FUNDAMENTOS DE SISTEMAS DE INFORMAÇÃO

AULA 3

Profª Vívian Ariane Barausse de Moura

CONVERSA INICIAL

Nos últimos anos, fraudes cibernéticas e *crakers*/*hackers* tornaram-se muito comuns e, portanto, as empresas digitalizadas precisam garantir que os dados confidenciais do cliente, como informações de cartão de crédito, bem como registros bancários, além de dados relativos a transações financeiras das empresas, sejam protegidos. De fato, algumas das atuais políticas de sistemas de informação (SI) fazem fronteira com proteção e segurança extremas, para que os dados não sejam roubados, levando a ações legais e regulatórias.

A razão para tal questão é que a *dark web* surgiu como o lugar onde qualquer um e todos podem postar e vender coisas, bem como comprar esses dados críticos e, portanto, as empresas estão cada vez mais recorrendo a empresas especializadas em segurança de SI, para ajudá-las a formular políticas eficazes de proteção de dados. Afinal, lemos sobre roubo de dados quase diariamente, o que tem um efeito cascata na psique do cliente e de outras partes interessadas, pois eles começam a insistir para que seus fornecedores tenham políticas de sistemas de informação adequadas e abrangentes.

Segue a apresentação da etapa, com a sua estrutura de contéudos trabalhados nestes tópicos:

a. **Conceitos fundamentais de infraestrutura e segurança da informação**
b. **Gestão e armazenamento de dados: vulnerabilidades e segurança**

- Ferramentas para segurança da informação
- Medidas de segurança: senha e *backup*

c. **Gestão e armazenamento de dados**
d. **Redes de computadores**

- Redes organizacionais: LAN e WAN

e. **Recursos na nuvem**

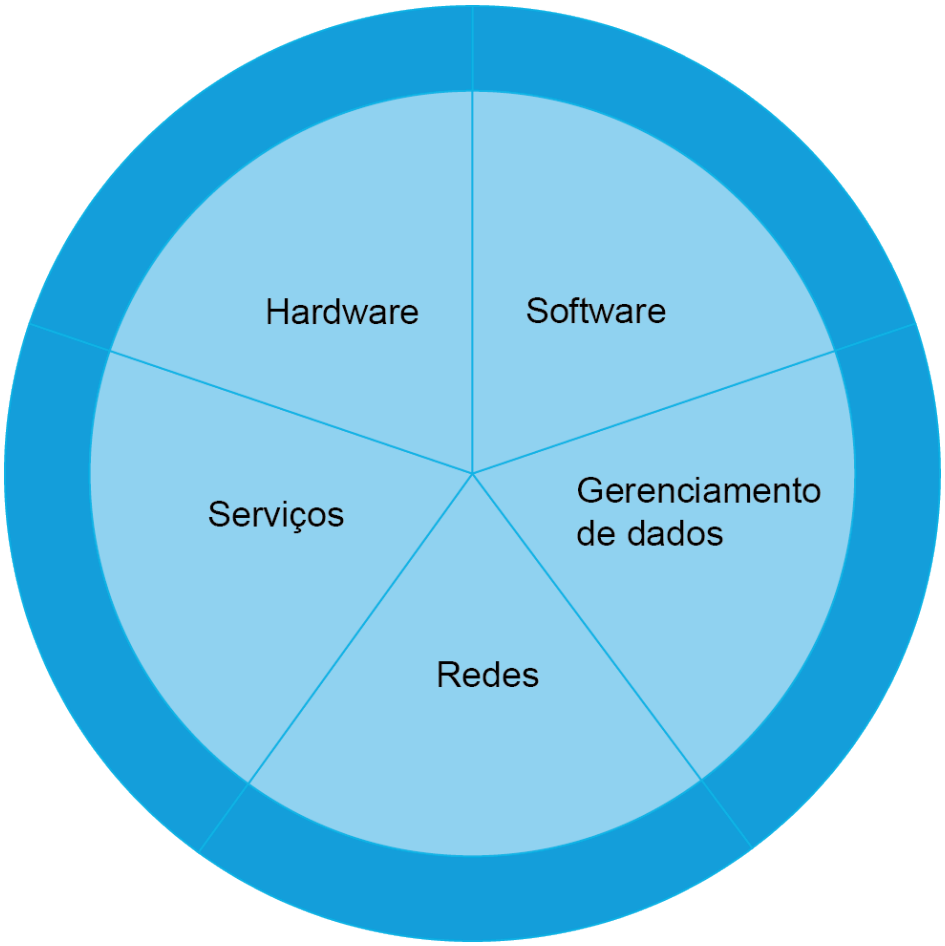
O objetivo desta etapa é introduzir os principais conceitos e temas pertinentes aos componentes da infraestrutra e segurança de tecnologia de informação (TI). Sendo assim, é preciso saber as vunerabilidades da segurança da gestão e armazenamento de dados, assim como as questões envolvendo as medidas de segurança dos SI, com base nos principais conteúdos relacionados à segurança e ao controle das informações em uma empresa, bem como a importância da análise de riscos e as principais ameaças decorrentes do

mapeamento desses riscos. Aprenderemos também aspectos inerentes à rede de computadores e recursos na nuvem.

TEMA 1 – CONCEITOS FUNDAMENTAIS DE INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

À medida que os computadores e outros dispositivos digitais se tornaram essenciais para os negócios e o comércio, eles também se tornaram, cada vez mais, alvos de ataques. Para que uma empresa ou um indivíduo use um dispositivo de computação com confiança, eles devem primeiro ter certeza de que o dispositivo não está comprometido de forma alguma e que todas as comunicações serão seguras. Retomando alguns conceitos, na Figura 1, tem-se apresentada "[...] a infraestrutura de TI, composta por: hardware, software, tecnologias de gestão de dados, tecnologias de rede e telecomunicações e serviços de tecnologias". (Laudon; Laudon, 2014, p. 147).

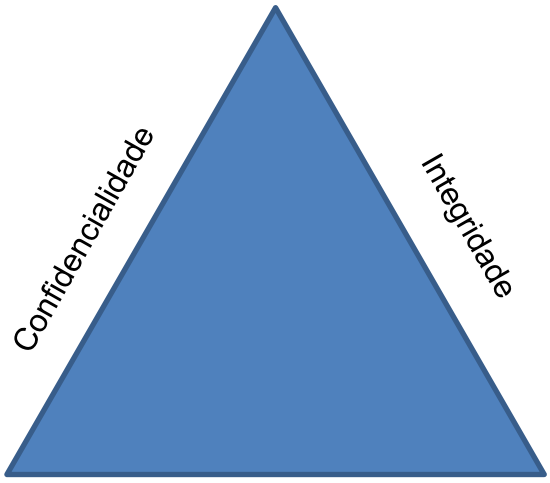
Figura 1 – Componentes da infraestrutura de TI



Fonte: Laudon; Laudon, 2014, p. 147.

O fluxo de informações faz parte do conhecimento pleno da organização e é de extrema importância para a manutenção e desenvolvimento da empresa. Esse conhecimento deve ser preservado e mantido em sigilo e envolve a segurança empresarial. De acordo com Caiçara Junior (2015, p. 157), “a segurança deve ser entendida como o conjunto de meios processos e medidas que visam efetivamente a proteção empresarial”.

O autor também defende que existe uma crença de que os valores utilizados na segurança consistem em gastos, quando, na verdade, são investimentos que preservam a organização, visto que são realizados em sistemas relacionados à produtividade, qualidade do produto e eficiência, que podem ser comprometidos por uma sabotagem e até mesmo falta de treinamento do pessoal (Caiçara Junior, 2015). Existem várias medidas diferentes que uma empresa pode tomar para melhorar a sua segurança, representadas pela tríade de SI: confidencialidade, integridade, disponibilidade.



Ao proteger nossas informações, queremos restringir o acesso, a elas, por parte de terceiros a quem não queremos permitir esse acesso. Essa é a essência da confidencialidade. Por exemplo, a legislação exige que as universidades restrinjam o acesso às informações particulares dos alunos. A universidade deve certificar-se de que apenas aqueles que estão autorizados têm acesso para visualizar os registros de notas, por exemplo.

Integridade é a garantia de que as informações acessadas não foram alteradas e representam verdadeiramente o que se pretende registrar. Assim como uma pessoa com integridade significa uma pessoa confiável para representar consistentemente a verdade, uma informação com integridade

significa que a informação realmente representa o significado pretendido. As informações podem perder sua integridade por meio de intenção maliciosa, como quando alguém não autorizado faz uma alteração para deturpar algo intencionalmente. Um exemplo disso seria quando um *hacker* é contratado para entrar no sistema de uma universidade e alterar uma nota. A integridade também pode ser perdida involuntariamente, como quando um pico de energia do computador corrompe um arquivo ou alguém autorizado a fazer uma alteração exclui acidentalmente um arquivo ou insere num sistema informações incorretas.

A disponibilidade de informações é a terceira parte da tríade. Disponibilidade significa que as informações podem ser acessadas e modificadas por qualquer pessoa autorizada a fazê-lo, em um prazo apropriado. Dependendo do tipo de informação, o prazo adequado pode significar coisas diferentes. Por exemplo, um corretor de ações precisa que as informações estejam disponíveis imediatamente, enquanto um vendedor pode ficar feliz em obter os números de vendas do dia em um relatório na manhã seguinte. Empresas como a Amazon exigirão que seus servidores estejam disponíveis 24 horas por dia, 7 dias por semana. Outras empresas podem não sofrer se seus servidores *web* ficarem inativos por alguns minutos, de vez em quando.

Caiçara Junior (2015, p. 158) destaca que

> [...] a falta de segurança pode trazer prejuízos tangíveis e intangíveis, e Alguns podem comprometer o próprio negócio. Podemos citar alguns efeitos decorrentes da falta de segurança: perda de oportunidades de negócio, perda de produtividade, perda de mercado, atrasos na entrega de produtos ou serviços, desgaste da imagem, perda de credibilidade com os clientes, entre outros.

Para evitar esse cenário, o autor relata a importância de se tomar medidas protetivas quando da implantação de medidas de segurança, conforme podemos observar no Quadro 1 (Caiçara Junior, 2015).

Quadro 1 – Questões a serem respondidas sobre implantação de medidas de segurança

Perguntas a serem realizadas pela empresa:
1. Quanto tempo a empresa sobreviverá sem os recursos de informática?
2. Quais ameaças poderão afetar o negócio?
3. O que deverá ser protegido?
4. Quem será afetado se ocorrer um desastre?

5. Qual é a capacidade de recuperação da empresa, ou seja, em quanto tempo ela voltará a operacionalizar suas atividades e a que custo?
6. Que recursos serão disponibilizados para a segurança da informação?

Fonte: Caiçara Junior, 2015, p. 158.

Nesse contexto, fica evidente que a segurança dos sistemas de informação é uma preocupação não apenas técnica como principalmente administrativa, levando em consideração tudo o que está envolvido nesses recursos, pois, além das instalações físicas e dos equipamentos, devem ser considerados os usuários: executivos, acionistas, clientes, entre outros. Assim, Caiçara Junior (2015, p. 160) afirma que as funções básicas de segurança dos SI devem estar alinhadas conforme o Quadro 2.

Quadro 2 – Funções básicas de segurança de SI

dissuasão	para que ocorra o desencorajamento da prática de irregularidades
prevenção	com o intuito de reduzir a ocorrência dos riscos
detecção	para sinalizar a ocorrência dos riscos
contenção	limitar o impacto do risco
recuperação	ter alternativa para a continuidade operacional
restauração	corrigir os danos causados pelos riscos

Fonte: Caiçara Junior, 2015, p. 160.

A segurança da informação e a proteção de dados são centrais para as políticas de tecnologia de qualquer organização e mais ainda quando os processos e metodologias organizacionais são totalmente virtuais, tornando-os mais vulneráveis ao roubo de dados.

TEMA 2 – GESTÃO E ARMAZENAMENTO DE DADOS: VULNERABILIDADES E SEGURANÇA

Uma vulnerabilidade de sistema de computador é uma falha ou fraqueza em um sistema ou rede que pode ser explorada para causar danos ou permitir que um invasor manipule o sistema de alguma forma. Existem vulnerabilidades, no sistema de computador, no ativo da rede, por exemplo, em um computador, em um banco de dados ou até mesmo em um aplicativo específico, para começar.

A maneira como uma vulnerabilidade de computador é explorada depende da natureza da vulnerabilidade e dos motivos do invasor. Essas vulnerabilidades podem existir devido a interações imprevistas de diferentes programas de *software*, componentes do sistema ou falhas básicas em um programa individual. É importante saber que as vulnerabilidades estão presentes em praticamente todas as redes, e que não há como identificar e lidar com todas elas devido à natureza incrivelmente complexa da arquitetura de rede moderna. No entanto, você pode reduzir significativamente o risco de uma violação de dados ou evento semelhante conhecendo algumas das vulnerabilidades de rede mais comuns e encontrando maneiras de resolvê-las.

As vulnerabilidades de segurança do computador podem ser divididas em vários tipos, com base em diferentes critérios, como onde a vulnerabilidade existe, o que a causou ou como ela pode ser usada. Algumas categorias amplas desses tipos de vulnerabilidade incluem:

- Vulnerabilidades de rede: esses são problemas com o *hardware* ou o *software* de uma rede, que a expõem a uma possível intrusão de terceiros. Os exemplos incluem pontos de acesso Wi-Fi inseguros e *firewalls* mal configurados.
- Vulnerabilidades do sistema operacional (SO): essas são vulnerabilidades específicas, que podem ser exploradas para se obter acesso a um ativo no qual o SO está instalado ou para causar diversos danos. Os exemplos disso incluem contas de superusuários padrões que podem existir em algumas instalações de SO e programas de *backdoor* ocultos.
- Vulnerabilidades humanas: o elo mais fraco, em muitas arquiteturas de segurança cibernética, é o elemento humano. Os erros do usuário podem expor facilmente dados confidenciais, criar pontos de acesso exploráveis para invasores ou interromper sistemas.
- Vulnerabilidades do processo: algumas vulnerabilidades podem ser criadas por controles de processos específicos (ou pela falta deles). Um exemplo seria o uso de senhas fracas, que também podem se enquadrar em vulnerabilidades humanas.

As organizações e pessoas, em geral, assumem que a segurança de sua rede está boa como está – pelo menos, até que algo dê errado e a organização sofra uma interrupção de serviço ou violação de dados devido a vulnerabilidades

de segurança que não se conseguiu, antes, prever ou resolver. Encontrar vulnerabilidades de segurança e fechar as lacunas de segurança de forma proativa é uma necessidade absoluta para as empresas. Mas, muitas organizações não têm as ferramentas e o conhecimento para identificar vulnerabilidades de segurança. Para ajudar sua empresa a melhorar sua segurança, seguem algumas dicas sobre como encontrar vulnerabilidades de segurança:

- **Como encontrar vulnerabilidades de segurança: audite seus ativos de rede** – para encontrar vulnerabilidades de segurança na rede da empresa, é necessário ter um inventário preciso dos ativos na rede, bem como dos SO e dos *softwares* que esses ativos executam. Ter essa lista de inventário ajuda a organização a identificar vulnerabilidades de segurança de *software* obsoleto e *bugs* de programa conhecidos em tipos de SO e *softwares* específicos. Sem esse inventário, uma organização pode presumir que sua segurança de rede está atualizada, mesmo que possa ter ativos com vulnerabilidades de anos. Além disso, se um novo protocolo de segurança for aplicado, a ativos, na rede, para fechar as lacunas de segurança, mas houver ativos desconhecidos na rede, isso poderá levar a uma proteção desigual para a organização. Por exemplo, digamos que os servidores A, B e C são atualizados para exigir autenticação multifator, mas o servidor D, que não estava na lista de inventário, não recebe a atualização. Quando se trata de encontrar vulnerabilidades de segurança, uma auditoria de rede completa é indispensável para o sucesso da proteção.
- **Como encontrar vulnerabilidades de segurança: teste de penetração** – depois de concluir a auditoria da rede e inventariar todos os ativos, a rede precisa passar por um teste de estresse para determinar como um invasor pode tentar quebrá-la. Esse teste de penetração é como os profissionais de segurança cibernética verificam as falhas de segurança para que essas possam ser sanadas antes que ocorra um ataque malicioso. A metodologia por trás de um teste de penetração pode variar um pouco, dependendo da arquitetura de segurança de rede da organização e do perfil de risco de segurança cibernética – não existe uma verdadeira abordagem “tamanho único” para testes de penetração.

No entanto, as etapas gerais de um teste de penetração geralmente envolvem:

a. executar teste em uma data/hora definida;
b. auditar os sistemas existentes para se verificar ativos com vulnerabilidades conhecidas;
c. executar ataques simulados, na rede, que tentem explorar potenciais pontos fracos ou descobrir novos;
d. executar um plano de respostas a incidentes para tentar conter ataques simulados durante o teste de penetração (além de identificar vulnerabilidades de segurança, esse último item da lista também pode ajudar a encontrar deficiências na resposta a incidentes da empresa, o que pode ser útil para modificar planos e medidas de resposta para se reduzir ainda mais a exposição a alguns riscos de segurança).

- **Como encontrar vulnerabilidades de segurança: criando uma estrutura de inteligência de ameaças** – o teste de penetração é muito útil para encontrar vulnerabilidades de segurança. No entanto, não é o único método que as empresas podem usar. Outra ferramenta para identificar possíveis problemas é a estrutura de inteligência de ameaças, que requer os seguintes passos:

a. defina o que precisa se proteger;
b. defina metas para a segurança geral da rede;
c. identifique as principais fontes de ameaças;
d. refine as proteções de segurança;
e. escolha *feeds* de inteligência de ameaças apropriados para monitorar ameaças cibernéticas novas e emergentes e estratégias de ataque.

Saber quais são as maiores ameaças à segurança é crucial para manter medidas de proteção de segurança atualizadas. É por isso que muitas empresas recorrem a um provedor de serviços de segurança gerenciados, que geralmente dispõem de ferramentas e experiência que facilitam a criação de uma estrutura de inteligência de ameaças. Muitos especialistas podem fornecer testes de penetração e serviços de gerenciamento de vulnerabilidades para identificar rapidamente os principais problemas de segurança e ajudar seus clientes a fechar essas lacunas de segurança antes que um invasor possa delas se aproveitar. Também podem ajudar a criar ou modificar planos de resposta a

incidentes para que as empresas possam minimizar os impactos se ocorrer uma violação de segurança.

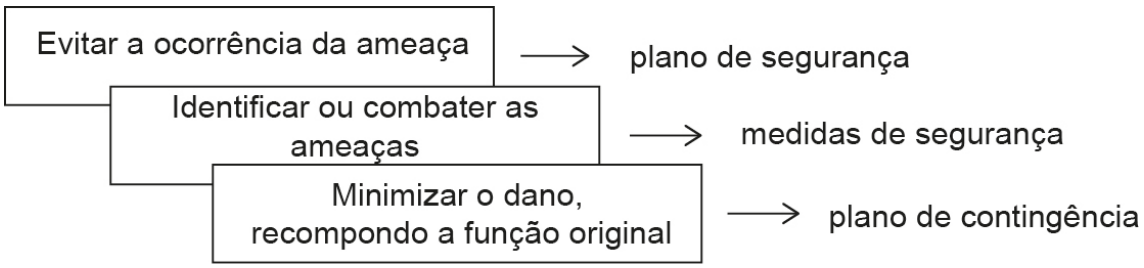
2.1 Ferramentas para segurança da informação

Além dos controles técnicos, as organizações também precisam implementar políticas de segurança como forma de controle administrativo. Na verdade, essas políticas devem ser realmente um ponto de partida para o desenvolvimento de um plano geral de segurança. Uma boa política de segurança da informação estabelece as diretrizes para o uso dos recursos de informação da empresa pelos funcionários e fornece à empresa um recurso no caso de um funcionário violar uma política.

De acordo com o Sans Institute, uma boa política é "[...] uma declaração ou plano formal, breve e de alto nível que abrange as crenças gerais, metas, objetivos e procedimentos aceitáveis de uma organização para uma área específica". As políticas exigem conformidade; o não cumprimento de uma política resultará em ação disciplinar. Uma política não apresenta os detalhes técnicos específicos, mas concentra-se nos resultados desejados. Uma política de segurança deve ser baseada nos princípios orientadores da tríade de segurança: confidencialidade, integridade e disponibilidade.

Caiçara Junior (2015, p. 162) defende que realizar avaliação das ameaças é o ponto de partida para que ocorra o desenvolvimento ou mudança do plano ou das políticas de segurança da empresa. O autor aponta que, quando a análise de riscos está na etapa final, é necessário gerar ou revisar o plano de segurança da organização, e que qualquer plano de segurança deve atender às preocupações básicas com as medidas necessárias para evitar, impedir ou minimizar as ocorrências, conforme ilustrado na Figura 2.

Figura 2 – Etapas para segurança



Fonte: Caiçara Junior, 2015, p. 163.

Para garantir a confidencialidade, a integridade e a disponibilidade das informações, as organizações podem escolher entre uma variedade de ferramentas, iniciando pela autenticação. A maneira mais comum de identificar alguém é por meio de sua aparência física. Mas, como identificamos alguém sentado atrás de uma tela de computador ou no caixa eletrônico? As ferramentas de autenticação são usadas para garantir que a pessoa que acessa a informação seja, de fato, quem ela se apresenta.

A autenticação pode ser realizada identificando alguém por meio de um ou mais de três fatores: algo que ele saiba, algo de que ele disponha ou algo que ele seja. Por exemplo, a forma mais comum de autenticação hoje é a *identity* (ID) do usuário e a senha. Nesse caso, a autenticação é feita confirmando algo que o usuário conhece, sua ID e sua senha. Mas essa forma de **autenticação** é fácil de ser comprometida e às vezes são necessárias formas mais fortes de autenticação. Identificar alguém apenas por algo que possui, como uma chave ou um cartão, também pode ser problemático. Quando esse *token* de identificação é perdido ou roubado, a identidade pode ser facilmente roubada. O fator final, algo que você é, é muito mais difícil de comprometer. Esse fator identifica um usuário por meio do uso de uma característica física, como um exame de olho ou impressão digital. Uma maneira mais segura de autenticar um usuário é fazer a autenticação multifator. Ao combinar dois ou mais dos fatores listados, torna-se muito mais difícil alguém burlar esse processo.

Depois que um usuário é autenticado, a próxima etapa é garantir que ele possa acessar apenas os recursos de informação apropriados. Isso é feito por meio do uso de **controle de acesso**. O controle de acesso determina quais usuários estão autorizados a ler, modificar, adicionar e/ou excluir informações. Existem vários modelos de controle de acesso diferentes. Ora abordaremos dois: a lista de controle de acesso e o controle de acesso baseado em função. Para cada recurso de informação que uma organização deseje gerenciar, pode ser criada uma lista de usuários que podem realizar ações específicas. Essa é uma lista de controle de acessos. Para cada usuário, recursos específicos são atribuídos, como *read*, *write*, *delete* ou *add*. Somente usuários com esses recursos têm permissão para executar essas funções. Se um usuário não estiver na lista, ele não poderá nem mesmo saber que o recurso de informação existe.

As listas de controle de acesso são simples de entender e manter. No entanto, elas têm várias desvantagens. A principal desvantagem é que cada

recurso de informação é gerenciado separadamente; portanto, se um administrador de segurança quisesse adicionar ou remover um usuário de um grande conjunto de recursos de informação, isso seria bastante difícil. E, à medida que o número de usuários e recursos aumenta, isso se torna mais difícil de gerir, o que levou à criação de um método aprimorado de controle de acesso, chamado *controle de acesso baseado em função*. Em vez de se conceder direitos de acesso a usuários específicos de um recurso de informação, os usuários são atribuídos a funções e, em seguida, essas funções recebem o acesso. Isso permite que os administradores gerenciem usuários e funções separadamente, simplificando a administração e, por extensão, melhorando a segurança.

Muitas vezes, uma organização precisa transmitir informações pela internet ou transferi-las em mídia externa. Nesses casos, mesmo com a devida autenticação e controle de acesso, é possível que uma pessoa não autorizada tenha acesso aos dados. A criptografia é um processo de codificação de dados durante sua transmissão ou armazenamento, para que apenas indivíduos autorizados possam lê-los. Essa codificação é realizada por um programa de computador, que codifica o texto simples que precisa ser transmitido; então, o destinatário recebe o texto cifrado e o decodifica, realizando uma descriptografia. Para que isso funcione, o remetente e o destinatário precisam concordar com o método de codificação para que ambas as partes possam se comunicar adequadamente. Ambas as partes compartilham a chave de criptografia, permitindo que se codifiquem e decodifiquem as mensagens uma da outra. Isso é chamado de *criptografia de chave simétrica*. Esse tipo de criptografia é problemático porque a chave está disponível em dois locais diferentes.

Uma alternativa à criptografia de chave simétrica é a criptografia de chave pública. Na criptografia de chave pública, duas chaves são usadas: uma chave pública e uma chave privada. Para enviar uma mensagem criptografada, você obtém a chave pública, codifica a mensagem e a envia. O destinatário, então, usa a chave privada para decodificá-la. A chave pública pode ser dada a qualquer pessoa que deseje enviar uma mensagem ao destinatário. Cada usuário simplesmente precisa de uma chave privada e uma chave pública para proteger as mensagens. A chave privada é necessária para descriptografar algo enviado com a chave pública.

2.2 Medidas de segurança: senha e *backup*

Por que usar apenas uma ID de usuário/senha simples não é considerado um método seguro de autenticação? Acontece que essa autenticação de fator único é extremamente fácil de se comprometer. Boas políticas de senha devem ser implementadas para garantir que as senhas não sejam violadas. A seguir estão algumas das políticas mais comuns que as organizações devem implementar, nesse sentido.

- **Exigência de senhas complexas**: uma razão pela qual as senhas são comprometidas é quando elas podem ser facilmente adivinhadas. Um estudo recente descobriu que as três principais senhas que as pessoas usaram em 2012 foram *senha*, *123456* e *12345678*. Uma senha não deve ser simples, ou uma palavra que possa ser encontrada em um dicionário. Ora, uma das primeiras coisas que um *hacker* fará é tentar decifrar uma senha testando todos os termos do dicionário! Em vez disso, uma boa política de senha é aquela que exige o uso de no mínimo oito caracteres e pelo menos uma letra maiúscula, um caractere especial e um número.
- **Alteração regular das senhas**: é essencial que os usuários alterem suas senhas regularmente. Os usuários devem alterar suas senhas a cada 60 a 90 dias, garantindo que quaisquer senhas que possam ter sido roubadas ou adivinhadas não poderão ser usadas contra a empresa.
- **Treinamento dos funcionários para não fornecerem senhas**: um dos principais métodos usados para roubar senhas é simplesmente descobri-las perguntando aos usuários ou administradores. O pretexto ocorre quando um invasor liga para um *helpdesk* ou administrador de segurança e finge ser um determinado usuário autorizado, então com problemas para fazer *login*. Isto é: outra maneira pela qual os funcionários podem ser induzidos a fornecer senhas é por meio de *phishing*, por *e-mail*. O *phishing* ocorre quando um usuário recebe um *e-mail* que parece ser de uma fonte confiável, como seu banco ou seu empregador. Nesse *e-mail*, do usuário é solicitado que ele clique em um *link* e faça *login* em um *site* que imita o *site* original e nele insira sua ID e senha. Outra ferramenta essencial para a segurança da informação é um plano de **backup** abrangente, para toda a organização. Não só deve ser feito *backup* dos dados nos servidores corporativos, mas também deve ser feito *backup* dos computadores

individuais usados em toda a organização. Um bom plano de *backup* deve consistir em vários componentes, em uma compreensão completa dos recursos de informação organizacional. Afinal, quais informações a organização realmente possui? Onde estão armazenadas? Alguns dados podem ser armazenados nos servidores da organização; outros dados, nos discos rígidos dos usuários; alguns, na nuvem; e alguns, em *sites* de terceiros. Uma organização deve fazer um inventário completo de todas as informações que precisam de *backup* e determinar a melhor maneira de executar isso.

- ***Backups* regulares de todos os dados**: a frequência dos *backups* deve ser baseada na importância dos dados para a empresa, combinada com a capacidade da empresa de substituir quaisquer dados perdidos. Os dados críticos devem ser copiados diariamente, enquanto os dados menos críticos podem ser copiados semanalmente.
- **Armazenamento externo de conjuntos de dados de *backup***: se todos os dados de *backup* estiverem sendo armazenados na mesma instalação que as cópias originais dos dados, um único evento, como um terremoto, incêndio ou tornado, eliminaria os dados originais e o *backup*! É essencial que parte do plano de *backup* seja armazenar os dados em um local externo.
- **Teste de restauração de dados**: regularmente, os *backups* devem ser testados, com a restauração de alguns dados. Isso garantirá que o processo esteja funcionando e dará à organização confiança no seu plano de *backup*.

Além dessas considerações, as organizações também devem examinar suas operações para determinar qual efeito um tempo de inatividade teria em seus negócios. Se a TI ficasse indisponível por um longo período, como isso afetaria os negócios?

TEMA 3 – GESTÃO E ARMAZENAMENTO DE DADOS

Os volumes de dados corporativos continuam a crescer exponencialmente. Então, como as organizações podem efetivamente armazenar tudo isso? É aí que entra o gerenciamento de armazenamento de dados. O gerenciamento eficaz é fundamental para garantir que as organizações

usem os recursos de armazenamento de forma eficaz e que armazenem dados com segurança, em conformidade com as políticas da empresa e os regulamentos governamentais. Os administradores e gerentes de TI devem entender quais procedimentos e ferramentas abrangem o gerenciamento de armazenamento de dados, para desenvolverem sua própria estratégia.

O gerenciamento de armazenamento garante que os dados estejam disponíveis para os usuários quando eles precisarem desses dados, e normalmente isso faz parte do trabalho do administrador de armazenamento. As organizações sem um administrador de armazenamento dedicado podem usar um profissional de TI para gerenciamento de armazenamento. A política de retenção de dados é um elemento-chave do gerenciamento de armazenamento e um bom ponto de partida para implementação de uma proteção dos dados. Essa política define os dados que uma organização retém para necessidades operacionais ou de conformidade. Ela descreve por que a organização deve manter os dados, o período de retenção e o processo de descarte e a ajuda a determinar como ela pode pesquisar e acessar dados. A política de retenção é especialmente importante, agora, pois os volumes de dados aumentam continuamente e isso pode ajudar a reduzir o espaço de armazenamento e os seus respectivos custos. A tarefa de gerenciamento de armazenamento de dados também inclui provisionamento e configuração de recursos, dados estruturados e não estruturados e avaliação de como as necessidades podem mudar, ao longo do tempo.

Uma ferramenta de gerenciamento de armazenamento de dados que atenda às necessidades organizacionais pode aliviar a carga administrativa que surge diante da necessidade de se gerir grandes quantidades de dados. Os recursos a serem procurados em uma ferramenta de gerenciamento incluem planejamento de capacidade de armazenamento, monitoramento de desempenho, compactação e desduplicação. O gerenciamento de armazenamento de dados também facilita que se centralize a administração dos dados para que se possa supervisionar uma variedade de sistemas de armazenamento. Esses benefícios também levam a custos reduzidos, pois os administradores podem utilizar melhor os recursos de armazenamento. Uma estratégia de gerenciamento eficaz fornece aos usuários a quantidade certa de capacidade de armazenamento. As organizações podem aumentar e diminuir o

espaço de armazenamento de dados, conforme necessário. A estratégia de armazenamento acomoda necessidades e aplicativos em constante mudança.

Os desafios do gerenciamento de armazenamento de dados incluem ameaças cibernéticas persistentes, o entendimento de regulamentos de gerenciamento de dados e a exigência de uma força de trabalho bem distribuída. Esses desafios ilustram por que é tão importante implementar um plano abrangente: uma estratégia de gerenciamento de armazenamento deve garantir que as organizações protejam seus dados contra violações de dados, *ransomware* e outros ataques de *malware*, e os trabalhadores remotos devem saber que terão acesso a arquivos e aplicativos exatamente como teriam em um ambiente de escritório tradicional.

Sistemas distribuídos e complexos apresentam um obstáculo para o gerenciamento de armazenamento de dados. Não apenas os trabalhadores estão espalhados, mas os sistemas são executados tanto no local quanto na nuvem. Um ambiente de armazenamento local pode incluir *hard disk drives* (HDDs), *solid-state drives* (SSDs) e fitas. As organizações geralmente usam várias nuvens. Novas tecnologias, como a inteligência artificial (IA), podem beneficiar as organizações, mas também aumentar a complexidade da gestão de armazenamento. A quantidade de dados não estruturados – que incluem documentos, *e-mails*, fotos, vídeos e metadados – em circulação aumentou, e isso também complica o gerenciamento de armazenamento. Os desafios de dados não estruturados abrangem volume, novos tipos e como ganhar valor. Embora algumas organizações possam não querer perder tempo gerenciando dados não estruturados, no final, com eles, se economizam dinheiro e espaço de armazenamento.

Os processos e práticas de gerenciamento de armazenamento variam, dependendo da tecnologia, plataforma e tipo. Estes são alguns métodos e serviços gerais para gerenciamento de armazenamento de dados:

- *software* de gerenciamento de recursos de armazenamento;
- consolidação de sistemas;
- *arrays* de armazenamento multiprotocolo;
- camadas de armazenamento;
- implantação estratégica de SSD;
- nuvem híbrida;
- sistemas de escala;

- armazenamento de arquivo de dados acessados com pouca frequência;
- eliminação de máquinas virtuais inativas;
- desduplicação;
- recuperação de desastres como um serviço;
- armazenamento de objetos.

As organizações podem considerar a incorporação de interfaces de gerenciamento de armazenamento baseadas em padrões, como parte de sua estratégia de gerenciamento. As organizações também devem escolher entre armazenamento de objetos, blocos e arquivos. O armazenamento em bloco é o tipo padrão para HDDs e SSDs e oferece desempenho robusto. O armazenamento de arquivos coloca os arquivos em pastas e oferece simplicidade. O armazenamento de objetos organiza de forma eficiente os dados não estruturados, a um custo comparativamente baixo.

TEMA 4 – REDES DE COMPUTADORES

Nos primórdios da computação, os computadores eram vistos como dispositivos para fazer cálculos, armazenar dados e automatizar processos de negócios. No entanto, à medida que os dispositivos evoluíram, tornou-se evidente que muitas das funções das telecomunicações poderiam ser integradas ao computador. Durante a década de 1980, muitas organizações começaram a combinar seus departamentos de telecomunicações e sistemas de informação, antes separados, em um departamento de TI. Essa capacidade de os computadores se comunicarem uns com os outros e, talvez mais importante, facilitarem a comunicação entre indivíduos e grupos tem sido um fator importante no crescimento da computação, nas últimas décadas.

As redes de computadores realmente começaram na década de 1960, com o nascimento da internet. No entanto, enquanto a internet e a *web* evoluíam, as redes corporativas também tomavam forma em redes locais e computação cliente-servidor. Na década de 1990, quando a internet atingiu a maioridade, as tecnologias da internet começaram a permear todas as áreas das organizações. Agora, sendo a internet um fenômeno global, seria impensável ter um computador que não incluísse recursos de comunicação.

A comunicação em rede está repleta de alguns conceitos muito técnicos, mas baseados em certos princípios simples. Aprenda o que significam os termos a seguir e você poderá se manter atualizado em uma conversa sobre a internet.

- Pacote: unidade fundamental de dados transmitidos pela internet. Quando um dispositivo pretende enviar uma mensagem para outro dispositivo (por exemplo, seu computador pessoal – PC enviando uma solicitação, ao YouTube, para abrir um vídeo), ele divide a mensagem em partes menores, chamadas de *pacotes*. Cada pacote tem o endereço do remetente, o endereço de destino, um número de sequência e uma parte da mensagem geral a ser enviada.
- *Hub*: dispositivo de rede simples, que conecta outros dispositivos à rede e envia pacotes para todos os dispositivos conectados a ele.
- *Bridge*: dispositivo de rede que conecta duas redes e permite apenas os pacotes necessários.
- *Switch*: dispositivo de rede que conecta vários dispositivos e filtra pacotes com base em seu destino, nos dispositivos conectados.
- Roteador: dispositivo que recebe e analisa pacotes e os encaminha para seu destino. Em alguns casos, um roteador enviará um pacote para outro roteador; em outros casos, o enviará diretamente ao seu destino.
- Endereço de *internet protocol* (IP): cada dispositivo que se comunica na internet, seja um computador pessoal, seja um *tablet*, um *smartphone* ou qualquer outra coisa, recebe um número de identificação exclusivo chamado *endereço IP*. Historicamente, o padrão de endereço IP usado tem sido o IPv4 (versão 4), que tem o formato de quatro números, entre 0 e 255, separados por um ponto. O padrão IPv4 tem um limite de 4.294.967.296 endereços possíveis. À medida que o uso da internet proliferou, o número de endereços IP necessários cresceu a ponto de se esgotar o número de endereços IPv4. Isso levou ao novo padrão IPv6, que está sendo implementado. O padrão IPv6 é formatado como oito grupos de quatro dígitos hexadecimais, com 2001:0db8:85a3:0042:1000:8a2e:0370:7334.38 endereços possíveis.
- Nome de domínio: se você tivesse que tentar lembrar o endereço IP de cada servidor *web* que deseja acessar, a internet não seria tão fácil de usar. Um nome de domínio é um nome amigável para um dispositivo na

internet. Esses nomes geralmente consistem em um texto descritivo, seguido pelo domínio de primeiro nível.

- Sistema de nomes de domínio (DNS): o diretório, na internet. Quando uma solicitação para acessar um dispositivo com um nome de domínio é fornecida, um servidor DNS é consultado. Ele responde com o endereço IP do dispositivo solicitado, permitindo o roteamento adequado.
- Comutação de pacotes: quando um pacote é enviado de um dispositivo pela internet, ele não segue um caminho direto para seu destino. Em vez disso, ele é passado de um roteador para outro, pela internet, até chegar ao seu destino. De fato, às vezes dois pacotes da mesma mensagem tomarão rotas diferentes! Às vezes, os pacotes chegam ao destino fora de ordem. Quando isso acontece, o dispositivo receptor os restaura na ordem correta.
- Protocolo: em redes de computadores, um protocolo é o conjunto de regras que permite que dois (ou mais) dispositivos troquem informações pela rede.

4.1 Redes organizacionais: LAN e WAN

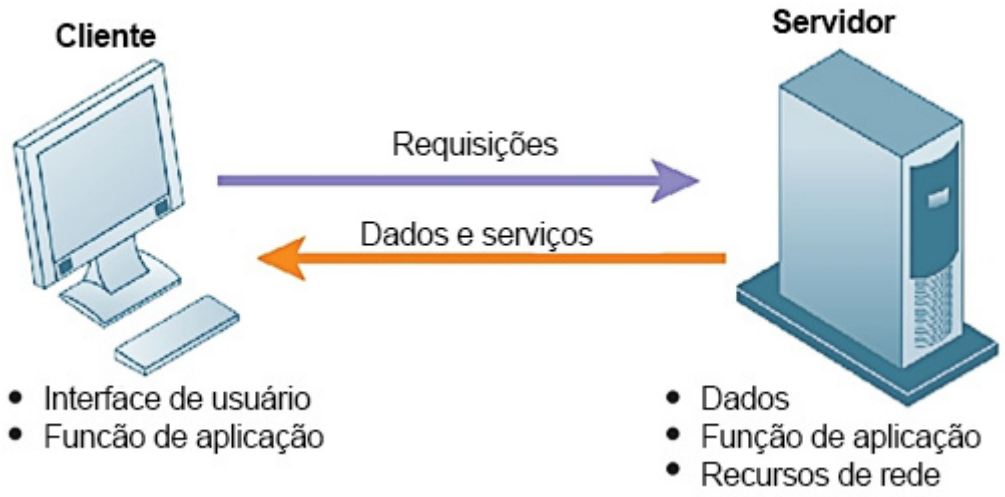
Enquanto a internet estava evoluindo e criando uma maneira de as organizações se conectarem umas com as outras e com o mundo, outra revolução estava ocorrendo, nas organizações. A proliferação de computadores pessoais dentro das organizações levou à necessidade de compartilhar recursos como impressoras, *scanners* e dados. As organizações resolveram esse problema por meio da criação de redes locais (LANs), que permitiram que os computadores se conectassem uns aos outros e a periféricos. Essas mesmas redes também permitiram que computadores pessoais se conectassem a computadores *mainframe* legados.

Uma LAN é (por definição) uma rede local, geralmente operando no mesmo prédio ou no mesmo *campus*. Quando uma organização precisava fornecer uma rede em uma área mais ampla (com locais em diferentes cidades ou estados, por exemplo), ela construía uma rede de longa distância (WAN).

4.1.1 Cliente-servidor

O PC foi originalmente usado como um dispositivo de computação autônomo. Um programa foi instalado no computador e, em seguida, usado para processamento de textos ou processamento de números. No entanto, com o advento das redes e das redes locais, os computadores podem trabalhar juntos para resolver problemas. Computadores de última geração foram instalados como servidores, e os usuários da rede local podiam executar aplicativos e compartilhar informações entre departamentos e organizações. Isso é chamado de *computação cliente-servidor*.

Figura 3 – Computação cliente-servidor



Fonte: Laudon; Laudon, 2014, p. 149.

4.1.2 Intranet

Assim como as organizações criam *sites* para fornecer acesso global a informações sobre seus negócios, elas também criam páginas internas para fornecer informações sobre elas próprias, aos seus funcionários. Esse conjunto interno de páginas da *web* é chamado de *intranet*. As páginas da *web* na intranet não são acessíveis a pessoas de fora da empresa; na verdade, essas páginas apareceriam como *não encontradas* se um funcionário tentasse acessá-las de fora da rede da empresa.

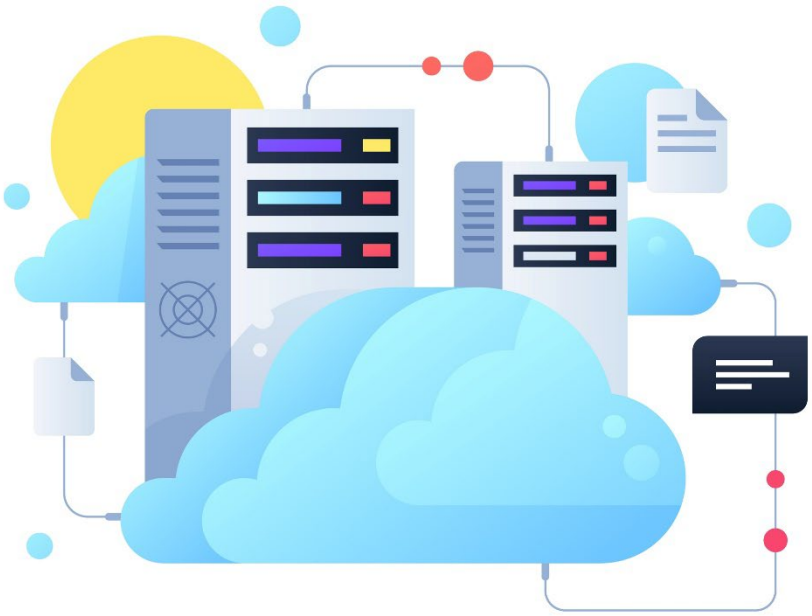
4.1.3 Extranet

Às vezes, uma organização deseja colaborar com seus clientes ou fornecedores e, ao mesmo tempo, manter a segurança de sua própria rede. Em casos como esse, uma empresa pode criar uma extranet, que é uma parte da rede da empresa que pode ser disponibilizada com segurança para quem está fora da empresa. As extranets podem ser usadas para permitir que os clientes façam *login* e verifiquem o *status* de seus pedidos ou para que os fornecedores verifiquem os níveis de estoque de seus clientes.

Às vezes, uma organização precisará permitir que alguém que não esteja fisicamente localizado em sua rede interna obtenha acesso. Esse acesso pode ser fornecido por uma rede privada virtual (VPN). Uma VPN permite que um usuário que está fora de uma rede corporativa faça um desvio ao redor do *firewall* e acesse a rede interna de fora. Por meio de uma combinação de *software* e medidas de segurança, isso permite que uma organização dê acesso limitado às suas redes e, ao mesmo tempo, garanta a segurança geral.

TEMA 5 – RECURSOS NA NUVEM

A disponibilidade universal da internet, combinada com o aumento do poder de processamento e da capacidade de armazenamento de dados, tornaram a computação em nuvem uma opção viável para muitas empresas. Usando a computação em nuvem, empresas ou indivíduos podem contratar um armazenamento de dados em dispositivos da internet. Os aplicativos podem ser “alugados” conforme necessário, dando à empresa a capacidade de implantar, rapidamente, novos aplicativos. Historicamente, para o *software* rodar em um computador, uma cópia individual desse *software* tinha que ser instalada no computador, seja em um disco, seja, mais recentemente, após ele ser baixado da internet. O conceito de computação em **nuvem** muda isso, no entanto.



Crédito: Jossnat/Shutterstock.

Para entender a computação em nuvem, primeiro temos que entender o que é a nuvem. **A nuvem** refere-se a aplicativos, serviços e possibilidades de armazenamento de dados na internet. Esses provedores de serviços contam com *farms* de servidores gigantes e dispositivos de armazenamento massivos, conectados por meio de protocolos da internet. A computação em nuvem é o uso desses serviços por indivíduos e organizações.

Você provavelmente já usa computação em nuvem de algumas formas. Por exemplo, se você acessar seu *e-mail* pelo navegador da *web*, usará uma forma de computação em nuvem. Se você usar os aplicativos do Google Drive, estará usando a computação em nuvem. Embora sejam versões gratuitas da computação em nuvem, há um grande negócio no fornecimento de aplicativos e armazenamento de dados pela *web*. A computação em nuvem não se limita, também, a aplicativos da *web*: também pode ser usada para serviços como telefone ou *streaming* de vídeos.

Quadro 3 – Computação em nuvem

Computação em nuvem	
Vantagens	Desvantagens
Nenhum *software* para instalar ou atualizações para manter	Suas informações são armazenadas no computador de outra pessoa – qual é a segurança disso?
Disponível de qualquer computador que tenha acesso à internet	Você deve ter acesso à internet para usá-la
Pode escalar facilmente para muitos usuários	Você está confiando em um terceiro para fornecer esses serviços
Novos aplicativos podem ser instalados e executados muito rapidamente	Falta de controle
Os serviços podem ser alugados por tempo limitado, conforme a necessidade	Gerenciamento de várias nuvens
Informações não serão perdidas se o disco rígido travar ou se o *laptop* for roubado	
Não há limitação de memória disponível ou espaço em disco, no computador	

Fonte: Moura, 2022.

A computação em nuvem tem a capacidade de realmente impactar a forma como as organizações gerenciam a tecnologia. Por exemplo, por que um departamento de TI precisa comprar, configurar e gerenciar computadores pessoais e *softwares* quando tudo o que é realmente necessário é uma conexão com a internet?

Muitas organizações temem abrir mão do controle de seus dados e de alguns de seus aplicativos usando a computação em nuvem. Mas eles também veem o valor em reduzir a necessidade de instalação de *softwares* e adicionar armazenamento em disco aos computadores locais. Uma solução equilibrada para isso está no conceito de **nuvem privada**. Embora existam vários modelos de nuvem privada, a ideia básica é que o provedor de serviços de nuvem seccione o espaço do servidor *web* para uma organização específica. A organização tem controle total sobre esse espaço de servidor, enquanto ainda obtém alguns dos benefícios da computação em nuvem.

Uma tecnologia que é amplamente utilizada como parte da computação em nuvem é a da **virtualização**. A virtualização é o processo de usar *softwares* para simular um computador ou algum outro dispositivo. Por exemplo, usando a virtualização, um único computador pode executar as funções de vários computadores. As organizações também estão implementando a virtualização para reduzir o número de servidores necessários para fornecer os serviços necessários.

FINALIZANDO

Nesta etapa, foram aprofundados os conceitos sobre a infraestrutura e a segurança dos sistemas de informação. Destacamos que mesmo com as principais ferramentas de segurança, os sistemas de informação somente serão confiáveis e seguros se souberem como e onde utilizar adequadamente tais ferramentas. Para isso, é imprescindível conhecer onde a empresa corre risco e os controles necessários para proteger seus sistemas de informação, assim como se desenvolver políticas de segurança e planos para manter o negócio em funcionamento se ocorrer de os sistemas de informação pararem de operar. As empresas devem, assim, contar com ferramentas e tecnologias para proteger seus recursos de informação.

REFERÊNCIAS

CAIÇARA JUNIOR, C. **Sistemas integrados de gestão**: ERP – uma abordagem gerencial. 2. ed. Curitiba: InterSaberes, 2015.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais**. 11. ed. São Paulo: Pearson Prentice Hall, 2014.