GUIA DE

Backup

Introdução

Imagine que você possui informações pessoais ou trabalhos da universidade armazenados em seu computador; ou no caso dos servidores coporativos, informações sensíveis que ajudam o negócio a operar corretamente, e que quando chega ao momento em que deseja utilizá-la, se dá conta de que ela não está mais disponível.

A causa? Um defeito em seus dispositivos de armazenamento como um disco rígido, problema de energia elétrica, roubo de dispositivo, ou ainda, uma infecção por um código malicioso conhecido como ransomware.

Alguns usuários subestiman esse tema e pensam que é pouco provável que vá acontecer com eles alguma das situações citadas anteriormente, no entanto, com o crescimento de casos de ransomware na região isso já nos dá uma ideia do alcance dessa problemática.

Por esse motivo, este guia possui o objetivo de ajudar usuários para que possam adotar as medidas necessárias para proteger informações importante por meio do backup de dados.

Índice

O que é uma cópia de segurança ou backup?

É um processo em que se cria uma cópia dos arquivos importantes com o objetivo de recuperá-los caso haja uma perda de informação. Isso é muito importante já que existem múltiplas causas pelas quais um usuário poderia passar por esse problema. Por exemplo, a vida útil limitada dos discos rígidos, roubos ou perdas de dispositivos e os códigos maliciosos já mencionados.

É necessário ter em mente que as cópias de segurança também estão expostas a esses riscos. Por esse motivo, não é recomendado que a unidades de backup estejam conectadas a mesma rede de produção de forma integral já que, dessa maneira, caso houvesse uma infecção esses arquivos poderiam ser afetados. Por outro lado, é importante que os usuários não estejam o tempo todo com seu disco rígido onde guardam o backup de sua informação, além do dispositivo que foi feito a cópia de segurança, já que podem ocorrer perdas ou roubos de ambos os dispositivos.

Códigos maliciosos e perda de informação

Dentro das diversas causas pelas quais um usuário poderia perder sua informação, se encontram os códigos maliciosos, particularmente os do tipo **ransomware**, ou seja, um malware que infecta o equipamento, criptografa os arquivos e, logo em seguida, solicita um resgate em dinheiro para que o usuário possa ter acesso a seus dados novamente.

Esse método transformou o ransomware em uma das ameaças mais prolíficas dos últimos anos. Atualmente, não só encontramos casos em computadores, mas também em dispositivos móveis, e até mesmo dispositivos mais incomuns, como aqueles que fazem parte da Internet das Coisas.

A raíz dessa problemática do ransomware, é que se mostra essencial contar com um backup, já que é umas das ferramentas ideais para recuperar informação caso seja vítima de uma infecção.

Qual informação deve ser copiada?

Nem toda informação possui o mesmo valor, por isso, antes de começar com o processo de backup, é fundamental determinar quais informações serão copiadas. Ao atribuir valor aos dados, é possível estabelecer quais são os mais relevantes segundo suas preferências pessoais, tipo de trabalho realizado com essas informações, ou ainda objetivo e utilidade que possuem.

Uma consideração importante é analisar se o backup necessita de elementos de hardware ou se apenas recuperar os dados é a finalidade. Isso se deve porque, em alguns casos, copiar somente os dados pode gerar maiores conflitos para restabelecê-los, já que muitas vezes, se faz necessário reinstalar manualmente todo o sistema operacional e seus aplicativos.

Além disso, é importante ter o controle da frequência com que os arquivos são modificados. Existem informações que somente são utilizadas uma única vez, portanto precisam ser copiadas.

Por último, em situações que os arquivos do sistema se encontram em risco, não se esqueça de fazer o backup das configurações de segurança e outras documentações importantes que orientam o funcionamento padrão do sistema.

Meios de armazenamento

O próximo passo é escolher um meio de armazenamento para seu backup. Nesse ponto, o espaço físico em que será guardado o suporte de segurança também deve estar protegido.

Tal como mencionamos no começo, de nada serve sair por aí com seu notebook e seu disco rígido externo em que está armazenado seu backup, já que caso houvesse algum roubo, as informações originais e as cópias seriam perdidas.

Disco rígido

É uma boa ideia utilizar um disco rígido exclusivamente com este propósito para evitar desgastes desnecessários. Do memso modo, se o disco é interno, deve ser um fisicamente distinto do que se utiliza para iniciar o sistema operacional.

Dispositivos de armazenamento USB

É recomendável utilizar um exclusivamente para cópias de segurança e evitar transportá-lo fora de onde o guarda para evitar perdas ou roubos.

Meios óticos (CD / DVD / Blue-Ray)

São mais suscetíveis a sofrer danos físicos como riscos e rachaduras que podem corromper os dados. É recomendável armazenar a informação em mais de um meio ótico caso algum apresente falhas.

A Nuvem

Possui a vantagem, de facilitar o acesso à informação a partir de praticamente qualquer lugar com conexão de Internet, No entanto, é importante considerar as políticas de uso do serviço escolhido e os sistemas de proteção que utilizar para proteger os dados.

Frequência de backup

Logo após ter selecionado que informação será copiada e o meio de armazenamento, é importante estabelecer a periodicidade com que se deve realizar o backup.

Essa decisão deve ser adotada com base na frequência com que se modificam, eliminam e criam arquivos. Se trabalha todos os dias com um projeto, será necessário realizar uma cópia de segurança diária. No caso oposto, uma pasta de fotos deve ser novamente copiada comente quando se adicionem novas fotos.

Uma vez determinada a frequência, é possível escolher entre **3 tipos diferentes de backup**:

Completo

Ese tipo de backup faz uma cópia completa de todos os arquivos do equipamento. Abrange a totalidade dos dados e leva mais tempo e espaço de armazenamento. É possível escolher essa opção em um primeiro momento, e logo, utilizar uma das opções abaixo.

Diferencial

Contém somente os arquivos que mudaram no sistema desde a última vez que uma cópia completa foi realizada. São cópias acumulativas, ou seja, cada uma delas protege o que é diferente da última cópia completa. Recomendada quando se estabelece uma frequência diária de backup.

Incremental

Copia arquivos que foram modificados desde a última cópia de segurança diferencial ou incremental. Uma diferença importante a respeito das cópias diferenciais é que as incrementais ao fazer as cópias de segurança com menor quantidade de dados, elas são realizadas mais rápida e requer um espaço menor de armazenamento.

A informação de um dispositivo móvel deve ser copiada?

Os dispositivos móveis como smartphones e tablets costumam armazenar informações sensíveis e muito importantes. Por esse motivo, fazer o backup desses dispositivos também é necessário, assim como computadores, ainda mais se considerarmos que são utilizados para administrar as mesmas informações críticas.

Existe a possibilidade de guardar manualmente esses arquivos conectando-se a um computador. Serviços de armazenamento na Nuvem como o iCloud, no iPhone, e uma conta do Google, caso utilize Android, também podem ser úteis.

Como realizar backup em diferentes sistemas operacionais?

Windows

Se precisamos copiar informações pessoais em nossos computadores, os sistemas operacionais da Microsoft, a partir da versão Windows 7, possuem uma ferramenta embutida que permite criar cópias de segurança dos arquivos pessoais.

Para acessar esse recurso você deve ir ao Painel de Controle, depois clicar na opção de Sistema e manutenção, e por último, em Cópias de segurança e restauração. Do mesmo modo, a partir do Windows 8 foi incluída uma característica de backup denominada Histórico de Arquivos. Ativando essa opção, o sistema mantém uma cópia dos arquivos pessoais do usuário que estão armazenados no Área de Trabalho, pasta de arquivos e contatos, entre outros.

Para acessar esse recuso você deve procurar por Histórico de Arquivos no menu iniciar. Depos acessar Configuração, e por fim, clicar na opção de Histórico de Arquivos para ativá-lo.

Para mais informações, acesse o site de **Suporte da Microsoft.**

macOS

A partir da versão 10.5, o sistema operacional da Apple conta com uma ferramenta denominada Time Machine, que permaite criar cópias de segurança e restaurá-las caso necessário. Para acessar esse recurso é preciso inserir um meio de armazenamento externo USB ou outro, e logo após, o macOS automaticamente perguntará ao usuário se deseja utilizar esse dispositivo como Time Machine. Se não, também é possível configurar essa função manualmente.

Para acessar esse recurso de forma manual é necessário ir até Utilidade de Discos, selecionar o disco, clicar na aba de apagar e, por último, abrir as preferências do Time Machine em Preferências do Sistema.

Você pode encontrar mais informações no site de **Suporte de Apple.**

Que características uma boa ferramenta de backup deve ter?

Alguns usuários podem precisar de outro software de backup por necessidades particulares de seus aplicativos. Por isso, a seguir, mencionamos cinco características a serem consideradas antes de escolher um programa desse tipo:

- ✓ Que ofereça a possibilidade de selecionar manualmente a informação a ser copiada.
- ✓ Que permita criar um padrão do equipamento para restaurar o sistema operacional, os programas e arquivos de forma completa a partir de um disco de inicialização.
- ✓ Que possa estabelecer uma senha de proteção para acessar os dados e que criptografe a informação.
- ✓ Que comprima os arquivos copiados para economizar espaço de armazenamento.
- ✓ Que permita selecionar a frequência de backup dos arquivos.

Antivírus + Backup: duas soluções que se complementam

É importante considerar que um programa para copiar informações é complementar a uma solução de segurança, portanto, nenhum substitui ao outro.

Um software antivírus permite proteger o computador de ameaças e, assim, evitar infecções com ransomware, por exemplo, ou que criptografem a informação.

Por outro lado, uma solução de backup permite manter uma cópia de segurança da informação para poder restaurá-la mediante qualquer inconveniente, assim como vimos neste guia.

Ao cumprir objetivos distintos e complementários, recomendamos implementar ambos programas para alcançar um nível de proteção elevado.

Conclusão

A informação é um dos ativos mais importantes para as empresas e para as pessoas, portanto, realizar backups frequentemente é uma tarefa que deve ser considerada como prioridade e em nenhum caso se pode subestimá-la. Isso se dá, principalmente, por diversos motivos que poderiam ocorrer em uma situação de perda de dados.

Para garantir a segurança de sua informação lembre-se de realizar esse procedimento da forma correta, ou seja, considerando a informação a ser protegida, os tipos de cópias existentes, os meios de armazenamento e a frequênica dos processos.

www.eset.com/br

esetbrasil @eset_brasil ESET-Brasil