Introdução à Segurança da Informação

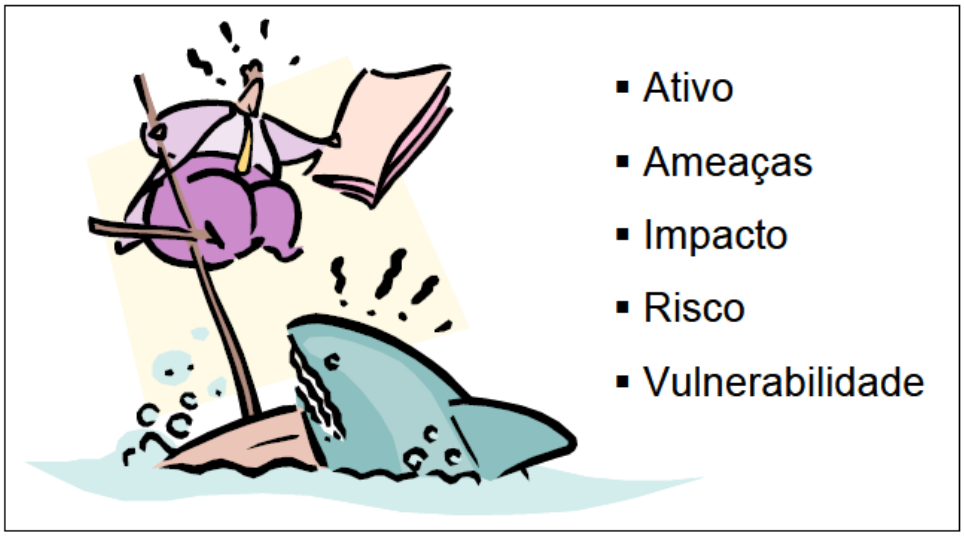
Segurança da informação é a proteção da informação e sistemas contra acesso, uso, divulgação, modificação, destruição e interrupção não autorizadas.

Os desafios para a implantação de um ambiente de segurança em qualquer empresa, independentemente do tamanho, são enormes. O maior problema é implementar as políticas e normas de segurança em um sistema real, que possui aplicações em funcionamento, hardware em produção, softwares proprietários e de terceiros e, acima de tudo, pessoas. É literalmente como trocar o pneu com o carro andando.

Como a maior parte das informações vitais para o sucesso de uma organização reside em computadores, perdas de dados podem ser catastróficas. Os riscos de um negócio com sistema de segurança da informação inadequado são incalculáveis. Segurança da informação é manter a confidencialidade, integridade e disponibilidade da informação. Ela abrange muito mais do que a segurança da informação de TI. Ela cobre a segurança de toda e qualquer informação da empresa, esteja ela em meios eletrônicos, papel ou até mesmo na mente dos funcionários.

Motivados pela busca de soluções para esses desafios, diversos profissionais de várias áreas e organizações, veem se esforçando para criar normas que sistematizem o trabalho de criar ambientes seguros de TI. Um desses resultados foi consolidado com a norma **ABNT NBR ISO/IEC 17799:2005**. Utilizando-se essa norma, que é um guia de melhores práticas, simplifica-se o trabalho de adoção e implementação de políticas e padrões definidos, bem como da posterior verificação da conformidade dos resultados alcançados.

Conceitos Básicos de Segurança da Informação



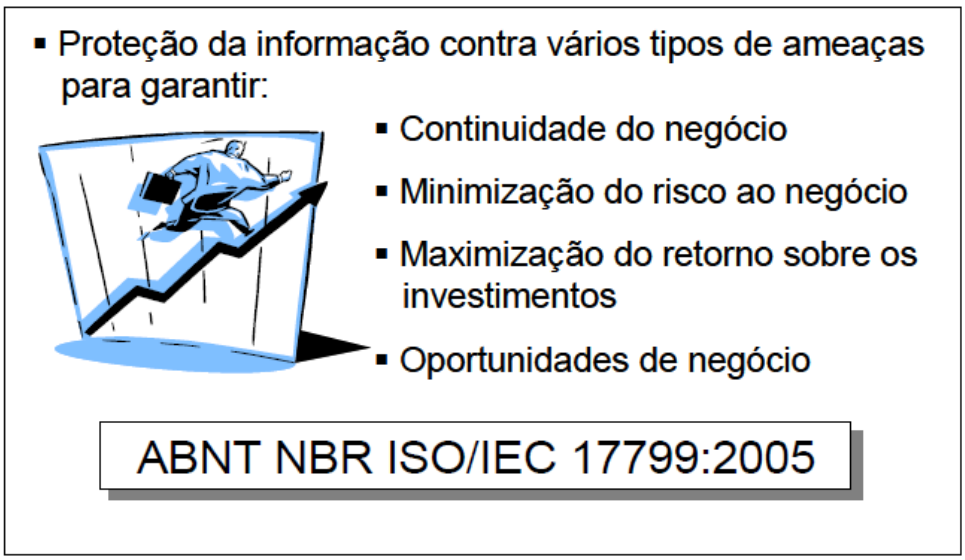
Toda e qualquer informação, que seja um elemento essencial para os negócios de uma organização, deve ser preservada pelo período necessário, de acordo com sua importância. A informação é um bem como qualquer outro e por isso deve ser tratada como um ativo.

A interconexão das empresas através de links cabeados e/ou sem fio (wireless), internos e/ou externos, pessoas e ações da natureza, pode expor vulnerabilidades que colocam em risco as informações. Assim, faz-se necessário a implantação de processos de segurança que protejam a informação contra essas ameaças.

A fim de proporcionar o bom entendimento das abordagens que serão feitas, é importante conceituarmos alguns termos.

- **Ameaça (threat):** causa potencial de um incidente indesejado, que caso se concretize pode resultar em dano.
- **Ativo (asset):** é qualquer coisa que tenha valor para um indivíduo ou uma organização, tais como, hardware de computadores, equipamentos de rede, edificações, software, habilidade de produzir um produto ou fornecer um serviço, pessoas, imagem da organização, etc...
- **Incidente de segurança (security incident):** é qualquer evento em curso ou ocorrido que contrarie a política de segurança, comprometa a operação do negócio ou cause danos aos ativos da organização.
- **Impacto (impact)**: consequências de um incidente de segurança.
- **Risco (risk)**: combinação da probabilidade da concretização de uma ameaça e suas consequências.
- **Vulnerabilidade (vulnerability):** fragilidade ou limitação de um ativo que pode ser explorada por uma ou mais ameaças.

OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO



Qualquer tipo de informação deve ser protegido, esteja ele escrito ou desenhado em papel, armazenado em meios magnéticos, em filmes ou falado.

"A segurança da informação é obtida através da implantação de controles adequados, políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware."

O objetivo da segurança da informação é garantir o funcionamento da organização frente às ameaças a que ela esteja sujeita. A norma ABNT NBR ISO/IEC 17799:2005 — estabelece diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Essa frase confirma que a norma está alinhada com os objetivos de todas as outras normas criadas com o mesmo fim.

É consenso das normas da área que os objetivos gerais da segurança da informação visam preservar a confidencialidade, integridade e disponibilidade da informação. Esse é um conceito da antiga ISO/IEC 17799:2000. Porém, é citado por se tratar de um conceito amplamente difundido.

Para ser possível manter a proteção diante das ameaças internas e externas existem alguns fundamentos básicos necessários em todas as empresas. Eles são essenciais para vencer os desafios do cibercrime:

- **Confidencialidade:** tem o objetivo de garantir que apenas pessoas autorizadas tenham acesso à informação. Essa garantia deve ser obtida em todos os níveis, desde a geração da informação, passando pelos meios de transmissão, chegando a seu destino e sendo devidamente armazenada ou, se for necessário, destruída sem possibilidade de recuperação. Esse processo tende a ser mais dispendioso, quanto maior for à necessidade de proteção da informação e, é claro, quanto maior for o valor da informação a ser protegida. Modernos processos de criptografia aliados a controles de acesso são necessários nessa etapa. É o modo de garantir que a informação estará acessível apenas para pessoas autorizadas. A principal forma de mantê-la é por meio da autenticação, controlando e restringindo os acessos. Ela impõe limitações aos milhares de dados sigilosos que as empresas possuem. Sem a confidencialidade, as empresas ficam vulneráveis a ciberataques, roubo de informações confidenciais e até utilização de dados pessoais de clientes, o que pode causar diversos prejuízos, inclusive financeiros. [1]
- **Integridade:** O objetivo da integridade é garantir que a informação não seja alterada, a não ser por acesso autorizado. Isso significa dizer que uma informação íntegra não é necessariamente uma informação correta, mas sim que ela não foi alterada em seu conteúdo. Esse processo é a proteção da informação contra modificações não autorizadas ou acidentais. O princípio de integridade refere-se a manutenção das condições iniciais das informações de acordo com a forma que foram produzidas e armazenadas. Ou seja, a informação mantém sua origem e ela não pode ser alterada, assim somente pessoas autorizadas poderão acessar e modificar os dados do sistema. Quando o processo é executado estrategicamente é possível utilizar ferramentas para realizar a recuperação de informações danificadas ou perdidas. [1]
- **Disponibilidade:** Garantir que a informação sempre poderá ser acessada quando for necessário. Esse objetivo é conseguido através da continuidade de serviço dos meios tecnológicos, envolvendo políticas de backup, redundância e segurança de acesso. De nada adianta ter uma informação confiável e íntegra se ela não está acessível quando solicitada. Os dados

corporativos precisam estar seguros e disponíveis para serem acessados a qualquer momento pelos usuários autorizados. Esse princípio diz respeito à eficácia do sistema e do funcionamento da rede para que seja possível utilizar a informação quando necessário. Ela deve ser hospeda em um sistema à prova de falhas lógicas e redundantes. Na hora de gerar relatórios para auditoria, por exemplo, é necessário que os dados possam ser facilmente encontrados e processados. Esse é o princípio da disponibilidade. [1]

- **Autenticidade:** Esse processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação. Ou seja, autenticidade é quando um usuário vai manipular algum dado e ocorre uma documentação sobre essa ação. [1]

Todos esses métodos são importantes para garantir a segurança das informações corporativas das possíveis ameaças, que podem ter origens tanto externas quanto internas. Elas podem ser uma pessoa, um evento ou uma ideia capaz de causar danos ao sistema.

- As ameaças externas são tentativas de ataque ou desvio de informações vindas de fora da empresa, normalmente originadas por pessoas com a intenção de prejudicar a corporação.
- As internas podem ser causadas por colaboradores de forma intencional, ou não. Essas ameaças podem causar pequenos incidentes e até prejuízos graves, por isso também devem ser levados em conta na hora do planejamento dos processos de segurança da empresa.

É importante que o profissional de SI mantenha sempre em alta a importância da segurança dos dados corporativos entre todos os usuários. Há diversas formas de manter a proteção da informação e não apenas criando mecanismos que realizam esse trabalho, mas desenvolver projetos que envolvam os usuários para conscientizá-los.

A ABNT NBR ISO/IEC 17799:2005 amplia o conceito acima enfatizando mais os resultados da implantação de um ambiente de segurança da informação, quando define que —segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Ameaças à Segurança da Informação

Malware é a abreviação de "software malicioso" (em inglês, malicious software) e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas. O malware pode infectar computadores e dispositivos de várias maneiras, além de assumir diversas formas, entre elas vírus, worms, cavalos de Troia, spyware e outros. [2]

As ameaças cibernéticas são agora muito comuns. As estatísticas sobre eventos de falha na cibersegurança e brechas de rede bem sucedidas continuam uma tendência que favorece os atacantes.

O resultado dessas ameaças volumosas e persistentes tem sido de centenas de milhões de dólares em negócios perdidos, sem contar os custos a longo prazo da diminuição da confiança do cliente e cidadão. [2]

As ameaças mais comuns à Segurança da Informação são:

Fator humano

O fator humano na segurança de TI é a única maior ameaça à nossa segurança cibernética empresarial. Os usuários, em geral, de todas as áreas de uma organização são um buraco intrínseco de segurança.

A “vulnerabilidade humana” pode ser oriunda de uma ameaça interna, bem como de fontes externas — nosso comportamento sendo usado contra nós como o motor da ameaça cibernética.

Uma ameaça interna ou Insider é uma grande preocupação para todas as organizações. Geralmente, ela é consequência do acesso e do uso errado de dados sensíveis, incluindo o vazamento de dados aos fornecedores para minar os poderes de negociação da companhia.

Outra coisa que os cibercriminosos usam para sua vantagem é entender como os seres humanos se comportam através de Engenharia Social. Eles usam nosso comportamento contra nós para ter um ataque bem-sucedido.

Scan

É um ataque que quebra a confidencialidade com o objetivo de analisar detalhes dos computadores presentes na rede (como sistema operacional, atividade e serviços) e identificar possíveis alvos para outros ataques.

A principal forma de prevenção é a manutenção de um firewall na empresa e uma configuração adequada da rede. [4]

Worm

Worms são alguns dos malwares mais comuns e antigos. Malwares são softwares com o intuito de prejudicar o computador “hospedeiro”.

Essa categoria engloba tanto os vírus quanto os worms, entre diversos outros tipos de programas maliciosos.

Os worms são perigosos devido à sua capacidade se espalhar rapidamente pela rede e afetar arquivos sigilosos da empresa. [4]

Rootkit

Esta é uma ameaça que teve origem na exploração de kits do Linux. Tem como objetivo fraudar o acesso, logando no sistema como root, ou seja, usuário com poder para fazer qualquer coisa.

Os ataques de rootkit são feitos a partir de um malware. Quando a máquina é infectada, os arquivos maliciosos se escondem no sistema e, com essa discrição, liberam o caminho para os invasores agirem.

Apesar de seu surgimento no Linux, o malware é capaz de causar danos nos sistemas operacionais Windows e Mac. Sem dúvidas, trata-se de um grande perigo para ambientes corporativos. [4]

DDoS (negação de serviço)

Os ataques de negação de serviço, mais conhecidos como DDoS (Distributed Denial of Service), estão entre os mais frequentes. Eles têm como objetivo tornar um sistema, infraestrutura ou servidores indisponíveis, causando interrupção dos serviços.

Como isso acontece? Ao receber o ataque, o alvo é sobrecarregado de diferentes formas (uso de banda larga, falhas de software ou excessivo uso de recursos), o que pode gerar muito prejuízo à vítima. [4]

Ransomware

A família ransomware é um conjunto de vírus do tipo malware e tem sido massivamente utilizada para a prática de crimes de extorsão de dados — prática também conhecida como sequestro de dados.

O modo como o ransomware age varia conforme a sua versão, pois cada malware lançado explora uma diferente brecha do sistema operacional. Esse detalhe, inclusive, é o que torna os ataques tão repentinos e, ao mesmo tempo, fatais.

Embora a maneira como o vírus se manifesta varie, a finalidade é a mesma: bloquear todos os arquivos do computador, impedindo que o sistema possa ser utilizado adequadamente, e encaminhando mensagens solicitando o pagamento pelo resgate.

Algumas empresas chegaram a negociar valores milionários com os criminosos para que os dados fossem devolvidos.

Contudo, fazer o pagamento não é uma atitude recomendável, porque não há garantias de que a situação se normalize — além de acabar estimulando o crime.

Devido ao número de ataques, o ransomware é visto atualmente como a maior das ameaças. [4]

Vírus de resgate

Conforme a expansão dos ataques de ransomware foi acontecendo, muitos usuários (a maioria corporativos) se desesperaram por não saber como agir diante do sequestro de dados.

A recomendação é sempre evitar o pagamento pelo resgate e utilizar uma solução para recuperar os arquivos — de preferência desenvolvida por fabricantes confiáveis.

Contudo, os cibercriminosos buscaram driblar isso ao criar um vírus que ativa a oferta de um programa para resgatar os dados sequestrados. Ou seja, é um vírus que oferece outro para que o usuário pague por uma solução ilegítima. [4]

Antivírus falsos

Selecionar os produtos de antivírus não é uma tarefa simples como parece, visto que existem soluções que, na verdade, são raízes para problemas ainda maiores que sua rede possa estar enfrentando.

Da mesma maneira que existe o vírus de resgate, uma nova onda de antivírus falsos, os quais oferecem um produto para rastrear ameaças e limpar o computador.

Esses vírus são conhecidos como do tipo locker (bloqueador), assim como o ransomware e o malware, solicita pagamentos por bitcoins ou cartão de crédito. [4]

Phishing

A prática de phishing consiste no envio de mensagens de email, onde o invasor se passa por uma instituição legítima e confiável (geralmente bancos e serviços de transação online), induzindo a vítima a passar informações cadastrais.

Essa é uma das mais antigas armadilhas conhecidas na Internet e, ainda assim, continua atraindo muitas vítimas que utilizam email.

Ultimamente o phishing vem sendo utilizado em ataques de BEC (Business Email Compromise), que tem como propósito fazer com que representantes da empresa alvo pensem estar se comunicando com executivos.

Dessa maneira, as instituições acabam fazendo depósitos em conta de terceiros sem saber que se trata de uma fraude. O pior disso tudo é que o criminoso não deixa rastros, pois a mensagem não contém nenhum anexo ou links. [4]

Keylogger

Keylogging (em português, registro de tecla) é a ação de gravar/registrar (logging) as teclas pressionadas em um teclado, normalmente de maneira secreta, para que a pessoa que usa o teclado não saiba que suas ações estão sendo monitoradas. Os dados podem ser recuperados pela pessoa que opera o programa de registro. Um keylogger pode ser um software ou hardware.

Apesar dos programas, propriamente ditos, serem legais, com muitos deles sendo projetados para permitir que os empregadores supervisionem o uso de seus computadores, os keyloggers costumam ser usados para roubar senhas e outras informações confidenciais.

O keylogging também pode ser usado para estudar a interação homem-computador. Existem vários métodos de keylogging: eles vão desde abordagens baseadas em hardware e software até análises acústicas.

Man-in-the-middle

O man-in-the-middle (pt: Homem no meio, em referência ao atacante que intercepta os dados) é uma forma de ataque em que os dados trocados entre duas partes (por exemplo, você e o seu banco), são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vitimas se apercebam.[1] Numa comunicação normal os dois elementos

envolvidos comunicam entre si sem interferências através de um meio, aqui para o que nos interessa, uma rede local à Internet ou ambas.

Durante o ataque man-in-the-middle, a comunicação é interceptada pelo atacante e retransmitida por este de uma forma discricionária. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação.

Como os participantes legítimos da comunicação não se apercebem que os dados estão a ser adulterados tomam-nos como válidos, fornecendo informações e executando instruções por ordem do atacante.

Cibercrime

Cibercrime é o nome dados aos crimes cibernéticos que envolvam qualquer atividade ou prática ilícita na rede. Essas práticas podem envolver invasões de sistema, disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso a informações confidenciais e tantos outros. O cibercrime compreende também os crimes convencionais realizados por meio de dispositivos eletrônicos ou que incluam a utilização de alguma ação digital como instrumento para a prática do crime.

O termo "cibercrime" (ou "cybercrime", em inglês) apareceu em uma reunião de um subgrupo do G-8 (grupo composto pelos sete países mais ricos do mundo, mais a Rússia, por sua importância histórica e militar) próximo do final dos anos 90. Essa reunião abordava exatamente as maneiras e os métodos utilizados para combater as práticas ilícitas da internet.

Uma das fortes características do cibercrime é a predominância transnacional, o que dificulta as investigações e a apuração de provas contra o acusado. Outra característica também tem relação com o aumento dos computadores pessoais, que permitem que qualquer pessoa no mundo possa realizar práticas criminosas contra indivíduos de qualquer lugar do planeta sem mesmo sair de casa.

A prática do cibercrime é tão comum que, segundo dados divulgados pela Norton, empresa especializada em segurança digital, cerca de 65% dos internautas já foram vítimas de alguma forma de cibercrime. A maior dificuldade para combater esses crimes é a falta de leis e punições eficientes em diversos países na luta contra os crackers.

Existem vários tipos de cibercrimes e esse fato deixa as autoridades com ainda mais dificuldades para punir os transgressores, por falta de leis aplicáveis a determinadas infrações. Veja abaixo alguns dos principais crimes cibernéticos:

- **Pornografia Infantil:** maliciosos utilizam a internet e dispositivos de acesso para criar e distribuir materiais com conteúdo pornográfico de crianças e menores de idade.
- **Lavagem de dinheiro:** esse tipo de crime é bastante comum. Os criminosos realizam transferências de dinheiro de maneira ilegal com o objetivo de esconder a sua fonte e também o seu destino.
- **Ciberterrorismo:** esse crime é mais comum em países desenvolvidos e de conflitos políticos, mas também pode ser visto em larga escala em outros lugares do mundo. Consiste em ações premeditadas com motivações políticas

cometidas, geralmente, contra governos, partidos e instituições governamentais. Também podem ser cometido amplamente contra civis.

- **Ciberativismo:** crime praticado contra organizações que defendem determinadas causas. Esse cibercrime envolve roubo de informações e manipulações nos materiais que são divulgados ao público e à imprensa.
- **Roubo:** envolve a utilização de computadores ou outros dispositivos para desviar fundos ilegalmente, roubar dados de outros indivíduos, empresas ou instituições, para realizar espionagem, roubo de identidade, fraude, plágio e pirataria.

Para prevenir-se contra cibercrimes, especialistas orientam que os internautas tomem o máximo de cuidado ao navegar na internet. Também alertam sobre emails suspeitos e anexos maliciosos, especialmente em formato .exe, que são enviados por remetentes desconhecidos. É importante procurar evitar sites pouco conhecidos e banners, links e ofertas que ofereçam benefícios muito especiais e duvidosos.

Manter o antivírus e o firewall sempre atualizados, além de outras ferramentas de segurança do computador, bem como o próprio sistema operacional, também é de suma importância para evitar ser vítima desses ataques cibernéticos. [5]

Antivírus

Antivírus é um software que detecta, impede e atua na remoção de programas de software maliciosos, como vírus e worms. São programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário.

Existem diversas formas de uma máquina contrair vírus. Eles podem aparecer por meio de pendrives, emails, sites de conteúdo erótico ou duvidoso, download de arquivos e programas infectados e por vários outros meios. Esses vírus e códigos maliciosos possuem a finalidade de interferirem no funcionamento do computador ou outro aparelho para registrar, corromper, destruir dados e transferir informações para outras máquinas.

O antivírus, contudo, possui vários métodos de identificação para impedir a entrada de vírus, incluindo atualização automática, escaneamento, quarentena e outros meios. Alguns dos principais métodos podem ser lidos em detalhes abaixo:

- Escaneamento de vírus conhecidos - Assim que um novo vírus é descoberto, o antivírus desmonta seu código e o separa em grupos de caracteres chamados de string que não são encontrados em outros programas do computador. A partir daí, a string começa a identificar esse vírus, enquanto o antivírus faz uma varredura pelo sistema para identificá-lo em algum programa. Caso encontrado, o antivírus notifica o usuário e deleta o arquivo automaticamente, enviando para um espaço que pode ser visualizado posteriormente pelo usuário.
- Sensoriamento heurístico - Trata-se do segundo passo de uma execução quando o usuário solicita o escaneamento da máquina. O antivírus, por meio de um método complexo e muitas vezes sujeito a erros, realiza a varredura de todo o sistema em busca de instruções que não são executáveis nos programas usuais.

Muitas vezes pode apresentar erros por necessitar gravar sobre ele mesmo, ou outro arquivo, dentro de um processo de reconfiguração ou atualização.

- Busca algorítmica - trata-se de uma busca que utiliza algoritmos para encontrar os resultados.
- Checagem de integridade - refere-se ao mecanismo que registra dígitos verificadores em um banco de dados para que possa ser consultado futuramente pelo antivírus com objetivo comparativo. Quando uma nova checagem é realizada, o sistema utiliza o banco de dados com as informações armazenadas para fazer comparações a fim de se certificarem de que não existem alterações nos dígitos verificadores. [6]

Backup

A palavra “backup” significa reforço e passa a ideia de uma proteção extra, uma ajuda para guardar algo importante. Na informática, o termo tem o sentido de cópia de segurança: recurso usado para se proteger contra a perda de dados, permitindo recuperá-los em caso de imprevistos. [7]

O conceito de backup

A palavra “backup” tem origem no inglês e significa reforço. Essa expressão dá a ideia de uma proteção extra, uma ajuda para guardar algo importante.

Dentro do contexto da gestão de dados eletrônicos e ativos digitais, isso faz todo o sentido, já que o termo backup pode ser traduzido de forma mais fiel como cópia de segurança.

O objetivo de ter backups é se proteger contra a perda de documentos digitais. As cópias de segurança permitem que você consiga recuperar dados perdidos com facilidade. [7]

A importância das cópias de seguranças

Alguns donos de empresas acreditam que ter um bom computador é o suficiente para garantir que nenhuma informação valiosa vai se perder.

Mas esse conceito está errado e pode gerar transtornos para todos na empresa. Afinal de contas:

- um computador está sujeito a pegar algum vírus que afete todas as coisas armazenadas nele;
- por uma desatenção você pode apagar algum dado errado e perder informações importantes;
- existe a possibilidade de acontecer um roubo em sua empresa, de forma que seu computador seja levado com a única cópia dos dados;

- o uso incorreto dos computadores também pode gerar bugs e perda de informações valiosas.

Algumas informações da sua empresa são exigidas durante uma fiscalização, e é da sua responsabilidade manter cada uma delas arquivada em segurança.

Por isso, independente da sua motivação, é importante se proteger contra a perda dos seus dados, evitando assim transtornos no seu dia a dia e problemas com a fiscalização.

Tipos de backup

Para começar a fazer as suas cópias de segurança, você precisa entender que nem todo backup é igual e cada situação exige um tipo diferente de backup.

Como saber se você vai fazer as suas cópias de segurança do jeito que precisa? Para isso, vamos listar 4 tipos de backups e como funciona cada um deles.

1. Backup completo

O backup completo faz uma cópia de todos os arquivos que você tem no computador. Nesse processo, se você usa um sistema de automatização, é feita uma marcação nos dados copiados, de forma que tais cópias não se dupliquem.

Você precisa fazer o backup completo apenas na primeira vez, depois há outros métodos para manter a sua cópia de segurança atualizada e completa.

2. Backup incremental

Esse tipo de backup serve para fazer cópias apenas dos arquivos que foram alterados ou criados do zero após o backup normal. Como o nome sugere, esse tipo de cópia incrementará as novas informações dos documentos que já estavam salvos anteriormente.

A vantagem de se fazer esse processo é que não será necessário muito tempo para completar todo o processo e ter os seus dados seguros.

Quando feito de modo automatizado, os dados copiados pelo backup incremental são marcados para que não sejam feitas novas cópias de um mesmo arquivo.

3. Backup diferencial

Assim como o incremental, o backup diferencial faz a cópia dos arquivos criados ou modificados desde o backup anterior. Ele recebe esse nome porque apenas o que é diferente da cópia anterior é armazenado.

Nesse caso, ao fazer uso de sistemas de automação, o backup não é marcado. Em outras palavras, esses arquivos podem ter cópias repetidas, o que exigirá que você tenha mais espaço para armazenamento, tornando o backup um processo mais demorado.

A principal vantagem do backup diferencial é que, em casos de perda de dados, o tempo para ter acesso às cópias de segurança será menor.

4. Backup diário

O backup diário diz respeito a cópias de segurança de todos os documentos feitas diariamente. Ele é importante para quem precisa ter a confiança da data de um arquivo.

Os sistemas de cópias de segurança fazem uma marcação na data em que foram feitos os backups e não nos arquivos copiados. Assim, no seu armazenamento, você terá uma cópia de todos os seus documentos diariamente.

Locais para armazenar seu backup

Até agora você conseguiu ver como é importante fazer o backup e que existem várias formas de fazê-lo. Mas é preciso selecionar bem onde manter as cópias de segurança. Será que ter vários computadores com o mesmo conteúdo é a solução? Não!

Como você já sabe, os computadores têm uma capacidade limitada de armazenar informação, de forma que ter vários deles com as mesmas informações pode tornar essa ferramenta de trabalho lenta e gerar transtornos no seu dia a dia.

Então onde é indicado que você tenha as cópias de segurança? Conheça agora 4 modos de armazenar os seus dados.

Pendrives

Os pendrives são pequenos dispositivos de entrada USB que permitem a gravação de dados. Eles são muito versáteis, já que permitem que os arquivos salvos sejam editados e dão a você a possibilidade de ter sempre consigo as informações de que precisa.

A desvantagem de usar os pendrives para a gravação de dados é a capacidade de armazenamento do dispositivo. Caso você tenha muitos arquivos, será necessário o uso de mais de um pendrive.

HD externo

O HD é responsável por guardar todas as informações do seu computador. Quanto ao HD externo, trata-se de um dispositivo que funciona com uma entrada USB e tem a mesma função daquele que está dentro do seu computador, ou seja, armazena dados.

A vantagem de fazer uso dessa ferramenta para os backups é a grande capacidade de armazenamento. Ele também se conecta com muita facilidade a diversos computadores e pode ser guardado dentro de um cofre, caso você precise de algo extremamente seguro.

Nuvem

É possível encontrar diversos servidores online que permitem o armazenamento de dados. Para isso não é preciso ter nenhum dispositivo físico, como os pendrives ou o HD externo. Esse tipo de armazenamento é conhecido como “nuvem”.

Alguns dos servidores mais usados para isso são:

- Google Drive;
- Dropbox;

- iCloud.

Optar por manter os seus backups salvos na nuvem é totalmente seguro, afinal, para ter acesso aos dados é preciso usar login e senha.

Outra vantagem desse método de armazenamento dos seus backups é a facilidade de acessar as informações. Você poderá acessá-las de outro computador ou de dispositivos móveis, como tablets e celulares.

Com o recurso de nuvem, você tem a possibilidade de fazer cópias de segurança de informações importantes que estão salvas no seu celular ou tablet, não apenas do que está no computador.

RAID

RAID é sigla de Redundant Array of Inexpensive Disks, que quer dizer Matriz Redundante de Discos Independentes.

De modo simples e resumido, RAID quer dizer que você pode ter vários discos rígidos, ou seja, HDs formando uma única unidade. Assim, os dados de um disco são os mesmos dados do outro. Afinal, são vários HDs funcionando como se fossem um.

Mas qual é a vantagem disso? Caso haja falhas em um dos discos, todos os outros continuarão funcionando normalmente, sem que informações sejam perdidas.

O RAID é uma ótima ferramenta para backups e também para evitar que o seu fluxo de trabalho seja interrompido por falta de informações.

Maneiras de automatizar os backups

Fazer backups rotineiramente e de modo manual é muito trabalhoso e pode gerar muitos erros. Por isso, você precisa usar ferramentas de automação para esse importante processo.

A maioria dos sistemas operacionais de computador, como o Windows, contam com assistentes nativos que auxiliam você nesse processo.

Além deles, existem softwares com versões pagas e gratuitas que oferecem criptografia, diferentes tipos de backup, possibilidade de agendamento da cópia de segurança e sincronização com outros dispositivos e com a nuvem.

Alguns dos softwares que podem ajudar você nesse processo são:

- Acronis Backup;
- Paragon Backup;
- Backup Maker;
- Uranium Backup;
- Comodo Backup.

Como você viu, ter um backup dos seus arquivos pode evitar muitos transtornos e problemas com a fiscalização. Por isso, não deixe de sempre fazer cópias de segurança dos seus

dados, visto que esse é o melhor método para que você tenha tranquilidade e a convicção de que suas informações estarão sempre em segurança. [7]

Obras Citadas

[1] Westcon, “SAIBA QUAIS SÃO OS 4 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO,” CANAL SYNNEX WESTCON, 2019. [Online]. Available: https://blogbrasil.westcon.com/saiba-quais-sao-os-4-principios-da-seguranca-da-informacao. [Acesso em 01 Maio 2020].

[2] “Aprenda sobre malware e como proteger todos os seus dispositivos contra eles,” Kaspersky, [Online]. Available: https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it. [Acesso em 1 Maio 2020].

[3] “Conheça 6 ameaças à segurança da informação nas empresas,” IP5 Tecnologia, 16 Maio 2017. [Online]. Available: http://blog.ip5tecnologia.com.br/conheca-6-ameacas-a-seguranca-da-informacao-nas-empresas/.

[4] “Segurança da informação: entenda as principais ameaças,” Alerta Security, 20 Agosto 2018. [Online]. Available: https://www.alertasecurity.com.br/seguranca-da-informacao-entenda-as-principais-ameacas/.

[5] “O que é cibercrime?,” Canaltech, [Online]. Available: https://canaltech.com.br/seguranca/O-que-e-cibercrime/. [Acesso em 01 Maio 2020].

[6] “O que é um antivírus?,” Canaltech, [Online]. Available: https://canaltech.com.br/antivirus/o-que-e-antivirus/. [Acesso em Janeiro 2020].

[7] D. Moraes, “O que é backup e como fazer a cópia de segurança das suas informações,” Rock Content, 4 Janeiro 2019. [Online]. Available: https://rockcontent.com/blog/backup/.