# Propósito

A Norma de Backup **NOR-SGSI-005** complementa a Política de Segurança da Informação, definindo as diretrizes para a criação, armazenamento, manutenção, recuperação e descarte de cópias de segurança de dados e informações da **Demarco**.

# Escopo

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

# Glossário

* **Ativo de Informação**: Englobam dados, informações, aplicações, sistemas, equipamentos de rede, hardware, software e firmware utilizados pela **Demarco**.
* **Backup**: Cópia de dados de um dispositivo de armazenamento para outro, a fim de que possa ser restaurado em caso da perda, dano, sequestro de dados, entre outras ocorrências com os dados originais.
* **Restauração ou Restore:** Execução de procedimento de restauração de dados a partir de um backup funcional.
* **Backup incremental**: Somente os arquivos novos ou modificados desde a última execução do procedimento de backup são copiados.
* **Backup completo:** Todos os dados são copiados durante o procedimento do backup.
* **Comite de Segurança da Informação e Privacidade (CSIP):** Comite responsável pela implementação e manutenção dos requisitos de Segurança da Informação e Privacidade da **Demarco**.
* **Desastre:** Incidente catastrófico que pode ocasionar a indisponibilidade de dados ou serviços.
* **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.
* **Responsável pelos dados**: (procurar definição nas normas existentes)

# Diretrizes

O backup é um controle fundamental para evitar Incidentes envolvendo a perda de dados e informações corporativas da **Demarco**. As seguintes diretrizes devem ser observadas para assegurar uma gestão adequada do ciclo de vida de backups:

## Criação de novos Backups

1. Anualmente, deve ser promovido pelo **CSIP** a discussão sobre o escopo de backup, como por exemplo, sua abrangência em relação aos todos os dados críticos para a empresa, banco de dados, arquivos importantes e sistemas;
2. Os colaboradores devem ser orientados de forma adequada sobre quais são as ferramentas de armazenamento que fazem parte do escopo de backup;
3. Durante a criação de novos processos, produtos, sistemas ou serviços, deve ser realizada análise para determinar se será necessário criar um backup para este novo ativo de informação da **Demarco**;
4. Para prosseguir com a criação de novos backups, a área de Infraestrutura e Segurança da Informação deverá ser acionada para avaliar se será possível utilizar alguma solução de backup já contratada ou se outra solução deverá ser adquirida ou criada;
5. Deve ser estabelecido e mantido pela área de Infraestrutura e Segurança da Informação um plano contendo a regularidade e frequência dos backups, bem como os métodos utilizados: se são incremental, diferencial ou completo.

## Armazenamento do Backup

1. Os backups devem ser armazenados em locais seguros e sempre que possível, em localidade e espaço físico diferente da fonte de dados original, visando a prevenção contra Incidentes como desastres naturais;
2. Deve ser definido um critério de redundância conforme a criticidade do backup;
3. Deve ser assegurado que as ferramentas utilizadas para a realização do backup possuam recurso de criptografia, para que os dados sejam protegidos em seu estado de repouso.

## Restauração e Manutenção do Backup

1. Solicitações de restauração do backup devem ser formalmente registradas junto à área de Infraestrutura e Segurança da Informação. Desde que solicitada pelo responsável pelos dados, não é necessária a aprovação para executar o procedimento de restauração. Caso o solicitante não seja o responsável pelos dados, deve-se obter a autorização do responsável ou de um diretor para a execução da restauração;
2. A restauração do backup em ambiente de produção somente deve ocorrer com a aprovação do responsável pela área de Infraestrutura e Segurança da Informação;
3. A permissão e acessos necessários para a execução de procedimentos de backup deve ser rigorosamente controlada;
4. Devem ser realizados testes de restauração anualmente, para assegurar que o backup é integro e confiável. Os resultados dos testes de restauração devem ser documentados, contendo no mínimo:

* Responsável;
* Data do teste;
* Breve descrição;
* Tipo de dado restaurado: somente arquivos, banco de dados etc.;
* Tempo necessário para a restauração completa;
* Principal objetivo;
* Passos realizados;
* Resultado.

1. Os testes de restauração do backup devem ser realizados em ambiente específico para testes;
2. Sempre que necessário, os procedimentos de backup devem ser atualizados para que reflitam de maneira exata as etapas necessárias para a execução de um backup ou restauração;
3. Um sistema de monitoramento automatizado deve ser mantido para assegurar que os backups foram realizados e alertar a ocorrência de falhas na execução de backups à área de Infraestrutura e Segurança da Informação. Sempre que possível, devem ser implementados sistemas para realização de testes automáticos de integridade do backup.

## Retenção e Descarte de Backup

1. Deve ser estabelecido, pelo CSIP e o responsável pelos dados, o tempo máximo de retenção do backup, sempre observando requisitos legais e de privacidade e segurança da informação;
2. Deve ser estabelecida política com período de retenção máxima para as caixas de correio eletrônico. Podem ser estabelecidas, pelos gestores de áreas, pastas com período de retenção superior ao máximo estabelecido pela caixa de correio, visando assegurar que as informações sejam mantidas pelo tempo adequado;
3. Durante o desligamento de colaborador, deve ser avaliado, junto ao gestor responsável, se será necessário obter uma cópia de segurança dos e-mails ou de pastas de arquivos específicas do colaborador. Os dados backupeados não devem ser mantidos por período superior a 90 (noventa) dias;
4. O descarte de mídias de backup deve ser realizado de forma segura, no mínimo através do uso de criptografia, software de sanitização ou destruição física da mídia, conforme Norma de Uso Aceitável de Ativos (NOR-SGSI-002). Estas medidas têm como principal objetivo assegurar que dados não possam ser recuperados através de softwares de restauração de dados.

# Papéis e Responsabilidades

## COMITE DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Assegurar que o escopo de backup esteja adequado às necessidades e requisitos do negócio;
2. Definir responsáveis pelos dados;
3. Definir tempo máximo de retenção de dados conforme leis aplicáveis.

## INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

1. Estabelecer e manter atualizado o plano de backup;
2. Criar e manter rotinas de backups de acordo com o escopo definido;
3. Assegurar o uso de ferramentas adequadas para a realização e monitoramento do backup;
4. Tratar alertas da ferramenta de monitoramento do backup;
5. Executar e documentar testes de backup;
6. Atender, conforme os requisitos desta norma, a solicitações de restauração de dados;
7. Criar e manter atualizados procedimentos para a criação ou restauração de dados.

## RESPONSÁVEIS PELOS SISTEMAS

1. Validar se os testes de recuperação foram bem-sucedidos.

# 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 | 21/08/2023 | CSIP | Criação da norma |
| 0.2 | 16/05/2024 | CSIP | Ajustes |
| 0.3 | 11/07/2024 | CSIP | Revisão Anual |