# Propósito

A Norma de Ações Corretivas e Melhoria Contínua **NOR-SGSI-010** complementa a Política de Segurança da Informação e Política de Proteção de Dados, definindo as diretrizes para o tratamento de causas de não conformidades, reais ou potenciais que possam impactar a **Demarco**, a fim de assegurar que a sua repetição não ocorra e melhorar nossas capacidades de Segurança da Informação e Privacidade.

# Escopo

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

# Glossário

* **Conformidade:** Atendimento a requisitos de Segurança da Informação ou Privacidade.
* **Não-conformidade**: Não atendimento a um requisito de Segurança da Informação ou Privacidade

**Ação corretiva:** Ação para eliminar a causa de uma não conformidade identificada ou outra situação indesejável existente, a fim de prevenir sua repetição.

* **Ação imediata:** primeira ação feita quando uma não conformidade é percebida na empresa. Essa ação é feita para controlar a ocorrência, impedindo que ela continue acontecendo no momento, e é realizada após a identificação do problema.
* **Ação preventiva:** ação feita antes da não conformidade acontecer. Pode ser um evento inédito na empresa, ou inédito em um processo. Portanto, **são analisados os riscos que foram previamente detectados sobre uma potencial não conformidade** e assim é definida a ação que impedirá essa ocorrência.
* **Eficácia:** Extensão na qual as atividades planejadas são realizadas e os resultados são alcançados.

# Diretrizes

As ações para correção ou melhorias dos requisitos de Segurança da Informação e Privacidade são fundamentais para assegurar a conformidade com nossas diretrizes para estas matérias. Para garantir a tomada de ações corretivas e melhorias, estabelecemos as seguintes diretrizes:

## Identificação de não conformidade e/ou melhorias

1. Ações corretivas e/ou de melhorias devem ser formalmente registradas em um Relatório de Não Conformidade e Melhorias (RACM). Estas ações podem ser iniciadas através dos seguintes eventos:

* Incidente de Segurança da Informação ou Privacidade;
* Resultado de auditoria interna ou externa;
* Outra não conformidade;
* Identificação da ação corretiva e/ou melhoria por alguma parte interessada.

## Gestão de RACMs

As ações corretivas e/ou de melhorias devem ser controladas através de estrutura que permita no mínimo:

* Identificar o evento originário;
* Motivo de elaboração do RACM;
* Resumo do evento identificado;
* A qual controle este evento afeta;
* Matéria referente ao evento;
* Responsável pelo RACM;
* Status do RACM;
* Eficácia do RACM.

## Abertura do RACM

Para toda não conformidade e/ou ação de melhoria associada com o funcionamento e operação da Segurança da Informação e Privacidade, deve ser elaborado um Relatório de Não Conformidade e Melhorias (RACM). A seguinte tabela orienta as ações que devem ser tomadas de acordo com o tipo de ação:

|  |  |  |
| --- | --- | --- |
| **AÇÃO** | **NÃO CONFORMIDADE** | **OBSERVAÇÃO OU MELHORIA** |
| Ação imediata | Obrigatório | Não é necessário |
| Análise de causa raiz | Obrigatório | Não é necessário |
| Ação corretiva | Obrigatório | Opcional (caso optarmos pelo tratamento, deve ser realizada) |
| Ação de melhoria | Não obrigatório | Opcional (caso optarmos pelo tratamento, deve ser realizada |
| Verificação de implementação e eficácia | Obrigatório | Opcional (caso optarmos pelo tratamento, deve ser realizada) |

## Tratamento dos RACMs

O tratamento e atividades a serem executadas variam pelo tipo de evento registrado. Algumas atividades são obrigatórias para não conformidades que forem identificadas e outras são opcionais, caso forem uma observação ou melhoria.

## Ação imediata

Esta atividade deve ter como foco a tomada de uma ação imediata para remediar os efeitos de uma não conformidade;

Ex.: *Não conformidade: máquina corporativa estava fora dos padrões de configuração estabelecido.*

*Ação imediata: aplicar os padrões de configuração da máquina.*

As ações imediatas devem ser registradas como atividades, com responsável, prazo e o status destas atividades deve ser periodicamente acompanhado.

* + 1. Análise de causa raiz

1. Esta atividade deve ter como foco realizar um estudo aprofundado da causa raiz da não conformidade ter se concretizado. Podem ser utilizadas metodologias como diagrama de Ishikawa, 5 porquês, FMEA ou outras metodologias que possam alcançar este objetivo;
2. É essencial que o responsável pela não conformidade e demais envolvidos estejam presentes para esta análise.

## Ação corretiva e/ou de melhoria

1. Após a conclusão da análise de causa raiz de uma não conformidade, devem ser definidas as atividades para as ações corretivas;
2. Explicar ação de melhoria e sua relação com a (não) conformidade
3. Tanto as ações corretivas quanto ações de melhoria devem ser registradas como atividades, com responsável, prazo e o status destas atividades deve ser periodicamente acompanhado.

## Verificação de implementação e eficácia

1. Após a conclusão das atividades definidas para ações corretivas e/ou melhorias, deve ser realizada a verificação de evidências da implementação destas atividades e realizar apontamento se a ação foi eficaz ou não;
2. Ações que não forem eficazes devem gerar uma novo RACM para tratamento;
3. Caso a verificação aponte que as ações foram implementadas e eficazes, o RACM pode ser dado como concluído.

# Papéis e Responsabilidades

## COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Assegurar que a causa raiz seja registrada e tratada;
2. Apoiar o tratamento da causa raiz;
3. Acompanhar o status dos RACMs;
4. Armazenar evidências que comprovem que as atividades foram executadas;
5. Validar as ações de correção do RACM;
6. Validar as ações corretivas e/ou melhorias tomadas, verificando a eficácia através de evidências.

## GESTORES DE ÁREA/ RESPONSÁVEIS PELOS SISTEMAS

1. Executar análise de causa raiz;
2. Definir e executar as atividades de ações imediatas, corretivas ou de melhoria;
3. Gerar e manter evidências que comprovem que a execução das atividades foram eficazes.

# 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 | 18/09/2023 | CSIP | Criação da política |
|  |  |  |  |
| 0.2 | 18/12/2023 | CSIP | Revisão e ajustes |
| 0.3 | 09/07/2024 | CSIP | Revisão anual |