Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Política de Criptografia

Objetivo

Estabelecer e definir o gerenciamento de controles criptográficos ao enviar ou receber informações em meios eletrônicos, visando proteger a confidencialidade, a integridade e a rastreabilidade das informações da Instituição.

Visão Geral

A criptografia tem como objetivo escrever em cifras, que são obtidas através de um conjunto de operações matemáticas que transformam um texto claro em um texto cifrado.

A utilização de controles criptográficos nos documentos da Instituição visa manter a confidencialidade das informações e dados mantidos pela Instituição, bem como a integridade e a autenticidade da informação.

1. Diretrizes da Utilização de Criptografia

Todas as informações confidenciais devem ser devidamente criptografadas através dos procedimentos previstos nesta política, especialmente no que diz respeito aos dispositivos móveis utilizados pela Instituição, tais como laptops, mídias de armazenamento removível e mídias de backup.

Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

As senhas para criptografia de informações devem ser protegidas e gerenciadas seguindo os controles de segurança definidos na Política de Segurança da Informação e na Política de Senhas.

Ao utilizar sistemas de troca de informações, como e-mails ou outros sistemas de transferência de dados, deve-se empregar os mecanismos de criptografia adequados e autorizados pelo Responsável pela Segurança da Informação.

Ao criptografar informações, uma cópia das chaves de criptografia deve ser mantida em um local seguro, para que a recuperação de informações criptografadas seja viável em caso de ausência temporária ou permanente do responsável das informações criptografadas.

A criptografia de informações com mecanismos não autorizados pelo Responsável pela Segurança da Informação ou a divulgação não-autorizada de chaves de criptografia são condutas expressamente proibidas.

O Responsável pela Segurança da Informação deve documentar, divulgar e atualizar os procedimentos para criptografar informações, incluindo as atividades de geração, gerenciamento e proteção das chaves utilizadas para a criptografia de informações.

Os integrantes responsáveis pelas informações, processos, procedimentos ou atividades que envolvam o processamento, transmissão ou armazenamento de informações por meio eletrônico devem solicitar, por meio eletrônico, através dos

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

procedimentos definidos pelo Responsável pela Segurança da Informação, a criptografia de informações classificadas como restritas ou confidenciais que estiverem sob sua responsabilidade.

O Responsável pela Segurança da Informação da Instituição determinará os mecanismos de criptografia de dados que melhor se adequam às necessidades específicas de cada tipo de informação, incluindo metodologias de criptografia assimétrica para a maioria das aplicações.

No processo de criptografia utiliza-se uma chave (também chamada de senha), que faz parte da segurança do processo. Existem dois tipos de procedimentos de criptografia baseados em chaves: os procedimentos de criptografia simétrica ou de chave privada e os procedimentos de criptografia assimétrica ou de chave pública.

2. Criptografia Simétrica

A encriptação de uma determinada mensagem, ou seja, o processo em que um conteúdo é criptografado, é baseado em 02 componentes: um algoritmo e uma chave de segurança.

O algoritmo trabalha junto com a chave, de forma que eles tornam um conteúdo sigiloso com um conjunto único de regras.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

A criptografia simétrica faz uso de uma única chave, que é compartilhada entre o emissor e o destinatário de um conteúdo. Essa chave é uma cadeia própria de bits, que vai definir a forma como o algoritmo vai cifrar um conteúdo.

Como vantagem, a criptografia tem uma boa performance e a possibilidade de manter uma comunicação contínua entre várias pessoas simultaneamente. Caso a chave seja comprometida, basta efetuar a troca por uma nova, mantendo o algoritmo inicial.

A segurança de um sistema de criptografia vai variar conforme o tamanho da chave utilizada. A Instituição deve possuir sistemas de criptografia baseados em RC2, que utiliza o protocolo S/MIME, que possui uma chave variável entre 8 e 1.024 bits. Assim, as chances de alguém conseguir decifrar um conteúdo criptografado da Instituição por meio de algoritmos de força bruta diminui consideravelmente.

Entretanto, deve-se observar que a criptografia simétrica possui falhas graves de segurança. A gestão de chaves, por exemplo, torna-se mais complexa conforme o número de pessoas com que se comunica aumenta. Para cada N usuários, são necessárias N^2 chaves. A criptografia simétrica também não possui meios que permitem a verificação da identidade de quem envia ou recebe um conteúdo. Além disso, não há como garantir o armazenamento em ambientes confiáveis das chaves de segurança.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

3. Criptografia Assimétrica

A criptografia assimétrica, também conhecida como criptografia de chave pública, é baseada em 2 tipos de chaves de segurança — uma privada e a outra pública. Elas são usadas para cifrar mensagens e verificar a identidade de um usuário.

Desta forma, a chave privada é usada para decifrar mensagens, enquanto a pública é utilizada para cifrar um conteúdo. Assim, qualquer pessoa que precisar enviar um conteúdo para alguém precisa apenas da chave pública do seu destinatário, que usa a chave privada para decifrar a mensagem.

Esse sistema simples garante a privacidade dos usuários e aumenta a confiabilidade de uma troca de dados e deve ser privilegiado pela Instituição. Afinal, como o número de pessoas com acesso à chave privada é restrito, a chance de comprometimento das comunicações da Instituição é reduzida de forma considerável.

Para a criptografia assimétrica, a Instituição utilizará o sistema RSA, que é baseado na multiplicação de números primos de grande escala para a geração de uma chave pública, impossibilitando a quebra do algoritmo por meio de força bruta.