# Propósito

A Norma de Uso de Recursos Criptográficos **NOR-SGSI-009** complementa a Política de Segurança da Informação e Política de Proteção de Dados, definindo as diretrizes para o uso apropriado de recursos criptográficos para a proteção da disponibilidade, confidencialidade e integridade de dados e informações, além de apoiar a autenticidade e não-repúdio de ações.

# Escopo

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

# Glossário

* **Algoritmo criptográfico:** Algoritmo matemático cujas operações, parametrizadas por uma ou mais chaves, realizam a cifragem ou a decifragem dos dados.
* **Chave criptográfica:** Mecanismo que faz parte de um algoritmo criptográfico, que pode ser utilizado para realizar a cifragem ou decifragem de dados e, em alguns casos, verificar a identidade de uma entidade.
* **Criptografia:** É uma técnica utilizada para proteger a informação contra acesso indevido e falta de integridade. A criptografia baseia-se em dois processos, a encriptação – processo para que a informação legível seja transformada em informação cifrada através de algoritmos matemáticos; e a decriptação – processo inverso a encriptação, tornando –a informação acessível somente a um destinatário autorizado.

# Diretrizes

A criptografia é um controle essencial na manutenção confidencialidade e integridade de dados e informações processados no ambiente cibernético. Através deste recurso, podemos assegurar que somente pessoas autorizadas tenham acesso ao dado ou informação transmitidos. As seguintes diretrizes devem ser observadas:

## Uso de algoritmos criptográficos

1. Convém que sejam utilizados algoritmos criptográficos durante a transmissão/comunicação e armazenamento/repouso dos seguintes dados e informações:

* Dados pessoais;
* Dados pessoais sensíveis;
* Dados de crianças e adolescentes;
* Informações confidenciais ou restritas;

1. Os algoritmos criptográficos utilizados devem possuir alta capacidade de proteção (complexidade) e caso possuam vulnerabilidades ou forem ultrapassados não podem ser utilizados;
2. Convém que seja criado documento específico para a definição dos algoritmos permitidos;
3. Deverá ser estabelecida lista informando os algoritmos utilizados e a sua aplicação com base no tipo de dado/informação transferida e o sistema utilizado.

## Uso de certificados digitais

1. Os websites da **Demarco** que trafegarem dados e informações relevantes devem possuir certificado TLS em sua versão mais recente e segura, emitido por entidade certificadora confiável;
2. Certificados digitais podem ser utilizados internamente para a autenticação de usuários ou para a inspeção e filtragem de conteúdo trafegado pela rede.
3. Os certificados digitais utilizados, sejam eles de websites ou para uso em outras funções e sistemas deverão ser renovados, caso aplicável, antes de sua data de vencimento e deve ser mantido monitoramento destes prazos;

## Gestão de chaves criptográficas

1. Quando chaves criptográficas forem utilizadas, estas devem ser adequadamente protegidas contra vazamento, modificação inapropriada e destruição;
2. Convém que seja utilizado cofre de senhas com acesso restrito a pessoas que necessitam das chaves criptográficas;
3. As chaves criptográficas utilizadas devem ser diferentes para cada sistema/função executada;
4. Procedimentos específicos deverão ser elaborados para situações em que for necessário realizar a alteração, substituição ou destruição de chaves criptográficas;
5. Chaves de criptografia que possuírem período de validade ou tempo de substituição definido devem ser monitoradas.

# Papéis e Responsabilidades

## INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

1. Estabelecer e manter lista para os algoritmos de criptografia utilizados e os sistemas em que são utilizados;
2. Estabelecer e manter lista definindo os tipos de algoritmos de criptografia permitidos para uso;
3. Assegurar que os websites da **Demarco** possuem certificados digitais válidos;
4. Estabelecer e manter o monitoramento de chaves de criptografia e dos certificados digitais de websites pelo qual for responsável;
5. Estabelecer e manter procedimentos específicos para alteração, substituição ou destruição de chaves criptográficas pelo qual for responsável.

## RESPONSÁVEIS PELOS SISTEMAS

1. Avaliar e aplicar o uso de recursos criptográficos nas aplicações da **Demarco**;
2. Estabelecer e manter procedimentos específicos para alteração, substituição ou destruição de chaves criptográficas pelo qual for responsável;
3. Estabelecer e manter o monitoramento de chaves de criptografia pelo qual for responsável;

## COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Apoiar as áreas na identificação de fluxos de informação ao qual a criptografia precisa ser aplicada.

# Gestão de versões

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 10/10/2023 | CSIP | Criação da política |
| 0.2 | 08/07/2024 | CSIP | Revisão Anual |