Guia De Criptografia

Perguntas e repostas sobre a criptografia da informação pessoal

Guia para aprender a criptografar sua informação.

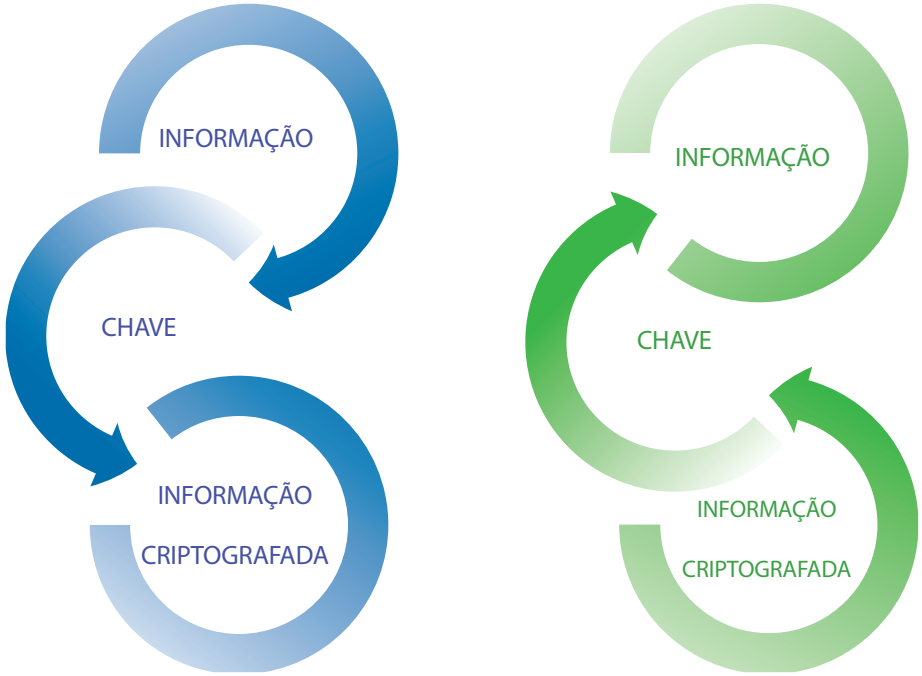
O que estamos protegendo?

Através da criptografia protegemos fotos, vídeos, mensagens de texto, conversas realizadas no chat, documentos, contatos e muito mais. É cada vez maior a quantidade de informação que guardamos em nossos dispositivos, que por sua vez é cada vez mais sensível. Por essa razão é indispensável proteger essa informação dos riscos existentes atualmente.

As ameaças existentes para a informação, podem ser malware, exploração de vulnerabilidades e até o roubo de dispositivos móveis. Com as atuais discussões sobre a privacidade das comunicações, o conceito de criptografia de dados se popularizou como uma forma de manter a informação segura.

Administrar informação de forma adequada no momento de um incidente é a chave para evitar maiores danos.

O que é a criptografia de dados?



Quando a informação é criptografada, seus dados são alterados de acordo com um padrão estabelecido por uma chave, de forma que somente podem ser compreendidos por quem conheça essa chave.

Assim, uma mensagem criptografada pode ser enviada ou armazenada em um dispositivo. Se alguém acessa esse arquivo sem ter essa chave, não poderá ver a informação.

Existem ataques para tentar acessar arquivos criptografados sem a chave. A dificuldade para descriptografar a informação com um ataque, depende do método de criptografia utilizado, da informação e da chave.

> A criptografia vem sendo utilizada há muito tempo. Na Roma antiga, era utilizada a "Criptografia de César", que significava substituir cada letra de uma mensagem por outra letra que se encontrava 3 posições à frente no alfabeto.

Realmente preciso criptografar os meus dados?

Como usuários, poderíamos achar que talvez nossa informação não seja alvo de um atacante, então talvez possa ser conveniente fazer as seguintes perguntas:

Que tipo de informação armazeno em meu dispositivo?

A informação é pessoal, financeira ou confidencial? É interessante tentar imaginar o que faria um atacante se pudesse acessar a informação que guardo em alguns dos meus dispositivos?

O que aconteceria se eu perdesse o meu dispositivo móvel ou meu computador portátil?

Temos certeza de que ninguém acessará nossa informação em caso de perda ou roubo de nossos equipamentos?

O que acontece se o dispositivo é infectado com malware?

Não é somente com a perda de um dispositivo físico que a informação pode ser roubada. Existem outros tipos de ameaças que podem roubar o que temos armazenado.

Então, devo criptografar toda a minha informação?

Armazenamos cada vez mais informação, e portanto criptografar tudo pode afetar o rendimento do nosso dispositivo. Devemos então selecionar os dados que queremos criptografar segundo a sua relevância:

- Fotografias e vídeos
- Informação de contatos
- Documentos confidenciais

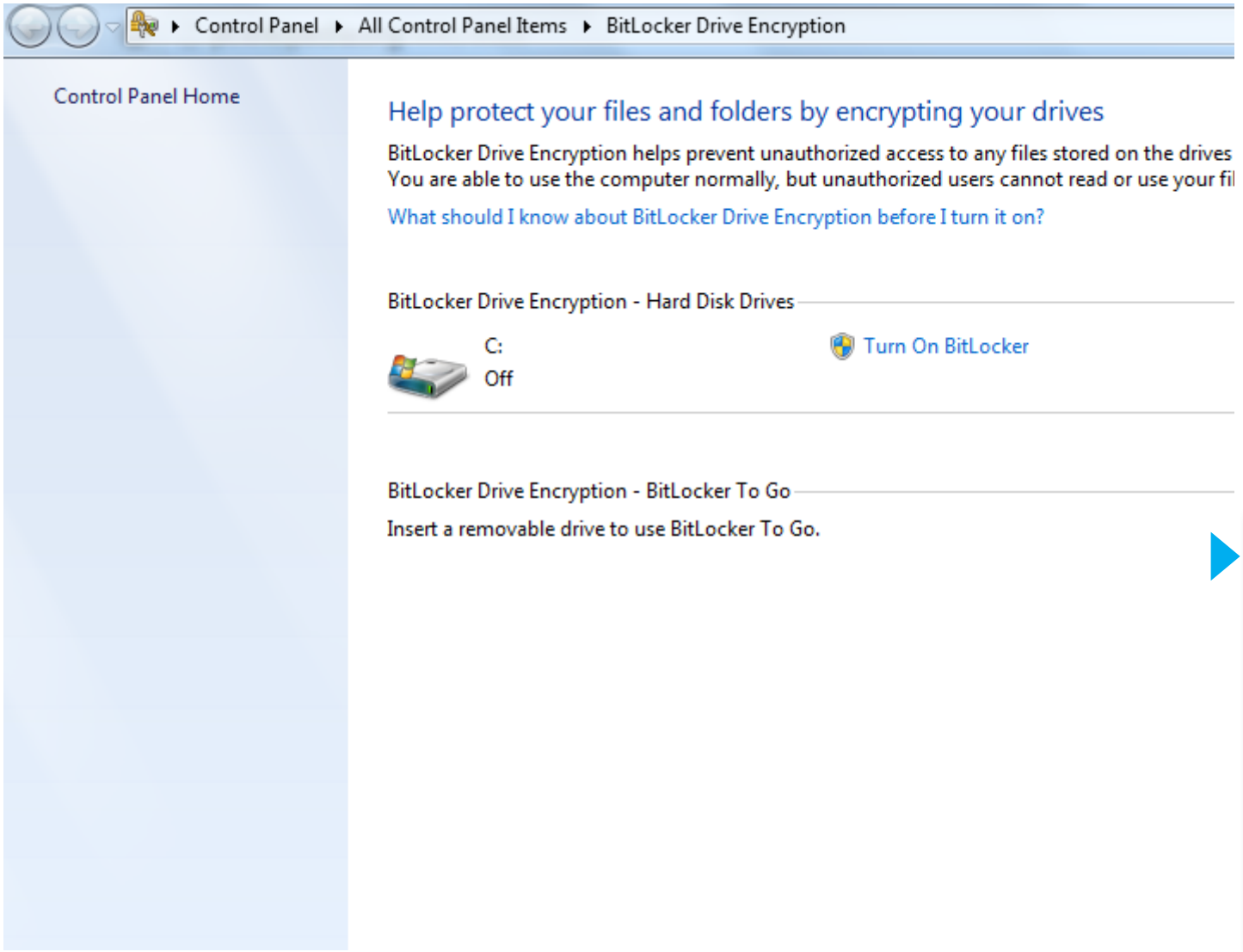
Criptografando a informação em computadores

Os principais meios de armazenamento se encontram em computadores ou em dispositivos acessados, portanto é muito importante ter um cuidado especial no momento de criptografar esses grandes depósitos de informação.

No caso de perda do computador ou para evitar o acesso indevido à sua informação, muitas vezes ter uma senha de acesso como único meio de proteção não é o suficiente. Uma alternativa válida é utilizar as opções de criptografia de dados que o sistema operacional atual oferece.

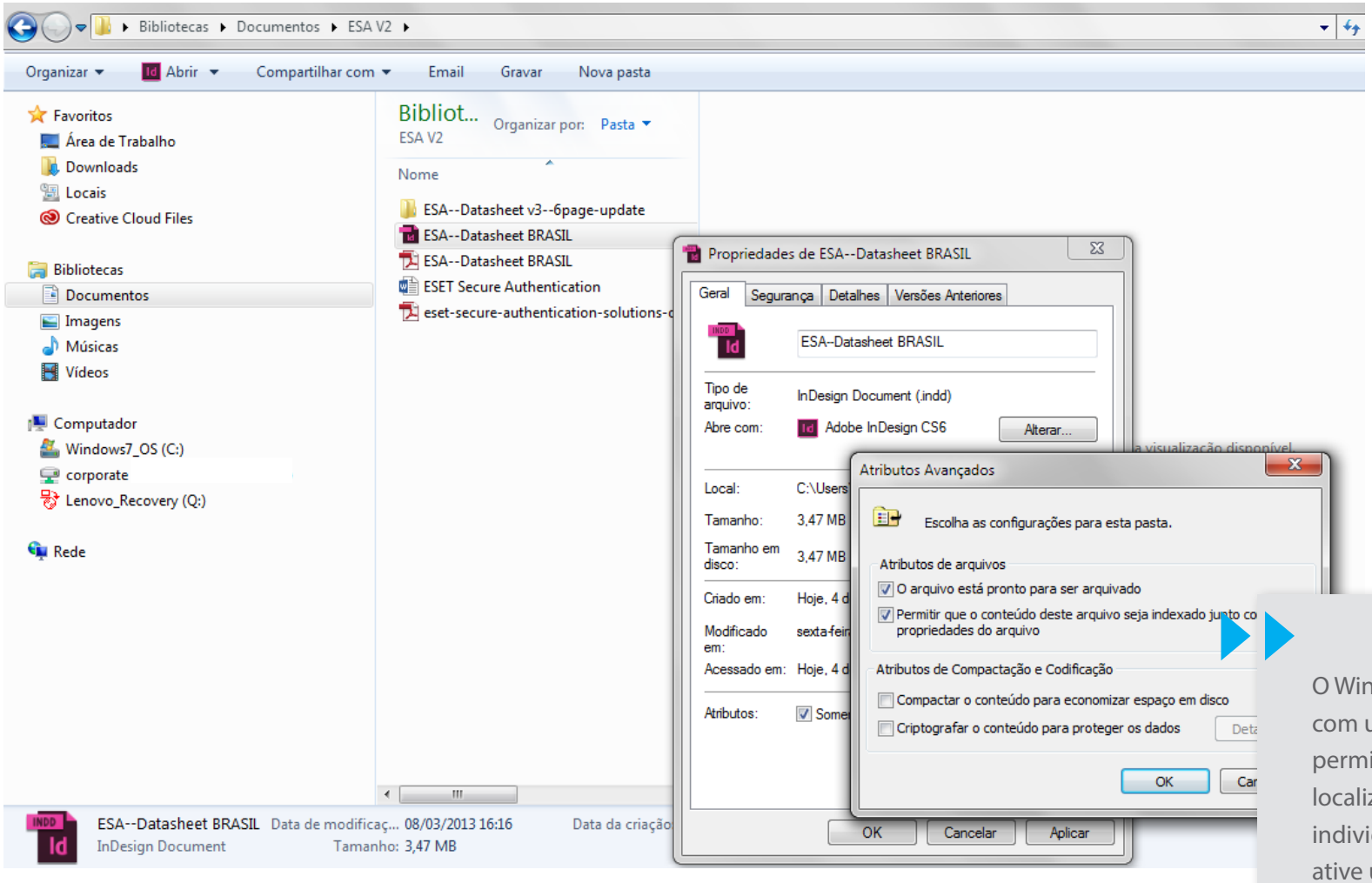
A utilização de arquivos comprimidos com senhas é uma alternativa prática para o intercâmbio de informação. Vale ressaltar que a senha utilizada para proteger a informação deve ser forte o suficiente e o algoritmo utilizado pelo software, altamente seguro.

Criptografia em Windows



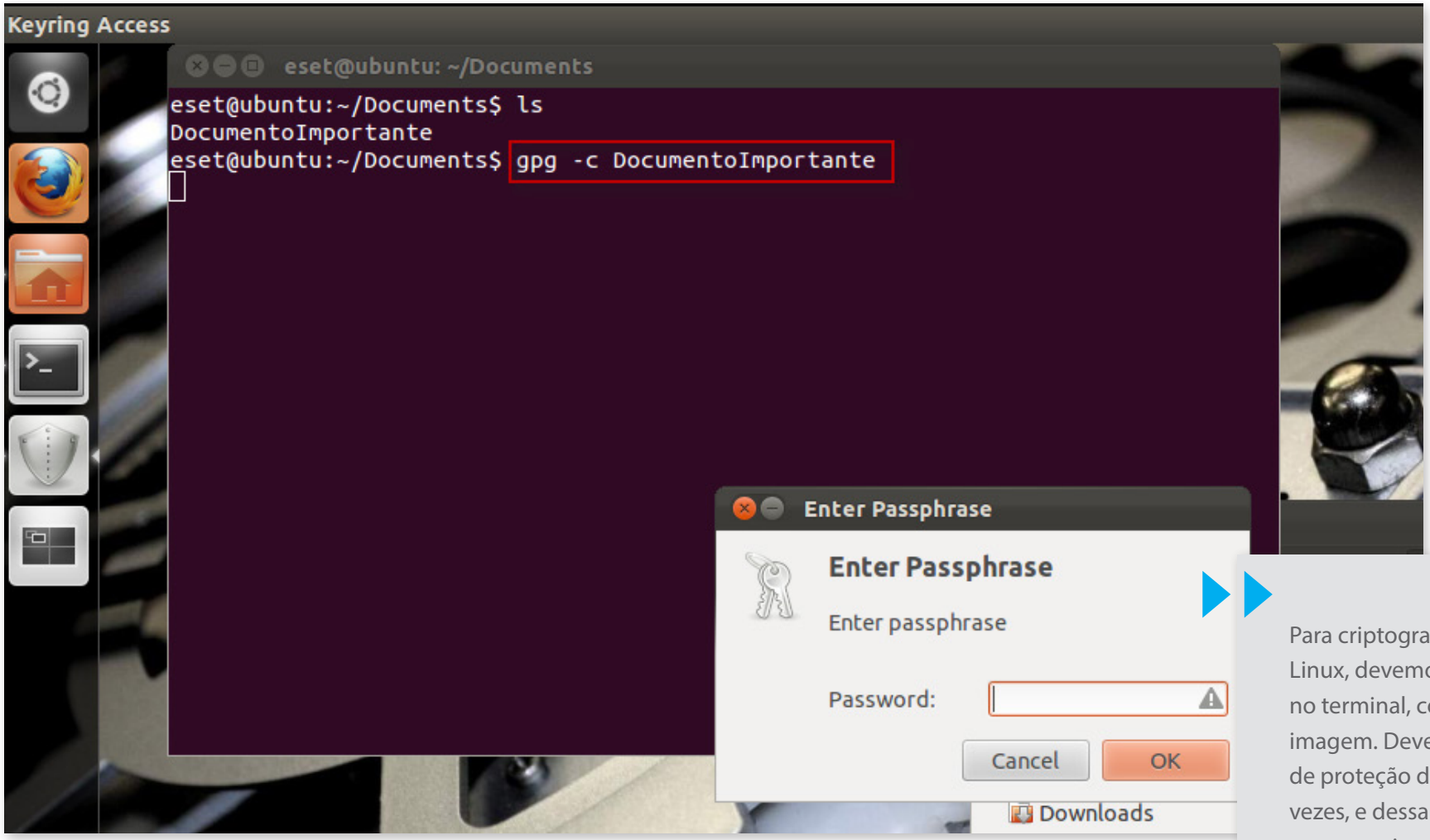
O Windows conta com o BitLocker, um aplicativo cujo objetivo é criptografar qualquer unidade de disco especificado pelo usuário, incluindo os arquivos de sistema do Windows necessários para o início do sistema e de sessão no disco de boot.

Criptografia em Windows



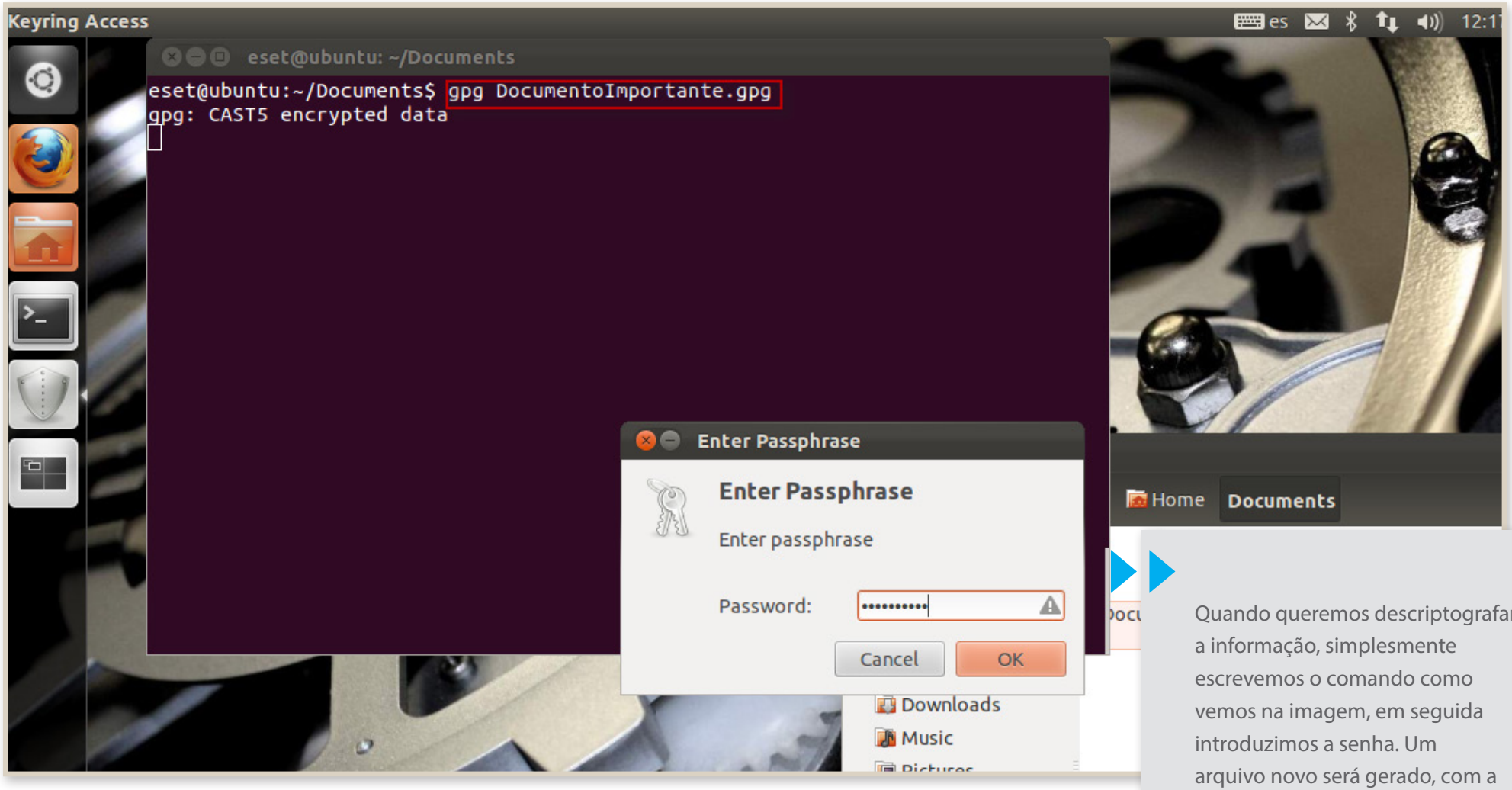
O Windows também conta com uma função que nos permite criptografar os arquivos localizados em nosso computador individualmente. Neste caso, ative uma opção encontrada nas propriedades do arquivo ou da pasta específica que queremos criptografar.

Criptografia em Linux



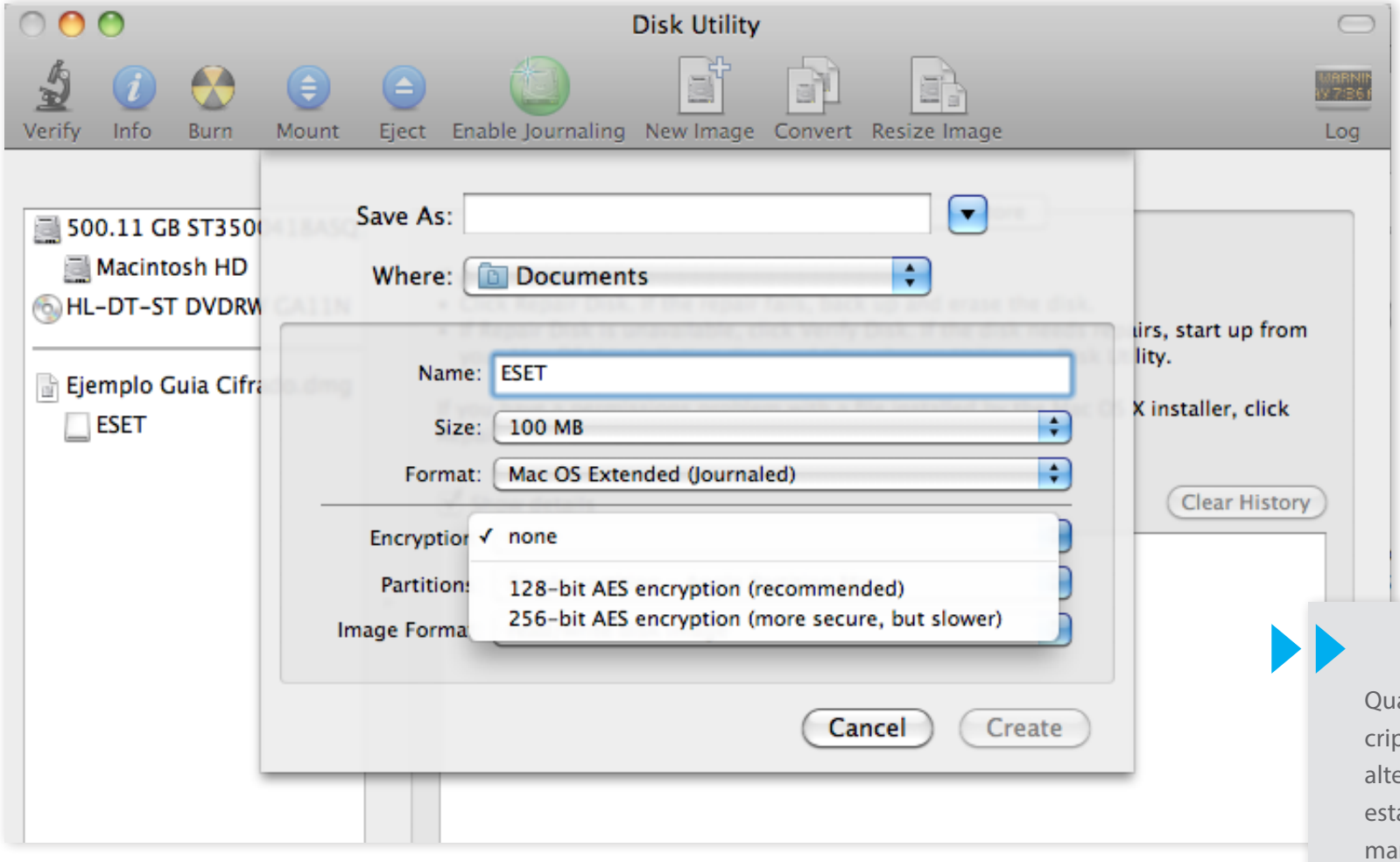
Para criptografar um arquivo em Linux, devemos escrever o comando no terminal, como pode ser visto na imagem. Deve-se introduzir a senha de proteção de informação duas vezes, e dessa forma é criado um novo arquivo com a extensão gpg.

Criptografia em Linux



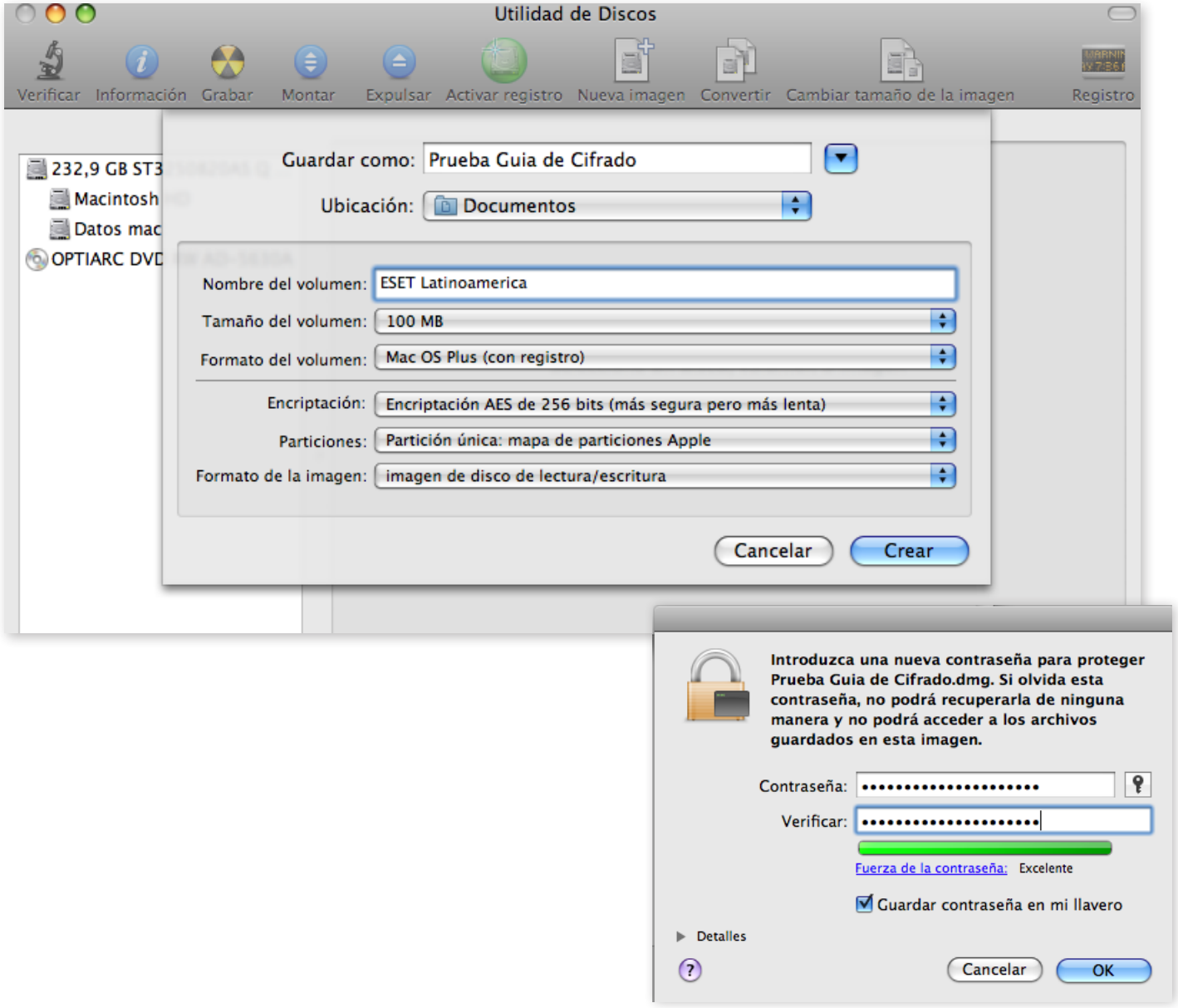
Quando queremos descriptografar a informação, simplesmente escrevemos o comando como vemos na imagem, em seguida introduzimos a senha. Um arquivo novo será gerado, com a informação pronta para ser lida.

Criptografia em Mac OS X



Quando a informação é criptografada, os dados são alterados segundo um padrão estabelecido por uma chave, de maneira que somente possam ser entendidos por aqueles que possuem a chave.

Criptografia em Mac OS X



Dessa forma, uma mensagem criptografada pode ser enviada de um lugar a outro, ou armazenada em um dispositivo. Se alguém acessar esse arquivo sem a chave correspondente, não poderá ver a informação.

Porém, existem ataques que visam acessar esses arquivos mesmo sem contar com as chaves para fazê-lo. A dificuldade para descriptografar a informação através de um ataque, dependerá do método de criptografia da informação e da chave utilizada.

E para dispositivos móveis, existe informação para criptografar?

Que tipo de atividade você realiza com o seu dispositivo móvel, seja ele um smartphone ou um tablet?

Se comparamos a resposta com o tipo de atividade que realizamos com nossos computadores pessoais, certamente não encontraremos diferenças importantes. Isso indicaria que também armazenamos e administramos informação importante nos dispositivos móveis.

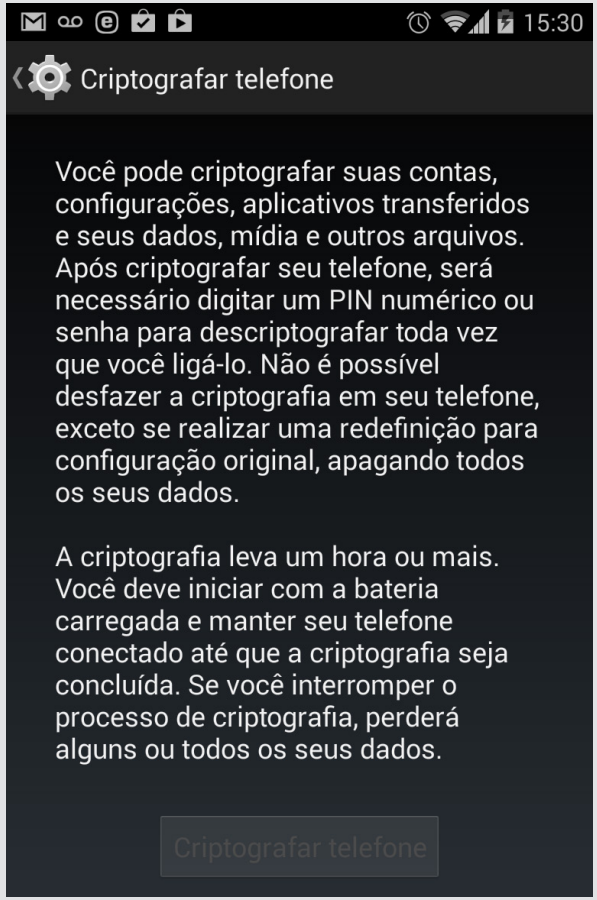
Porém, esses dispositivos estão mais expostos ao roubo ou extravio pois estão conosco durante muito tempo. Por esse motivo é fundamental que o dispositivo conte com pelo menos uma chave de acesso. Dessa forma impedimos que uma pessoa não autorizada possa acessar nossas fotos, vídeos, contatos e qualquer informação armazenada nos mesmos.

Existe também outra variável que temos que considerar: a forma mais utilizada de compartilhamento de informação por esses dispositivos é o ar, portanto alguém poderia monitorar os sinais das diversas redes. Por essa razão é preciso ter muito cuidado nas redes utilizadas para trocar informação. E é recomendado utilizar canais criptografados quando a informação é confidencial.

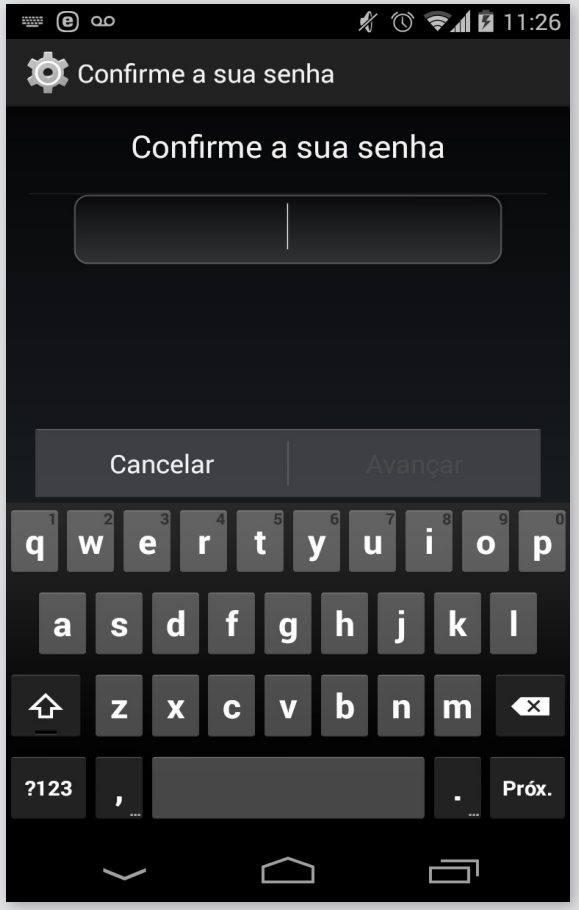
Igualmente aos computadores, as principais marcas de dispositivos móveis possuem ferramentas de criptografia nativas de cada sistema operacional.

Criptografia em Android

O Android oferece uma ferramenta de criptografia no menu Ajustes/Segurança para criptografar a informação do dispositivo e do cartão de memória SD. Ambos requerem uma senha, portanto a mesma deve ser forte para uma segurança maior



Quando selecionamos a opção "criptografar telefone", as contas, fotos, vídeos e outros arquivos multimídia serão criptografados



Insira uma senha e a seguir na opção de cartão SD externo Criptografar, você pode selecionar os arquivos a serem criptografados: os novos, todos os arquivos ou excluir arquivos de mídia.

Criptografia em iOS

Os dispositivos móveis que utilizam o sistema operacional iOS já vem de fábrica criptografados com o sistema AEES 256, e além disso contam com Data Protection para criptografar todas as entradas e saídas de informações.

Essa característica implementada pela Apple também tem um sistema de Número Pessoal de Identificação que apaga automaticamente todo o conteúdo do dispositivo depois de 10 tentativas com erro para advinhá-lo.

A chave de algoritmo é diferente para cada dispositivo e está inserida diretamente no hardware.

A criptografia como um meio adicional de proteção

A criptografia da informação é uma prática que vem se popularizando cada vez mais tanto em ambientes corporativos como nos domésticos, devido ao intenso uso da tecnologia pelos usuários e a confluência do âmbito pessoal e profissional no mesmo dispositivo.

Essa evolução produz como consequência o crescimento no número de ameaças digitais. Não é somente o roubo ou extravio do dispositivo que pode causar a perda de nossa informação, mas também malwares, vulnerabilidades, ataques dirigidos, engenharia social, entre outros.

Por essa razão a proteção deve ser integral, e para alcançar esse objetivo é aconselhável utilizar uma solução de segurança e certificar-se que a instalação dos aplicativos sempre ocorra a partir de fontes oficiais.

Dessa forma, pode-se aplicar a criptografia de informação sensível contida no dispositivo como uma camada adicional de proteção para poder disfrutar das tecnologias de forma mais segura.

ENJOY SAFER TECHNOLOGY™

www.eset.com.br

/ESETBRASIL

@ESET_BRASIL

/company/eset-brasil