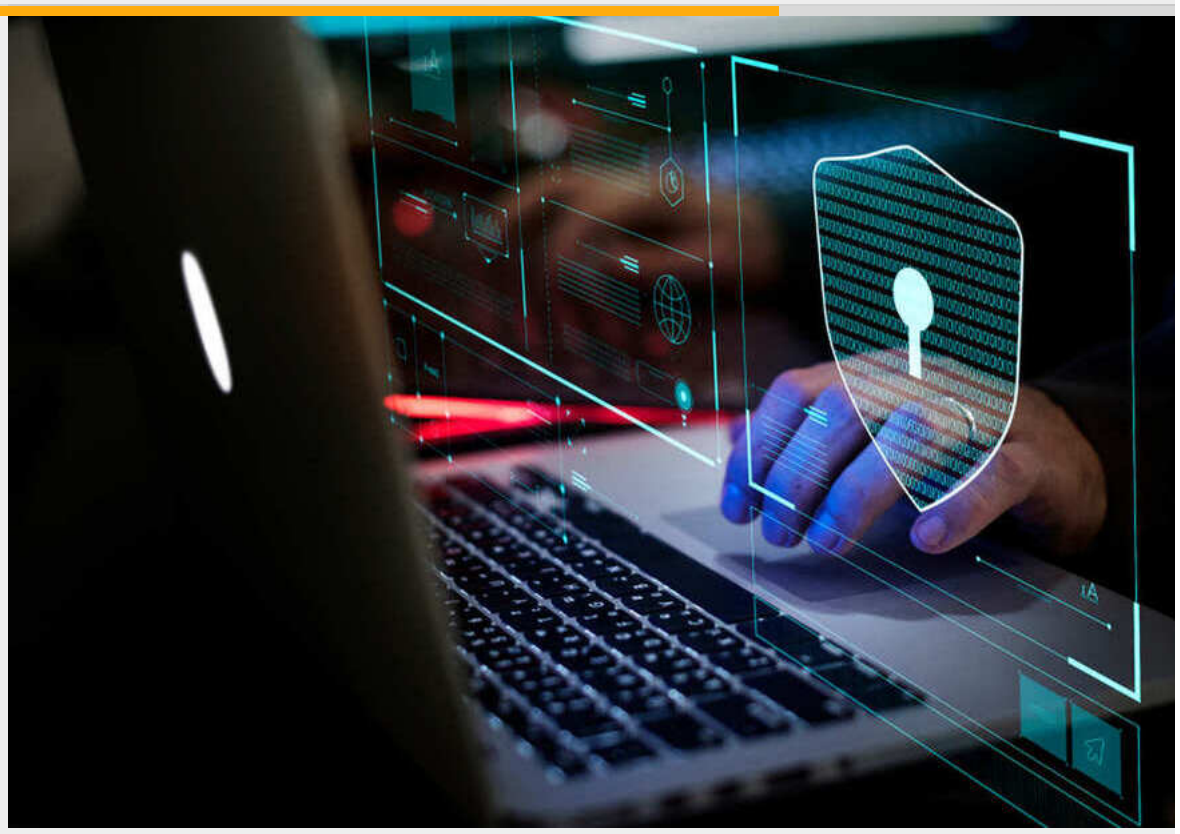


GESTÃO DE NEGÓCIOS

Criptografia: tipos, exemplos e importância nas empresas

EQUIPE TOTVS | 15 MARÇO, 2022

A criptografia é parte do mundo dos negócios e da rotina das pessoas atualmente — e tudo indica que se tornará ainda mais importante com o tempo. Esse processo elimina os riscos de terceiros acessarem dados e informações digitais, codificando-os.

E sua eficiência é comprovada: entre as estratégias de segurança de dados, a criptografia é uma das mais populares.

Não à toa, canais como WhatsApp e Telegram mantém as conversas de seus usuários protegidas sob uma forte camada de criptografia.

Acontece que, após diversos casos de vazamento de dados ocorridos com empresas, a segurança dessas informações passou a ser prioridade para diversas companhias.

A partir desses eventos, a Lei Geral de Proteção de Dados foi criada, visando proteger os dados pessoais dos usuários e exigindo que as empresas tenham esse cuidado.

Por isso, neste artigo, vamos falar sobre o que é criptografia de dados, como funciona e os motivos pelos quais é importante que seu negócio considere a utilização desta técnica.

Que tal conferir tudo que abordaremos em nosso guia completo sobre o assunto? Vamos lá:

Vamos lá? É só seguir a leitura conosco!

O que é e como funciona a criptografia de dados?

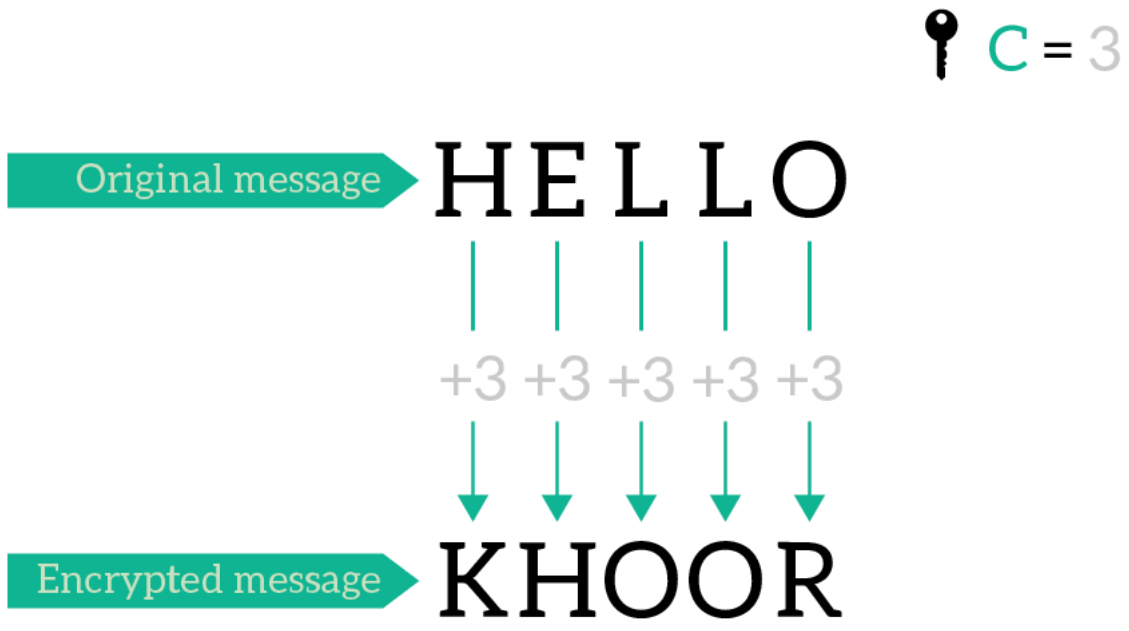
A criptografia é um conjunto de técnicas pensadas para proteger uma informação de modo que apenas o emissor e receptor consigam compreendê-la. É utilizada em comunicações digitais, como na troca de mensagens ou em pagamentos online.

Em geral são usados algoritmos para realizar o codificação e para decodificação é necessário ter acesso à chave utilizada no primeiro processo.

O princípio básico da criptografia é o seguinte: permitir que duas pessoas compartilhem secretamente mensagens entre si, sem que elas sejam acessadas por terceiros.

Normalmente, sistemas criptográficos usam texto cifrado (ciphertext) para disfarçar texto simples (plaintext), com base em uma chave.

Pegamos um exemplo da Tensumo para ilustrar exatamente como funciona:



Neste caso, trata-se de uma criptografia assimétrica (ou de chave única), em que as chaves para descriptografar são as mesmas para os dois extremos de um canal de comunicação.

Existe também a criptografia assimétrica (chave pública), em que cada extremidade conta com suas chaves — logo mais explicaremos em detalhes como funciona!

O funcionamento da criptografia é um pouco complexo para quem não é da área, mas vamos explicar de forma simplificada:

Basicamente, a criptografia envolve a codificação de informações importantes para que elas não caiam nas mãos de pessoas erradas — como no exemplo acima.

Para isso, um algoritmo é implementado para codificar os dados, fazendo com que só pessoas autorizadas possam decodificá-los e ter acesso ao seu conteúdo.

Chaves e protocolos

Atualmente, a base da criptografia simétrica e assimétrica são as chaves, que podem ser utilizadas para criptografar e também para descriptografar informações.

Como explicamos, quando a chave é simétrica, pode ser usada nas duas pontas da transmissão. Já quando é assimétrica, as chaves de criptografia e descriptografia são diferentes.

Alguns exemplos de protocolos são: DES, 3DES, AES, IDEA, RC4, TLS e SSL.

Existem também protocolos de criptografia que não utilizam chaves, chamados de algoritmos de HASH.

Eles transformam um texto, de qualquer tamanho, em uma sequência de caracteres, de tamanho fixo, única para identificar o texto original.

Pode ser utilizada como uma espécie de dígito verificador, mas que não permite a reversão desse código para o texto original.

Eles são usados a todo tempo por nós, quando os sistemas armazenam as nossas senhas, ou comparam o que digitamos com a senha armazenada. Alguns exemplos de protocolos são: MD5 e SHA-256.

Conheça a história da criptografia

É comum vincular a palavra “criptografia” à tecnologia, sistemas bancários e de segurança, bem como à matemática avançada e algoritmos. No entanto, a origem da criptografia é milenar.

A prática de codificar informações para mantê-las em segurança é, na verdade, feita desde a Antiguidade.

Estima-se que essa estratégia surgiu há cerca de 1.900 anos antes de Cristo, no Egito.

Você já percebeu que a humanidade, mesmo dotada de várias tecnologias, não conseguiu decodificar vários documentos e artefatos históricos do nosso passado?

Um exemplo é o Rongorongo, tábuas de madeira encontradas na Ilha de Páscoa e demarcadas com hieróglifos que, até hoje, não foram decifradas.

Trata-se de um mistério porque, por ser um arquipélago isolado, acredita-se que o conteúdo das tábuas é composto de conhecimentos próprios. Ou seja, um idioma completamente novo.

Já um exemplo da origem da criptografia que foi desvendada é a famosa Pedra de Roseta.

Encontrada no Egito em 1799, por tropas francesas comandadas por Napoleão Bonaparte, o pedaço de granito é coberto pelo mesmo texto, mas em 3 diferentes grafias/idiomas.

Eram eles: hieróglifos egípcios, grego antigo e demótico.

A presença das 3 grafias ajudou os estudiosos a traduzirem o texto em sua totalidade.

Posteriormente, isso ampliou a compreensão sobre outros documentos e artefatos egípcios, já que proporcionou entendimento sobre a língua egípcia grifada em hieróglifos.

Quais são os tipos de criptografia?

A confidencialidade de dados é o maior princípio da criptografia: e a forma de conquistá-la é com a encriptação de informações.

Esse processo, muitas vezes confundido com a criptografia, não é um sinônimo para a mesma.

A encriptação é parte da criptografia: trata-se especificamente do embaralhamento de informações para que elas sejam ilegíveis para qualquer um que não possua a chave correta.

Nesse sentido, quando falamos de criptografia, normalmente nos referimos a dois tipos: simétrico e assimétrico. Que tal conhecê-los?

Criptografia simétrica

A criptografia simétrica é o tipo mais tradicional e provavelmente o sistema que as pessoas estão mais familiarizadas.

Nele, a criptografia é realizada com base em uma única chave — que é utilizada para criptografar e também descriptografar uma mensagem.

O exemplo da imagem que postamos anteriormente ilustra bem a criptografia simétrica:

A chave é 3 e a mensagem original, "*HELLO*", foi criptografada como "*KHOOR*".

Ou seja, para descriptografar, basta aplicar a mesma chave/lógica, que é a troca de cada letra para a terceira letra posterior a ela no alfabeto.

Sua principal aplicação é na proteção de dados em repouso, como em bancos de dados ou discos rígidos — isso porque é necessário contar com um canal seguro para transmitir a mensagem.

Entre seus principais benefícios, a criptografia se destaca por ser mais rápida e por ser ideal para proteger dados que vão ficar em único local.

Porém, como desvantagem, destaca-se a dificuldade de distribuição segura de chaves.

A lógica é: se há um canal seguro para passar as chaves, porque não passar a mensagem de uma vez?

Assim, qualquer pessoa que interceptar e ler a chave, poderá tranquilamente descriptografar a mensagem.

Criptografia assimétrica

A criptografia assimétrica utiliza duas chaves diferentes para criptografia e descriptografia de um dado.

Vamos direto ao ponto:

A primeira chave é uma chave pública usada para criptografar uma mensagem e a segunda é uma chave privada utilizada para descriptografá-la.

O principal a se entender é que apenas uma chave privada pode descriptografar as mensagens criptografadas por uma chave pública.

A criptografia assimétrica é aplicada em várias operações do dia a dia, como assinatura eletrônica, envio de e-mails ou mesmo realizar uma conexão remota a um sistema privado.

O próprio protocolo de segurança do seu navegador (repare no "*https://*" antes da URL) é um exemplo de criptografia assimétrica.

O principal benefício da criptografia assimétrica é que as pessoas não precisam de nenhum esquema de segurança específico para trocar mensagens com confidencialidade.

Digamos que Gabriel queira se comunicar com Jorge usando criptografia assimétrica. Ele vai utilizar a chave pública de Jorge para criptografar a mensagem.

Assim, depois de receber a mensagem, Jorge usa sua chave privada para descriptografar as informações.

Dessa forma, ninguém pode interceptar e desvendar a mensagem entre os dois — e não é necessário que haja um canal seguro para a troca de chaves.

Hashing

Hashing é uma metodologia criptográfica que embaralha os dados de forma que sejam sequer reconhecíveis. A única diferença para o tipo simétrico e assimétrico, é que o hashing não foi projetado para ser reversível.

Ele fornece um resultado de tamanho fixo, conhecido como hash.

É uma função matemática aplicada sobre um determinado tipo de dado, que gera assim outro número único.

O hashing é utilizado na:

- Geração de assinaturas digitais;
- Análise e verificação da validade e integridade de arquivos digitais.

A finalidade do hashing não é necessariamente ocultar o conteúdo de uma mensagem, por exemplo, mas sim verificar sua integridade.

Uma das maneiras de fazer essa verificação é calculando o hash de um arquivo ou mensagem. Caso o resultado (o hash) seja o mesmo, quer dizer que o arquivo é o mesmo.

É desse jeito que o hashing é utilizado — junto de outros mecanismos de verificação — para garantir a validade jurídica de arquivos assinados digitalmente, por exemplo.

Onde encontramos a criptografia?

Hoje, a criptografia é muito mais comum do que se imagina. Os pagamentos digitais e por aproximação utilizam a criptografia para concretizar pagamentos.

Cartões ou dispositivos mobile que utilizam a tecnologia NFC, por exemplo, podem trocar informações com terminais de pagamentos para que o dinheiro saia de uma conta e vá para outra.

Essa troca de dados precisa ser protegida para que nenhum terceiro próximo o suficiente para interceptar a operação descubra as informações sigilosas (como a conta, senha, valores, etc).

Na verdade, a criptografia por trás de uma operação financeira como essa esconde totalmente a identidade do consumidor.

Outro exemplo é a criptografia de e-mails, que assegura que o conteúdo dos e-mails fique protegido de qualquer um que não faça parte da conversa.

Se alguém de fora, um terceiro, procura ler um conteúdo de um e-mail que não faz parte, ele apenas vai acessar uma forma criptografada do mesmo — que não é legível por um humano.

Apenas quem faz parte da conversa (ou possui acesso aos e-mails envolvidos nela) pode ler o conteúdo em sua totalidade.

Além disso, como mencionamos, redes sociais como o WhatsApp e o Telegram (específicos para troca de mensagens), bem como o Instagram, utilizam protocolos de criptografia.

Quais são os algoritmos de criptografia mais conhecidos?

A criptografia, apesar de ser resumida em poucos tipos, possui vários algoritmos: tanto simétricos, quanto assimétricos.

Talvez você se pergunte: "*porque existem tantos algoritmos diferentes?*"

Bom, os motivos são variados, como para o que o algoritmo é aplicado. Além disso, alguns deles são "evoluções" de outros, corrigindo falhas ou brechas encontradas.

Que tal conferir os principais?

Criptografia RC4

A criptografia RC4, sigla para Rivest Cipher 4, é uma cifra de fluxo (stream cipher) criada no fim dos anos 1980, um algoritmo simétrico.

Essa cifra opera nos dados um byte por vez, de modo a criptografar esses dados.

O RC4 é uma das cifras de fluxo mais usadas, tendo sido usado nos protocolos Secure Socket Layer (SSL) — hoje conhecido como Transport Layer Security (TLS).

Hoje, esse algoritmo não é tão utilizado, pois apresentou algumas vulnerabilidades, que permitiram que usuários quebrassem a chave em questão de um minuto.

Criptografia Twofish

Outro tipo de criptografia simétrica é a Twofish, uma evolução da Blowfish — sendo assim, apenas uma chave de 256 bit é necessária.

É bastante útil e segura, sendo finalista de uma competição do Instituto de Tecnologia e Ciências Nacional americano, que buscava uma criptografia [illegible] a DES.

Criptografia DES

A criptografia DES, sigla para Data Encryption Standard, é também um tipo de chave simétrica — um dos primeiros que foi criado, datando do começo da década de 1970, por um time de desenvolvedores da IBM.

O algoritmo converte texto simples em blocos de 64 bits em texto cifrado, com chaves 48 bits.

Por conta do tamanho pequeno da chave, ele é considerado inseguro para várias aplicações atualmente.

Hoje, o DES foi substituído pelo AES.

Criptografia 3DES

Derivada do DES, a criptografia 3DES (ou Triplo DES) se tornou popular nos anos 1990 — muito embora hoje já não seja uma unanimidade.

Além disso, vale mencionar, ele se tornará obsoleto a partir de 2023.

Sua diferença para o antecessor é que utiliza 3 chaves de 64 bits.

Criptografia RSA

Já a criptografia RSA é um tipo assimétrico. A sigla diz respeito ao nome de seus criadores, Rivest-Shamir-Adleman.

Ele é muito utilizado hoje em dia e seu funcionamento tem a mesma explicação da criptografia assimétrica.

Ou seja, é baseado na utilização de uma chave pública para criptografar dados e em uma chave privada para descriptografá-los.

Criptografia AES

Já a criptografia AES ou Advanced Encryption Standard é um tipo de cifra que protege a transferência de dados online.

É um dos melhores e mais seguros protocolos de criptografia e é utilizado em incontáveis aplicações.

Na prática, é uma chave simétrica, pois utiliza a mesma chave para criptografar e descriptografar o conteúdo.

Ele também usa o algoritmo SPN (rede de permutação de substituição), aplicando várias rodadas para criptografar dados.

Essas rodadas de criptografia são a razão do alto nível de proteção do AES: se alguém quiser quebrar a criptografia, precisará fazê-lo por várias "rodadas".

Além disso, a criptografia AES conta com 3 tamanhos diferentes de chaves, partindo de 128 bits, 192 bits e 256 bits.

Anonimização, pseudonimização e criptografia

Você sabe qual é a relação entre anonimização, pseudonimização e criptografia? É importante compreender esses conceitos — e como eles se envolvem — para entender como a criptografia funciona. Vamos lá?

A anonimização no contexto da proteção de dados significa desassociar informações de indivíduos.

Portanto, existe a informação, mas ela não pode ser relacionada a uma determinada pessoa ou organização.

Nesse tipo de situação, pode-se utilizar os algoritmos de HASH mencionados anteriormente.

A pseudonimização também é uma forma de não atribuir informações a indivíduos, sem recorrer a informações suplementares. Isso é feito a partir de um tratamento de dados que garante a desassociação.

Porém é um processo reversível, podendo ser futuramente atrelado aos dados para voltar a identificação do indivíduo.

Neste tipo de situação, pode ser utilizada a criptografia simétrica ou assimétrica, sendo que a chave de criptografia se faz necessária para vincular os dados à pessoa a qual o dado faz referência.

É, portanto, um jeito mais confiável de tratar dados pessoais.

Esses três termos não são sinônimos, no entanto, a criptografia pode ser utilizada por uma empresa para fazer a anonimização ou a pseudonimização de dados.

Qual a importância da criptografia nas empresas?

Depois de escândalos de utilização indevida de dados (como o caso da Cambridge Analytica, que utilizou dados do Facebook) ficou clara a necessidade de criação de legislações que protegessem os interesses dos titulares de dados pessoais.

Diversos casos envolvendo exposição de dados já ocorreram e deixaram tanto pessoas quanto empresas prejudicadas.

Por esse motivo, foi criada a Lei Geral de Proteção de Dados, que visa garantir a segurança das informações coletadas pelas organizações através de medidas que precisam ser adotadas.

Sendo assim, a criptografia é uma boa alternativa — entre outras medidas que devem ser tomadas — para manter a segurança dos dados, além de p da empresa, que é tão importante para a conquista de novos neg

Veja outros benefícios de proteger as informações do seu negócio.

Processos sigilosos

Com a criptografia é possível garantir que todos os processos sigilosos da empresa (transações bancárias, dados de clientes, informações de colaboradores) sejam feitos com mais segurança.

Caso esse tipo de informação vaze, pode acarretar grandes prejuízos financeiros para a companhia. Por isso, o ideal é contar com meios seguros para efetuar essas transações.

Assim, ao realizar ou receber pagamentos, o processo poderá ser feito sem a preocupação de que pessoas não autorizadas tenham acesso a essas informações.

Proteção no envio e no recebimento de dados

Uma das formas mais comuns de vazamento de informações é por meio do trânsito de dados.

Quando uma empresa envia dados estratégicos em código criptografado, apenas quem está recebendo-os e possui a chave para codificar a mensagem poderá ter acesso a essas informações.

O processo também protege o titular do dado e a empresa, uma vez que a exposição e a utilização indevida desses dados pode acarretar em danos à imagem da empresa, multas e processos judiciais.

Por esse motivo, proteger o tráfego de dados é essencial para que a empresa possa garantir a integridade deles.

Segurança de informações

Desde informações de clientes a dados sobre estratégias, a maioria das empresas possui dados que não devem ser divulgados. No caso de dados pessoais de clientes, isso representaria um processo judicial para a companhia.

Para respeitar a legislação e manter a empresa protegida contra ataques, é preciso utilizar uma tecnologia que garanta essa segurança.

Isso pode ser feito por meio da encriptação de dados e outros métodos combinados.

Integridade dos dados

Uma maneira de proteger a integridade dos seus dados é através da criptografia, que assegura o conteúdo de uma mensagem ou arquivo através de algoritmos avançados.

Assim, é possível manter o sigilo das informações, bem como garantir que nenhum dado seja acessado por um terceiro não autorizado.

Garantia de conformidade

Manter-se à par das diretrizes de compliance digital — especialmente no que diz respeito à segurança de dados dos seus clientes — envolve o uso da criptografia.

Através dela, é possível alinhar-se aos padrões exigidos em lei, pelo mercado e fornecedores, de modo a evoluir a governança de informações.

Segurança na nuvem

Com cada vez mais usuários e empresas utilizando os recursos de cloud computing, é preciso cercar-se de maneiras de proteger os dados.

Afinal, por serem acessados de qualquer dispositivo, é essencial criptografá-los para garantir sua integridade.

Assegura a propriedade intelectual

Dados em repouso, especialmente arquivos que sejam parte de sua propriedade intelectual (seja de pessoa física ou da sua empresa), ganham um fator a mais de segurança ao serem criptografados.

Assim, é possível protegê-los de ações criminosas, como roubos com intenção de uso ou comercialização não autorizada.

Como é feita a criptografia?

Fazer uma criptografia vai depender do objetivo que você tem em mente. No caso de uma empresa, o uso de um servidor de e-mails como o Gmail, por exemplo, já garante que as comunicações por esse canal estarão criptografadas.

Até esse ponto, você já aprendeu que a criptografia depende de alguns fatores. Existem serviços que o fazem automaticamente.

Mas se você quiser criptografar alguns contratos e armazená-los na nuvem da sua empresa?

Em geral, utiliza-se algum software próprio para a tarefa.

Além disso, a empresa pode contar com um sistema de gestão que assegure a proteção aos dados com uso de algoritmos criptográficos.

Assim, todas as informações da empresa — ou àquelas utilizadas na ferramenta — estarão protegidas de terceiros maliciosos.

Criptografia: dúvidas frequentes

E agora, antes de finalizar esse conteúdo, que tal descobrir algumas respostas objetivas a dúvidas comuns sobre o tema? Separamos algumas perguntas que ouvimos de clientes e lemos de nossos leitores aqui no blog, continue para saber mais!

Quais são os conceitos básicos de criptografia?

Os princípios que denotam o conceito de criptografia são a confidencialidade, integridade, autenticidade e irretratabilidade.

Qualquer informação pode ser criptografada?

Sim, basicamente qualquer informação legível pode ser criptografada.

Ao longo do guia completo, nosso foco foi em discutir a criptografia para texto simples, mas é possível encriptar qualquer dado digital, como uma imagem ou áudio, por exemplo.

O que é criptografia de ponta a ponta?

A criptografia de ponta a ponta (*end-to-end encryption* ou E2EE) é um tipo de proteção à informações durante uma troca de mensagens — ela acontece no WhatsApp, por exemplo.

Assim, permite que apenas o remetente e o destinatário das mensagens possam acessá-las (e ninguém mais, nem mesmo a própria dona do aplicativo).

Qual a diferença entre criptografia em trânsito e em repouso?

A criptografia de dados em repouso significa que se aplica apenas a informações “paradas” em algum banco de dados, HD ou drive externo.

Já a criptografia em trânsito refere-se à proteção de dados em movimento (como mensagens trocadas no WhatsApp) ou quando você acessa um site na Internet.

O que é o protocolo TLS (Transport Layer Security)?

O protocolo TLS (Transport Layer Security) foi projetado para aumentar a segurança na comunicação computacional. Ele permite que duas partes (como seu computador e o servidor de um site) se identifiquem e autentiquem-se, liberando a comunicação de dados e garantindo sua proteção.

O que é criptografia homomórfica?

Um dos tipos mais complexos, a criptografia homomórfica parte do princípio que um texto cifrado pode ser trabalhado (ou seja, conhecido), sem que seja necessariamente descriptografado.

Ou seja, alguém pode somar dois valores criptografados e outra pessoa pode utilizar uma chave para desencriptar o resultado, sem que nenhuma delas descubra os valores individuais.

É o tipo de criptografia que possibilita uma apuração segura das urnas eletrônicas.

Como funciona a criptografia em sites da internet?

A criptografia em sites funciona de diferentes maneiras. Pode ser com o uso do protocolo TLS. Ao acessar um domínio na Web, o site se comunica com seu computador, de modo que possam se identificar e permitir a troca segura de informações.

Existem vários protocolos do tipo, como SSL, Wildcard, Multidomínio SAN, entre outros.

Com a criptografia minha empresa estará 100% segura?

A criptografia, embora não seja a única maneira de proteger suas informações, é essencial para assegurar a integridade e confidencialidade dos dados do seu negócio.

Uma empresa não deve utilizar apenas um tipo de proteção aos seus dados — como a criptografia — mas ela com certeza deverá ser parte do stack de soluções com esse intuito.

É essencial utilizar antivírus, anti-malwares, sistemas e ferramentas altamente protegidas e com recursos de proteção de ponta — constantemente atualizados.

Como a tecnologia pode manter seus dados seguros?

Tecnologias como inteligência artificial, machine learning e sistemas de gestão podem manter a segurança de dados de uma empresa.

A computação em nuvem, por exemplo, é uma forma de armazenar informações importantes com um design de soluções criado para isso.

O principal é entender que, hoje, no mercado, existem plataformas e soluções que possuem recursos de proteção de altíssimo nível — garantindo total integridade e confidencialidade dos dados.

Muitas vezes, é claro, utilizando da criptografia para tal.

Um sistema de gestão capacitado, por exemplo, pode ser responsável por integrar todos os dados do seu negócio, protegendo-os sob camadas intrincadas de criptografia — tornando-os acessíveis apenas àqueles com acesso, bem como hierarquia para tal.

ERPs da TOTVS

Com os sistemas de gestão da TOTVS, sua empresa cresce, se moderniza e opera com total segurança dos dados e informações.

Os ERPs da TOTVS, maior empresa de tecnologia do Brasil, alinham sua operação às demandas atuais, tornando sua atuação mais robusta e flexível.

Potencialize sua produtividade, aumente sua eficiência, automatize processos e conte com os mais altos níveis de criptografia para garantir a proteção de suas informações.

Conheça todos os detalhes, diferenciais e benefícios dos ERPs da TOTVS!

Conclusão

Ao desenvolver uma maior compreensão dos métodos comuns de criptografia e seus algoritmos, você estará alinhado com um dos principais métodos para proteger seus dados.

Você, como pessoa física e jurídica, precisa entender o que é criptografia e como esse método pode proteger as informações mais sensíveis da sua rotina.

Assim, é possível se proteger de possíveis ataques cibernéticos e violações aos seus dados.

É hoje, com a transformação digital e a evolução tecnológica, esse tópico é mais importante do que nunca.

Gostou de aprender mais sobre o assunto em nosso guia completo? Esperamos que seja útil e que esse conhecimento agregue valor ao seu dia a dia!

Entender mais sobre segurança das informações é essencial!

Por esse motivo, é muito importante estar por dentro das novidades em proteção de dados. Leia nosso artigo sobre anonimização e conheça mais sobre o assunto.

Continue acompanhando o blog da TOTVS e não deixe de assinar a newsletter!

NEWSLETTER

Receba as nossas mais recentes postagens de blog no seu e-mail

Nome

Sobrenome

E-mail

Adequação à Legislação | Business Performance | Cadeia de Suprimentos | Construção | Educacional | Hotelaria | Jurídico | Manufatura | RH | Saúde | Serviços | Techfin | Varejo e Distribuição

A TOTVS precisa das informações de contato que você nos fornece para entrar em contato com relação a produtos e serviços. Você pode deixar de receber essas comunicações quando quiser. Para obter informações sobre como cancelar o recebimento, além de nossas práticas de privacidade e compromisso de proteger sua privacidade, confira nossa Política de Privacidade.

CADASTRAR

ARTIGOS **RELACIONADOS**

GESTÃO DE NEGÓCIOS

LTV: o que é, importância, como calcular e aumentar

Você sabe quanto vale um cliente para a sua empresa? Essa é uma pergunta fundamental para qualque...

CONTINUE LENDO

GESTÃO DE NEGÓCIOS

IaaS: o que é e como funciona a Infraestrutura como Serviço?

Empresas estão entendendo a necessidade de se modernizar e embarcar nos avanços tecnológicos par...

CONTINUE LENDO

GESTÃO DE NEGÓCIOS

Modelagem de processos: compreenda e otimize a ge

Modelagem de processos é basi da operação mais eficiente que u t...

CONTINUE LENDO

DEIXE AQUI SEU COMENTÁRIO

NOME

E-MAIL

SEU SITE

Não sou um robô
reCAPTCHA
Privacidade - Termos