.

#### **Ativos de Informação:** refere-se aos meios de armazenamento, transmissão e processamento, aos sistemas de informação, aos locais onde tais meios se encontram, bem como às pessoas que têm acesso a eles.

#### **Risco:** 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.

# Diretrizes

##### A **Gestão de Riscos de Segurança da Informação** constitui uma das principais bases de sustentação do nosso **Sistema de Gestão de Segurança da Informação (SGSI)**. De modo geral, o processo de gestão de riscos deve percorrer etapas de:

#### **Identificação dos riscos:** nesta etapa, deverá ser identificada a vulnerabilidade, ameaça, o ativo afetado e apuração de responsáveis.

#### **Análise:** nesta etapa, deverá ser analisada a probabilidade e impacto de concretização da vulnerabilidade e ameaça identificada.

#### **Avaliação:** é o resultado da análise realizada, determinando o nível de risco que esta ameaça representa para o negócio.

#### **Tratamento:** nesta etapa, deve ser decidida a ação a ser tomada sobre o risco avaliado, bem como associar controles existentes para a redução do risco.

#### **Planejamento:** caso o risco seja considerado alto, será elaborado um plano de ação macro para a o tratamento.

#### **Monitoramento:** a depender do nível de risco identificado, deve ser mantido monitoramento periódico acerca do risco.

#### **Reavaliação: a avaliação de riscos deverá ser realizada periodicamente.** .

## Identificação dos riscos

##### Na etapa de identificação, necessário observar que:

#### Para a identificação dos riscos, podem ser conduzidas entrevistas e análise de cenários ou eventos que possam impactar os objetivos da **Demarco**. Ao registrar os riscos, devem ser considerados: a vulnerabilidade identificada, a ameaça que a vulnerabilidade representa ao negócio, a propriedade de Segurança da Informação afetada, eventuais responsáveis e o ativo ao qual o risco se aplica.

#### Os riscos identificados devem ser registrados nas planilhas de gestão de riscos.

## Análise dos riscos

##### Na etapa de análise, necessário observar que:

#### A análise deve fornecer insumos para a avaliação de riscos, subsidiando a tomada de decisões relativas à necessidade de mitigação dos riscos e às estratégias e métodos mais adequados para o seu tratamento.

#### A análise de riscos deve, ainda, abranger a avaliação das causas e das fontes de risco, bem como de seus impactos e da probabilidade de que tais riscos possam ocorrer.

#### Detalha-se abaixo a tabela de níveis de probabilidade que devem ser observadas na **Demarco**.

|  |  |  |  |
| --- | --- | --- | --- |
| **Pontuação** | **Classificações** | **Probabilidade** | **Impacto** |
| 1 | **MUITO BAIXO** | Nunca ocorreu ou é improvável que se concretize | A ocorrência causa impacto mínimo, quase irrelevante para a organização |
| 2 | **BAIXO** | Existe uma possibilidade, mas é improvável que ocorra | A ocorrência causa impacto parcial para a organização |
| 3 | **MÉDIO** | Já ocorreu anteriormente ou há chance razoável que se concretize | A ocorrência causa impacto relevante para a organização, mas sem custos financeiros |
| 4 | **ALTO** | Existe uma grande possibilidade de que ocorra | A ocorrência causa impacto alto para a organização, podendo ocorrer prejuízo financeiro |
| 5 | **MUITO ALTO** | Ocorre com certa frequência ou há alta probabilidade que se concretize | A ocorrência causa impacto muito alto para a organização, podendo ocorrer alta perda financeira ou reputacional |

## Avaliação dos riscos

##### Para realização de avaliação dos riscos, devem ser considerados o fator de probabilidade em relação à ocorrência e o fator de impacto que o risco possa causar. graduados de acordo com a Matriz de Avaliação de Riscos a seguir:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PROBABILIDADE**  **IMPACTO** | **MUITO BAIXA** | **BAIXA** | **MÉDIA** | **ALTA** | **MUITO ALTA** |
| **MUITO BAIXO** | **1** | **2** | **3** | **4** | **5** |
| **BAIXO** | **2** | **4** | **6** | **8** | **10** |
| **MÉDIO** | **3** | **6** | **9** | **12** | **15** |
| **ALTO** | **4** | **8** | **12** | **16** | **20** |
| **MUITO ALTO** | **5** | **10** | **15** | **20** | **25** |

##### Os controles requeridos e os níveis de conhecimento devem observar a criticidade do risco, conforme tabela abaixo:

|  |  |  |
| --- | --- | --- |
| **CRITICIDADE** | **VALORES** | **DESCRIÇÃO DO RISCO/CONTROLE REQUERIDO** |
| **SEVERO** | 17 a 25 | ***Risco intolerável***  Ações de controle do risco devem ser planejadas e implementadas. O monitoramento do risco deve ser realizado a cada 3 meses. |
| **ALTO** | 9 a 16 | ***Risco intolerável***  Ações de controle do risco devem ser planejadas e implementadas. O monitoramento do risco deve ser realizado a cada 6 meses. |
| **MÉDIO** | 4 a 8 | ***Risco aceitável***  Ações de controle do risco podem ser planejadas e implementadas. O monitoramento do risco deve ser realizado a cada 9 meses. |
| **BAIXO** | 1 a 3 | ***Risco aceitável***  Os controles existentes devem ser mantidos e aprimorados. O monitoramento do risco deve ser realizado a cada ano. |

##### A avaliação deve subsidiar as respostas aos riscos, que podem ser:

#### ***Evitar*** –, Eliminação da causa do evento do risco ou modificação da atividade e processo de modo a resguardar seus objetivos contra tais eventos.

#### ***Mitigar*** – Adoção de medidas e controles para reduzir a probabilidade ou o impacto dos riscos aos níveis aceitáveis definidos pela empresa.

#### ***Compartilhar ou Transferir*** – Redução da responsabilidade ou do impacto pela transferência ou pelo compartilhamento do risco com um terceiro.

#### ***Aceitar*** – Decisão consciente de assumir o risco. Em determinados casos, riscos intoleráveis podem ser aceitos pela direção.

## Critérios de aceitação de riscos

##### Os critérios de Aceitação de Riscos refletem a disposição da Demarco em tolerar determinados níveis de riscos. A tabela abaixo apresenta os possíveis fundamentos e critérios para aceitação de riscos.

|  |  |
| --- | --- |
| **MOTIVO** | **CRITÉRIO PARA ACEITAÇÃO** |
| Limitação Operacional | A mudança para controle do risco tem alto impacto as operações e atividades rotineiras. Deve ser avaliado e aprovado pela **Diretoria**. |
| Limitação Tecnológica | Não existe tecnologia apropriada para o controle do risco. Deve ser avaliado e aprovado pela **Diretoria**. |
| Limitação Financeira | O controle de segurança para a mitigação do risco tem custo financeiro maior que o impacto pela concretização do risco. Deve ser avaliado e aprovado pela **Diretoria**. |
| Limitação Jurídica | O risco não será tratado/alterado devido a requisitos regulatórios, contratuais e normativos. Deve ser avaliado e aprovado pela **Diretoria**. |
| Limitação Estratégica | O risco não será tratado/alterado devido às estratégias de negócio. Deve ser avaliado e aprovado pela **Diretoria**. |

## Tratamento dos riscos

##### Para o gerenciamento dos riscos, necessário implementar medidas de controle e desenvolver planos de ação para a redução do nível de risco, tornando-o compatível com o nível de tolerância da **Demarco**. O tratamento proposto deve contemplar, sempre que possível, a análise de custo-benefício. Os controles implementados devem ser formalmente estabelecidos e documentados, sendo acompanhados por meio de registros e indicadores quantitativos e/ou qualitativos.

##### A priorização para o tratamento dos riscos deve se pautar nos seguintes critérios:

#### Tempo necessário para implementação,

#### Recursos necessários para a implementação.

#### Tomada de decisão do Comitê de Segurança da Informação e Privacidade.

##### A partir destes critérios, há maior flexibilidade na tomada de decisões em relação às correções necessárias. por exemplo, em situações em que houver um volume considerável de riscos classificados como médio/alto para tratamento e for constado que esses riscos exigirão menos tempo e recursos para correção em comparação a um risco de gravidade mais severa, os riscos médio/alto podem ser priorizados.

##### A seleção dos controles para a redução de risco, pode ser realizada a partir do Anexo A da norma ISO/IEC 27.001 ou de diferentes frameworks de segurança, como CIS Controls e NIST.

## Monitoramento e Análise Crítica

##### .

##### O CSIP será responsável por conduzir de forma contínua o monitoramento dos riscos, controles e planos de ação, de acordo com uma periodicidade trimestral, considerando os diferentes níveis de risco.

##### Os resultados do monitoramento deverão ser registrados e comunicados para o **Comitê de Segurança da Informação e Privacidade** e para a **Diretoria**.

##### Para a efetiva Gestão de Riscos de Segurança da Informação, devem ser implementados indicadores que tenham como principal objetivo mensurar os resultados das atividades e o monitoramento do desempenho das práticas adotadas para a gestão dos riscos.

## Reavaliação dos Riscos

##### Devem ser realizadas reavaliações periódicas dos riscos identificados, com objetivo de verificar se as ações planejadas foram devidamente executadas e se demonstraram eficácia, além de analisar possíveis alterações nos níveis de risco e identificar novos riscos à Segurança da Informação do negócio.

##### Os critérios utilizados serão os mesmos empregados na etapa de identificação inicial.

##### A avaliação de eficácia deve seguir os seguintes critérios:

|  |  |
| --- | --- |
| **AVALIAÇÃO** | **DESCRIÇÃO** |
| Ineficaz | A ação de controle do risco tomada não atingiu o objetivo de redução do risco. |
| Eficaz | A ação de controle do risco tomada atingiu o objetivo de redução do risco. |

# Papéis e Responsabilidades

## Diretoria de Governança

#### Analisar os relatórios periódicos elaborados pelo **CSIP**.

#### Deliberar sobre as questões estratégicas concernentes ao processo de gestão de riscos, tais como o grau de apetite a riscos da empresa, suas faixas de tolerância,

#### Aprovar o Plano de Tratamento de Riscos,

#### Aceitar riscos de segurança da informação, de acordo com os critérios desta política,

#### Promover as ações necessárias à manutenção da Gestão de Riscos.

## Comitê de Segurança da Informação e Privacidade

#### Acompanhamento periódico do processo de gestão de riscos de Segurança da Informação.

#### Revisar o processo de gestão de riscos de Segurança da Informação.

#### Revisar as avaliações de riscos de Segurança da Informação e seus resultados.

#### Validar a apresentação de resultados para a **Diretoria**.

## Área de Privacidade e Segurança da Informação

#### Coordenar os processos de identificação, classificação e avaliação dos riscos a que está sujeita a empresa.

#### Coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos de Segurança da Informação.

#### Elaborar relatórios periódicos de suas atividades.

#### Recomendar a diretoria medidas necessárias para a correção de deficiências no programa ou para a remediação de irregularidades encontradas.

# Gestão de versões

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 09/05/2023 | CSIP | Criação da política |
| 0.2 | 11/05/2023 | CSIP | Ajuste de requisitos dos tópicos |
| 0.3 | 24/07/2023 | CSIP | Alteração de nomenclatura de programa para sistema |
| 0.4 | 18/07/2024 | CSIP | Revisão e ajustes |