

O que é criptografia: tudo o que você precisa saber

Para entender **o que é criptografia** e os benefícios que ela pode trazer para o negócio da sua empresa, você precisa saber como se deu o surgimento desse termo.

O termo criptografia surgiu da fusão de duas palavras gregas: “*kryptós*” e “*gráphein*”. Elas significam respectivamente “oculto” e “escrever”.

O envio e recebimento de informações sigilosas é uma necessidade muito antiga, que existe há centenas de anos.

E, com essa necessidade, a criptografia tornou-se uma ferramenta essencial para que apenas o emissor e o receptor tenham acesso livre às informações, sem sofrer com possíveis [riscos](#) de segurança.

O primeiro uso documentado de criptografia surgiu há cerca de 1900 anos antes de Cristo, no Egito, quando foram usados hieróglifos que não correspondiam ao padrão existente.

O uso de criptografias durante períodos de guerra é comum. As agências de inteligência criam suas próprias criptografias para se comunicar, **evitando que suas mensagens possam ser interceptadas e lidas**.

No filme “O Jogo da Imitação”, o ator Benedict Cumberbatch vive o matemático britânico Alan Turing, responsável por decifrar o código do Enigma.

Enigma era o sistema criptográfico usado pelas forças alemãs para transmitir mensagens a seus homens no campo de batalha durante a Segunda Guerra Mundial.

E muitos casos têm trazido maior atenção para esse tema, devido à preocupação das empresas em proteger suas informações contra [vazamento de dados](#) e outros [crimes digitais](#).

Agora que você sabe sobre o que é criptografia e da sua necessidade, continue lendo este post para entender mais a fundo sobre o assunto.

O que é Criptografia?

A criptografia trata-se de um conjunto de regras que visa codificar a informação de modo que só o seu emissor e receptor consigam decifrá-la.

Várias são as técnicas usadas e, com o passar do tempo, elas sofrem modificações visando seu aperfeiçoamento. Além do surgimento de novas práticas mais seguras.

A prática criptográfica visa **reforçar a segurança de uma mensagem**, ou de um arquivo, “embaralhando” o seu conteúdo.

Para criptografar ou descriptografar uma mensagem, você também precisa da **chave certa para decodificá-la**. É o modo mais eficaz para ocultar comunicações através de informações em código, onde o remetente e o destinatário têm a chave para decifrar os dados.

E com o surgimento dos meios digitais, os métodos precisaram se tornar mais avançados e eficazes.

Na tecnologia da informação, a técnica usada é chamada “Chave Criptográfica”. Trata-se de um conjunto de *bit's* baseado em um algoritmo capaz de realizar a codificação e decodificação das informações.

De forma simples, se o receptor da mensagem usar uma chave diferente e incompatível com a do emissor ele não conseguirá acessar a informação recebida.

Existem dois métodos de criptografia de chaves: **criptografia simétrica e assimétrica**. Falaremos delas logo a seguir.

Com o uso das chaves, um emissor pode usar o mesmo método para vários receptores. Basta fornecer uma chave diferente para cada um dos receptores.

Você não precisa utilizar de outra metodologia para entregar diferentes chaves a diferentes receptores.

Desse modo, você permite a visualização segmentada de um conteúdo para cada pessoa que possua acesso.

E caso alguém perca a chave ou ocorra a exposição dela devido a alguma interceptação, você pode trocar a chave sem alterar o seu algoritmo, evitando assim algum prejuízo.

Chave Criptográfica

Entender o que é chave criptográfica e a sua aplicação é fundamental para você conhecer melhor o que é criptografia. Pois essa pode ser uma **metodologia usada para proteger** a área de TI da sua empresa.

Essa metodologia é aplicada por meio de um valor secreto que modifica um algoritmo de encriptação. Para facilitar o seu entendimento, vamos imaginar um cenário próximo ao seu cotidiano

A fechadura de uma porta possui uma série de pinos. E cada um desses pinos tem múltiplas posições possíveis.

Quando você coloca a chave na fechadura, cada um dos pinos é movido para uma posição específica. E a chave é quem determina as posições dos pinos necessárias para a fechadura ser aberta.

Mencionamos, anteriormente, os dois métodos de criptografia de chaves existentes. Vamos esclarecê-los agora para você compreender melhor o que é criptografia.

A **criptografia simétrica**, também conhecida como criptografia de chave secreta, trata-se de uma chave única que é usada tanto para criptografar como para decodificar uma mensagem.

Ou seja, uma chave privada é gerada e usada nas duas pontas da transmissão: na emissão, por aquele que emite a mensagem, e na recepção, por aquele que a recebe.

A criptografia assimétrica, ou criptografia de chave pública, usa o que é chamado de um “par de chaves”, uma pública e a outra privada.

Nesse caso uma chave pública é gerada e usada para criptografar a mensagem, enquanto que uma chave privada é gerada e entregue ao receptor para decodificá-la.

Logo, são chaves distintas que possuem a função única de criptografar ou de decodificar o conteúdo transmitido.

Essas chaves são geradas por algoritmos que criam uma sequência de caracteres específica para cada processo. Elas podem ter tamanhos distintos e, quanto maiores, mais seguras elas se tornam.

Atualmente, existem incontáveis protocolos de proteção utilizados. Eles estão presentes a todo instante, como quando você digita seu usuário e senha para acessar algum serviço da web, por exemplo.

Protocolos como 3DES, RC AES, TLS e SSL são alguns dos mais comuns nos dias de hoje.

Por que eu deveria usar a criptografia?

Você já sabe **o que é criptografia** e quais são os principais métodos utilizados no meio digital, mas, talvez ainda não consiga pensar em bons motivos para usar essa proteção.

Ela pode ser usada inicialmente visando proteger a sua identidade e privacidade, além da identidade e privacidade dos colaboradores da sua empresa e clientes.

Porém, a criptografia vai além disso. A seguir, separamos para você alguns usos da criptografia para o seu negócio e o que pode ser feito com ela.

Utilidades da criptografia

- Proteger informações enviadas por e-mail;
- Proteger dados de backup em nuvem (*cloud*);
- Proteger arquivos de acesso indevido;
- Proteger dados de navegação.
-

Possibilidades da criptografia

O uso da criptografia, portanto, permite que você:

- Proteja os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- Crie uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- Proteja seus *backups* contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- Proteja as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.