# Criptografia de Informação

## Guia corporativo



ENJOY SAFER TECHNOLOGY™

# A criptografia de dados em empresas



# 1. Introdução

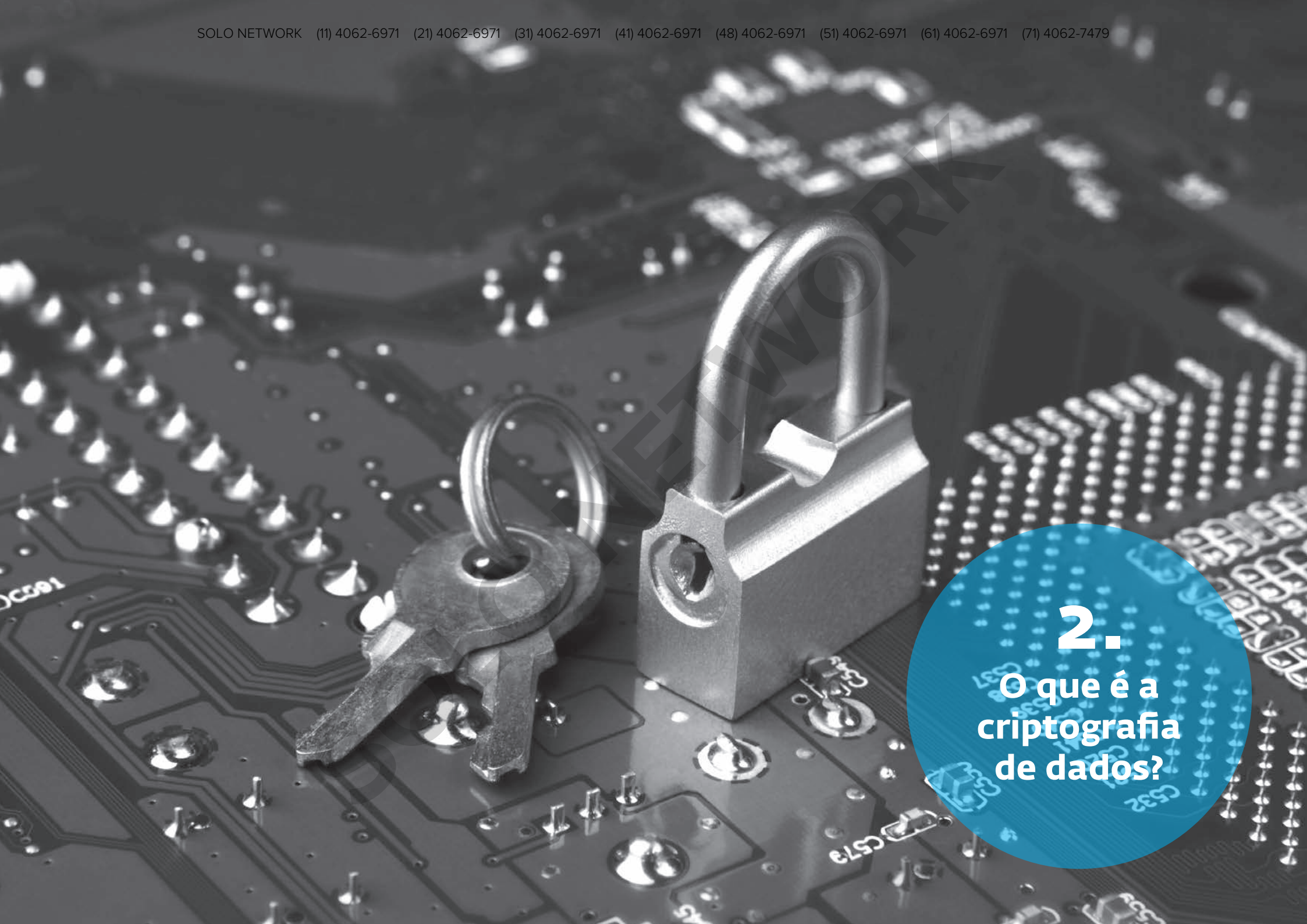
# 1. Introdução

A informação é um dos ativos mais importantes de uma empresa, não importando a quantidade. Por essa razão é indispensável protegê-los dos riscos existentes.

Seguindo esse raciocínio, a administração de informações de forma adequada pode fazer com que uma empresa não sofra as consequências de um ataque, principalmente no que diz respeito ao prestígio e confiança de seus clientes.

Atualmente, as ameaças contra informações corporativas vão desde o malware e a exploração de vulnerabilidades até o roubo de dispositivos móveis. Além disso, quando consideramos que a questão da privacidade nas comunicações é motivo de recentes debates internacionais, o conceito de criptografia de dados se tornou uma alternativa popular de proteger a informação doméstica e corporativa.

O objetivo desse guia é explorar detalhadamente aquestão da criptografia de dados, e dessa forma expor e explicar os benefícios que a mesma oferece às empresas.

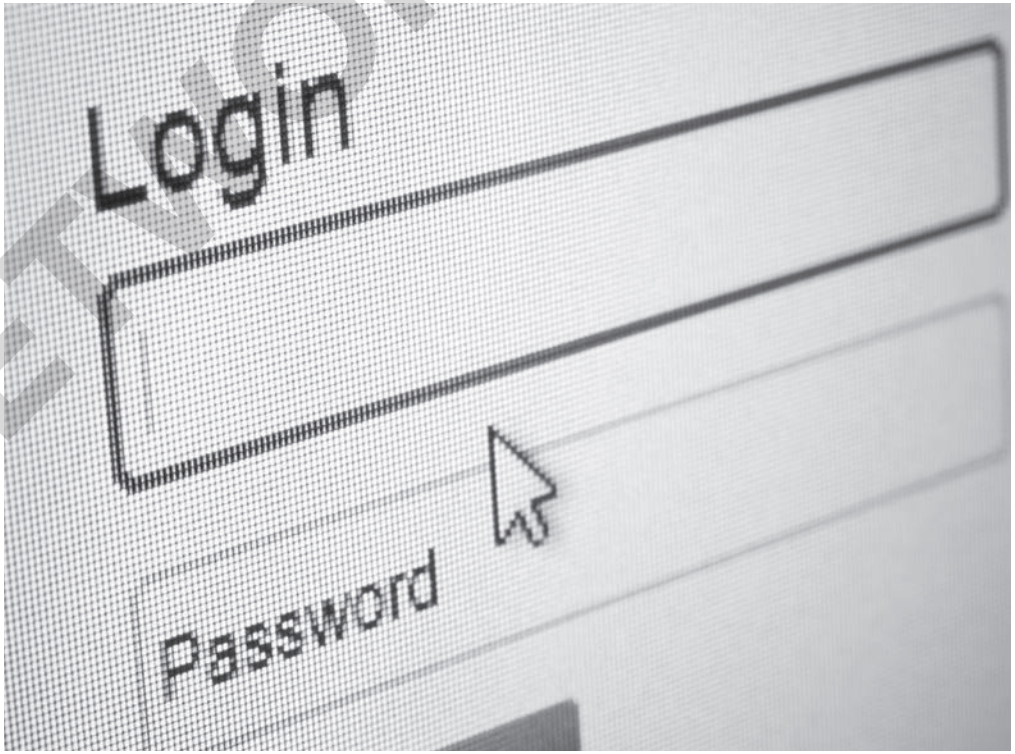


# 2.
# O que é a criptografia de dados?

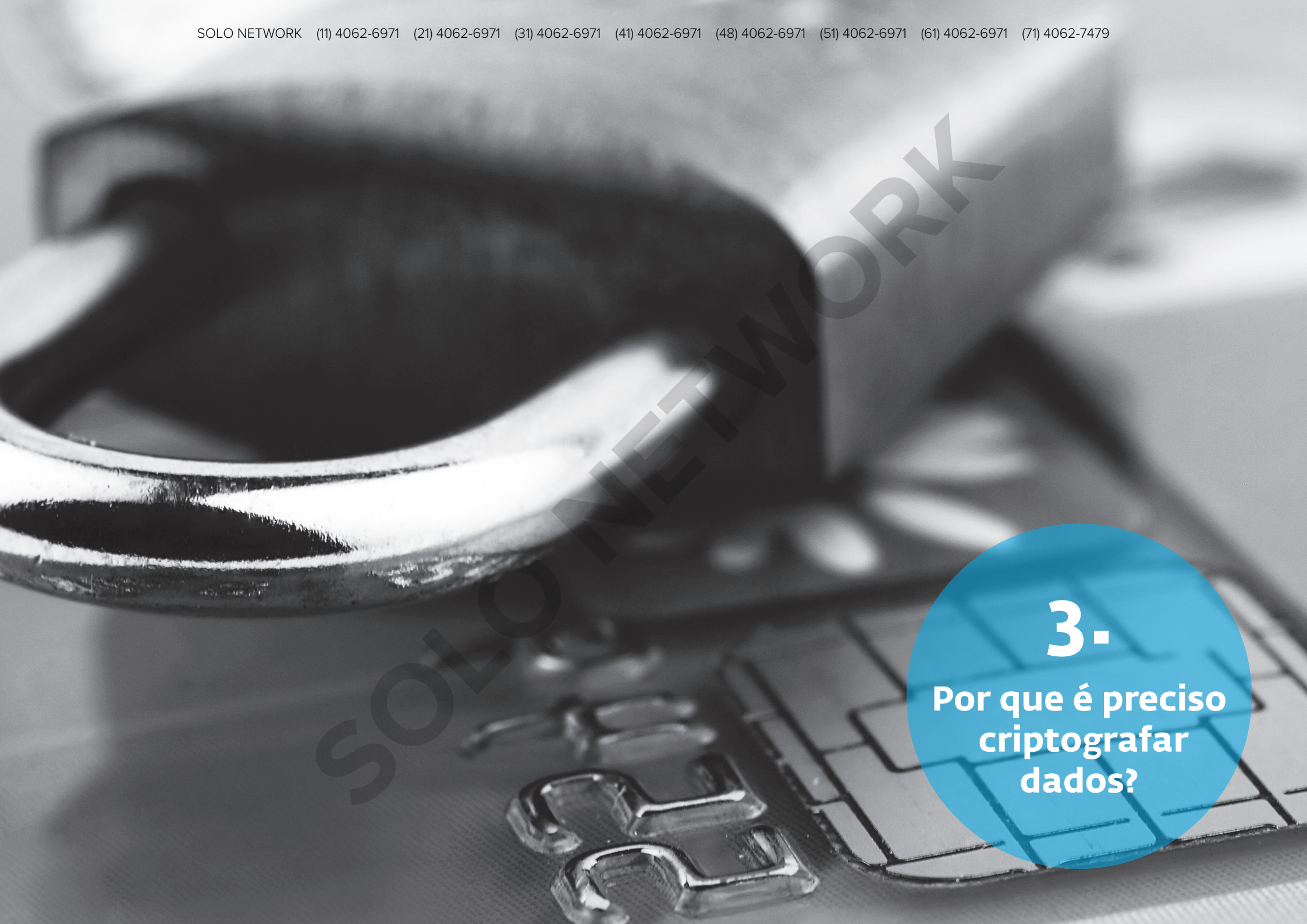
# 2.O que é a criptografia de dados?

Criptografar dados significa alterá-los, normalmente com o uso de uma chave que os torna ilegíveis para quem não a possui. Através do processo de criptografia, quem possui a chave mencionada pode utiliza-la para obter a informação original.

Essa técnica protege a informação sensível de uma empresa, pois caso os dados sejam interceptados, não poderão ser lidos.




**Uma das primeiras técnicas de criptografia utilizada na história foi o "Código de César", que consistia em substituir cada letra de uma mensagem por outra que a seguia no alfabeto. Devido à sua baixa complexidade, outros métodos foram desenvolvidos, por exemplo, tatuar os códigos de criptografia em escravos.**





# 3.

# Por que é preciso criptografar dados?

# 3. Por que é preciso criptografar dados?

Criptografar os dados significa que cada vez que houver a necessidade de acessá-los, é preciso descriptografar os mesmos, o que adiciona uma camada de complexidade ao acesso simples, além de reduzir a velocidade do processo em si. Por essa razão, surgem algumas questões: por que criptografar as informações importantes de uma empresa? Quais são os benefícios?

**Em setembro de 2011, a empresa holandesa DigiNotar declarou falência, após ter sofrido um ataque de fuga de informação.***

É muito difícil para uma empresa reverter o dano gerado por uma invasão significativa, razão pela qual é fundamental tomar as precauções necessárias para evitá-las, e se mesmo assim ocorrem, é preciso estar preparado adequadamente para minimizar os riscos, como por exemplo, utilizando dados criptografados.

**Fonte: http://www.welivesecurity.com/la-es/2011/10/07/ataque-informatico-lleva-diginotar-quiebra/*




# 4.
# Benefícios da criptografia

# 4. Benefícios da criptografia

A. **Proteção de informações confidenciais de uma empresa:**
Se a informação sensível de uma empresa cair em mãos erradas, existe a possibilidade de prejuízos econômicos, perda de vantagens competitivas ou até levar a empresa a falência. A criptografia ajuda a proteger informações delicadas como dados financeiros, informações dos funcionários, procedimentos ou políticas internas, entre outros.

B. **Proteger a imagem e prestígio de uma empresa:**
Existem certos tipos de informações, que se forem roubadas, podem causar danos à imagem corporativa. Um exemplo importante seria os dados de um cliente; o roubo das informações poderia afetar consideravelmente a empresa responsável pelo armazenamento dos dados, o que acarretaria em perdas irrecuperáveis.

C. **Proteção das comunicações de uma empresa:**
A criptografia normalmente é associada às transmissões de dados, já que as mensagens enviadas por uma empresa normalmente viajam por canais ou infraestruturas externas, como a Internet, e estão sujeitas a interceptação. O exemplo mais importante seria a criptografia de mensagens enviadas por e-mail.

D. **Proteção de dispositivos móveis ou sem fio:**
Todos os dispositivos que são utilizados fora do escritório, como telefones celulares, tablets ou notebooks podem ser extraviados ou roubados. Nessa situação é importante assegurar-se de que nenhuma pessoa, não autorizada possa acessar as informações encontradas.


# 5-
# Qual o papel da chave na criptografia?

# 5. Qual o papel da chave na criptografia?

A chave é uma parte essencial do mecanismo de criptografia de dados, já que representa a única possibilidade da informação ser descriptografada e acessada.O termo"chave"pode referir-se a um código gerado pelo software de criptografia ou senha criada pelo usuário. Por essa razão é imprescindível escolher uma senha forte, o que fará com que a barreira que separa os dados e os intrusos fique mais difícil de atravessar.

Escolher senhas como"1234" ou"secreta" é algo extremamente inseguro, porque embora sejam fáceis de lembrar, são igualmente fáceis de adivinhar, portanto não garantem nenhuma proteção de dados. Uma chave ideal seria uma senha o mais longa possível e com o conteúdo mais aleatório possível; no entanto se tornam mais difíceis de lembrar.

**Em fevereiro de 2013, o Burger King sofreu um ataque no qual conseguiram acessar e controlar a sua conta oficial do Twitter. Os atacantes mudaram a aparência da conta e mostraram imagens do seu principal rival. Aparentemente o ataque teve sucesso graças à uma senha fraca; uma alternativa para evitar casos assim é o uso de senhas fortes contidas em um software de armazenamento de chaves também criptografadas.***



# 6.
# Dicas para definir uma chave de criptografia

# 6. Dicas para definir uma chave de criptografia

A. **Não utilizar palavras reconhecíveis:** existe um tipo de ataque utilizado para adivinhar uma chave que consiste em experimentar uma por uma as palavras de um dicionário (e combinações das mesmas) até encontrar uma que coincida com a chave procurada

B. **Não utilizar chaves muito pequenas:** ataques por força bruta testam todas as combinações de caracteres possíveis até descobrir a chave. Dessa maneira, quanto mais caracteres existem na chave, maior será o tempo para testar todas as combinações. Quanto maior a senha, mais difícil será para adivinhá-la com a tecnologia atual.

C. **Utilizar letras minúsculas, maiúsculas, números e caracteres especiais:** seguindo a mesma lógica descrita acima, o ataque de força bruta pode ser dificultado através da variedade de caracteres, já que mais provas de combinações são necessárias.


D. **Não utilizar dados públicos:** mesmo tratando-se de uma prática comum, deve ser evitada. O endereço da empresa, dia de aniversário, nome, entre outros, são exemplos típicos.

E. **Utilizar um programa de administração segura de senhas:** contar com uma ferramenta de administração de senhas, é uma ótima opção. Esse tipo de programa oferece mecanismos para a geração de senhas seguras e as mantém em um repositório centralizado. Nesse caso só é preciso lembrar uma senha, a chave para acessar o repositório, que obviamente deveria ser estabelecida seguindo os conselhos mencionados até o momento.

# 7.

## Que tipo de informação deve ser criptografada?

# 7- Que tipo de informação deve ser criptografada?

As informações sensíveis de uma empresa estão presentes em muitos formatos e são transmitidas ou armazenadas em diversos dispositivos. Por essa razão é necessário considerar que o critério a ser usado para criptografar os dados corresponde ao valor da informação para o negócio.

Em primeiro lugar, a informação enviada em uma transmissão de dados pode ser criptografada, já que os canais utilizados para essa transmissão não pertencem a empresa e é possível que uma pessoa não autorizada intercepte essa mensagem. Por isso a implementação da criptografia de mensagens garante que somente os usuários que tenham a chave possam criptografar a mensagem e acessar seu conteúdo.

Existem também informações altamente importantes que, embora tenham sido armazenadas em dispositivos na empresa e não são retransmitidas, também correm o risco de serem acessadas por terceiros. Exemplos típicos são os computadores portáteis, que são utilizados somente pelos seus donos, entretanto existe o risco de roubo ou extravio, razão pela qual a informação deveria estar devidamente protegida. Seguindo a mesma lógica, a informação armazenada em servidores da empresa pode ser acessada se os cuidados necessários não são tomados.

Por último, vale a pena mencionar o caso dos smartphones e tablets. Esses tipos de dispositivos são cada vez mais comuns no âmbito corporativo, tanto para a transmissão de dados como para o armazenamento de documentos de trabalho. Portanto, devem ser levados em consideração no momento de definir que informação será criptografada.

Somente 20% das empresas da América Latina utilizam a criptografia para proteger a sua informação de acordo com o ESET Security Report 2013.*

**Fonte: http://www.welivesecurity.com/wp-content/uploads/2014/01/informe_esr13.pdf*



# 8.
# Criptografia de Comunicação

# 8. Criptografia de Comunicação

## • A. Email •

Uma forma de criptografar as mensagens de email é utilizando uma chave privada. Este método é mais fácil de implementar e consiste em criptografar o texto em questão para em seguida enviar o email; assim, o destinatário deve conhecer a chave para obter a mensagem original.Entretanto, cada vez que se envia uma mensagem criptografada para alguém que não conheça a chave, deve-se informar por um meio seguro.

Diante da incerteza de como transmitir a chave de forma segura, surge a alternativa de criptografia pública. Este sistema é mais robusto e é baseado na utilização de certificados: tanto o emissor como o receptor tem seu próprio certificado que podem publicar sem comprometer sua segurança. Assim, cada vez que enviar uma mensagem para alguém, deve-se criptografar o mesmo com a chave pública estabelecida no certificado do destinatário. Em outra extremidade, ao receber uma mensagem criptografada será aplicada uma chave secreta que não conhece o destinatário, que recebe a mensagem original. Em resumo, a chave com a criptografia é diferente daquela com a qual se criptografa, mas estão relacionadas, não se pode obter uma conhecendo a outra.

Uma vez que um usuário tem seu próprio certificado válido, deverá trocar mensagens digitalmente com seus contatos, para obter e armazenar os certificados deles. A partir daí, o processo de criptografia será prácticamente transparente para o usuário. Caso envie uma mensagem criptografada, e o destinatário não conte com a possibilidade de lê-lo, o emissor terá a opção de enviar a mensagem sem criptografar.

**O caso PRISM e os programas de espionagem de agências governamentais tem exposto a questão da privacidade na Internet em um centro de debate, popularizando a criptografia de dados como uma alternativa para a proteção dos emails e outros tipos de comunicações.**

A forma mais conveniente de implementar a criptografia de emails é através de componentes ou plugins que se integram aos serviços de email como Outlook por exemplo.
Assim, a gestão de chaves compartilhadas e o processo de criptografia serão transparentes ao usuário.

# 8. Criptografia de comunicações

## • B. Navegação criptografada para os clientes •

Quando os clientes navegam pelo site de uma empresa, realizam envios e constantes solicitações de informações que, em muitos casos podem ser confidenciais ou de alto valor para o cliente, portanto é necessário proporcionar um mecanismo de segurança para protegê-los. Uma forma muito utilizada é através da criptografia dos dados que foram enviados.

Neste caso, o processo de criptografia é similar ao que se descreveu para o envio de e-mails, mediante a utilização de certificados. Portanto, afim de proporcionar este mecanismo de segurança aos usuários, é necessario ter um certificado que identifique a empresa em seu site, o qual será obtido a partir de certificados autorizados.

A aplicação mais comum da navegação criptografada ocorre na hora de realizar o acesso a dados bancários ou principais cartões de crédito, mas também pode aplicar-se apenas a uma sessão de navegação: quando um usuário registrado quer autenticar-se será realizado o intercâmbio de certificados e o establecimiento de uma conexão segura; a comunicação criptografada, então, se manterá até que a sessão seja encerrada.

**Em alguns anos atrás, a navegação segura era vista em poucos sites. Por exemplo, o Facebook implementou este procedimento em janeiro de 2011 e o Twitter em março desse mesmo ano. Atualmente, os sites mais importantes a utilizam como padrão e é inevitavel quando há a necessidade de inserir dados bancários.**

# 9. Criptografia de dados locais

# 9. Criptografia de dados locais

A informação que não é transmitida também corre o risco de ser acessada por terceiros; por exemplo, antes da perda ou roubo de dispositivos móveis. A senha de início de sessão não é suficiente para proteger os dados, é onde a criptografia entra em jogo. Neste caso podemos criptografar o disco inteiro, de tal maneira que cada vez que o computador é acessado devemos iniciá-lo com a chave. Esta ação é geralmente sugerida em empresas, embora também existam alternativas para criptografar somente algumas pastas ou arquivos específicos. Além disso, vale esclarecer que pode ser extendido a qualquer dispositivo que transporte informações delicadas, como memórias USB.

Outra situação pode ocorrer quando dados ou serviços são inseridos para o público. O cenário ideal é aquele que cada usuário possa acessar apenas os dados para os quais tem liberação.Infelizmente, se existem vulnerabilidades em servidores da empresa, as mesmas podem ser exploradas dando acesso aos atacantes a informações confidenciais. Portanto,a medida de segurança principal consiste em evitar o acesso indevido,minimizando as vulnerabilidades. No entanto, é igualmente importante ter um plano de respostas para incidentes,caso um atacante consiga um acesso aos dados confidenciais.Nesta situação se determinados arquivos são criptografados é reduzida a utilidade para o atacante. A informação dos clientes é extremamente importante e não poder garantir sua segurança faz com que os clientes deixem de confiar na empresa

Um exemplo disso ocorre no armazenamento de dados de autenticação dos usuários: se senhas são armazenadas em uma base sem criptografia, as contas dos clientes estariam diretamente expostas para que o atacante conseguisse acessar estes registros.

**Em julho de 2012 o Yahoo! sofreu um ataque, e neste caso roubaram em torno de 500 mil senhas de usuários. As senhas não eram criptografadas, sendo assim, permitiu-se o acesso direto das contas e suas informações foram comprometidas.***

**Fonte: http://blogs.eset-la.com/laboratorio/2012/07/12/yahoo-nueva-brecha-seguridad-red/*




# 10.

# Criptografia de dispositivos móveis

# 10. Criptografia de dispositivos móveis

Os dispositivos móveis estão se transformando em um fator muito importante nas empresas, já que estão com os funcionários o tempo todo e em todos os lugares, além de fornecer acesso imediato a todo tipo de informação. Devido ao fato de que cada vez mais é possível acessar informações corporativas através de um dispositivo móvel, é necessária uma administração apropriada da segurança da informação nestes dispositivos.

Em primeiro lugar, é importante destacar que devido ao seu tamanho e portabilidade, esse tipo de dispositivo é suscetível ao roubo e extravio, o que representa um risco importante. Criptografar os dados armazenados é, então, uma medida eficaz contra o acesso não autorizado a essa informação. É possível criptografar os dados dos aplicativos, arquivos baixados, fotos, documentos e qualquer outro arquivo armazenado no dispositivo. Dessa forma, para acessar os dados é necessária a inserção de um PIN ou chave, que somente é de conhecimento de seu proprietário.

É importante também lembrar que os dispositivos móveis fornecem conexão a redes que utilizam o ar como meio de transmissão, e os dados poderiam ser interceptados por terceiros que estão ao alcance do sinal. Assim, sempre que for necessário transmitir informação sensível é imprescindível conectar-se a uma rede que possa enviar informação criptografada entre o dispositivo móvel e o ponto de acesso. Também é preciso implementar a criptografia nas comunicações através da Internet, como e-mails confidenciais, chats ou mensagens instantâneas.

É possível criptografar os dispositivos móveis com ferramentas nativas do próprio sistema operacional. No Android, por exemplo, esse ajuste pode ser feito em **Ajustes/Segurança/ Criptografar Telefone**.

Caso o processo de criptografia seja interrompido, a informação poderá ser perdida de forma definitiva; para evitar essa possibilidade, o dispositivo deve ser carregado ao máximo e estar conectado a eletricidade. Geralmente o processo demora aproximadamente uma hora, dependendo da quantidade de informação armazenada.



# 11.
# Conclusão

# 11. Conclusão

A segurança de uma empresa requer esforços constantes, que devem ser acompanhados por investimentos baseados no valor da informação a proteger, no impacto que pode ter nos negócios e na situação atual da segurança na empresa.

Além disso, é necessário contar com políticas de segurança detalhadas que identifiquem os ativos de informação e os riscos associados aos mesmos, para então determinar as possíveis ações preventivas e corretivas. Nesse contexto, a criptografia de dados é uma forma de proteger a informação sensível de uma empresa em sua totalidade: dados armazenados em servidores e inclusive comunicações nos dispositivos móveis de seus funcionários.