IT-ONE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PC12 - Política de Criptografia

1. HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
02/06/21	1.0	Criação do documento	Peterson Pires

INTRODUÇÃO

Hoje em dia podemos afirmar com toda certeza que estamos conectados a internet 24 horas por dia e 7 dias por semana. Na verdade, a internet se tornou tão essencial para nós que quando perdemos o acesso a internet deixamos de fazer muitas tarefas. Por exemplo, movimentações bancárias, envio/recebimento de email, compras on-line, entre tantos outros serviços. Mas ao mesmo tempo que a internet se tornou um grande facilitador, também trouxe consigo algumas 'armadilhas' que muitas vezes geram grandes transtornos para seus usuários. E uma maneira de tentar minimizar este risco para os usuários é a utilização de encriptação nas comunicações e transferências de dados que fazemos na internet e nas redes locais das empresas e até mesmo nas nossas redes domésticas.

OBJETIVO

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e integridade da informação.

ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da IT-One, quais sejam: funcionários servidores ou comissionados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da IT-One. Todos esses colaboradores serão tratados nesta política como usuários

DIRETRIZES

1. Identificar o nível de proteção exigido pelos ativos, levando em consideração uma avaliação de risco, para que seja possível definir a força e a qualidade do algoritmo de criptografia requerido.

2. Utilizar criptografia para proteger as informações críticas transportadas em dispositivos móveis, mídias removíveis ou através de redes de computadores.

3. Utilizar certificados SSL assinados por autoridades certificadoras confiáveis em sistemas web, para garantir que as informações acessadas ou transmitidas não sejam interceptadas por pessoas não autorizadas.

4. Utilizar assinaturas digitais ou códigos de autenticação para validar a autenticidade ou integridade de informações críticas armazenadas ou transmitidas.

5. Os algoritmos criptográficos e o tamanho de chaves devem ser selecionados de acordo com o nível de criticidade das informações e dos sistemas que a suportam, para que não ocorram impactos desnecessários tanto de falta de segurança, quanto de segurança excessiva (por exemplo, causando lentidão demasiada no acesso a informações simples e pouco críticas).

6. Todas as chaves criptográficas devem ser protegidas contra modificação e perda.

7. As chaves privadas e secretas devem ser protegidas contra uso ou divulgação não autorizada.

8. As chaves devem ser distribuídas de forma segura para os usuários devidamente autorizados.

9. Revogar chaves comprometidas ou aquelas utilizadas por usuários que não possuírem mais autorização para tal utilização.