FUNDAMENTOS DE SISTEMAS DE INFORMAÇÃO

AULA 3

Profª Vívian Ariane Barausse de Moura

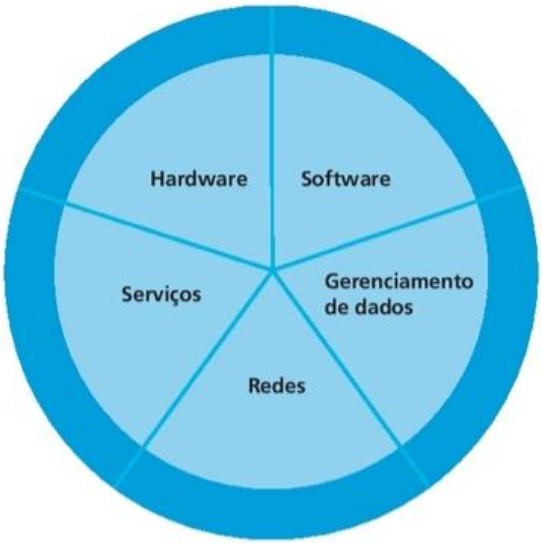
CONVERSA INICIAL

O objetivo desta aula é tratar dos principais conceitos e temas relacionados aos componentes da infraestrutra e da segurança de Tecnologia de Informação (TI). Para tanto, é preciso conhecer as principais tecnologias de *hardware* computacional, de armazenamento de dados e de entrada e saída de dados utilizadas em empresas. Veremos também questões que envolvem as medidas de segurança dos sistemas de informação, 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

TEMA 1 – INFRAESTRUTURA E SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Retomando alguns conceitos: na Figura 1, vemos 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.

Laudon e Laudon (2014) abordam uma questão muito importante para refletir a relação da infraestrutura de TI em uma empresa: por que as empresas do mundo inteiro gastam cerca de 3,7 trilhões de dólares por ano em sistemas de informação e computação? Ao levantar as possíveis respostas para esse

questionamento, são elencadas questões relacionadas ao que é necessário para abrir e administrar uma empresa na atualidade. Há uma variedade de componentes de *hardware* e *software* e de recursos computacionais que podem ser utilizados para resolver problemas organizacionais básicos.

Ao analisar o cotidiano de uma empresa, percebemos que o seu funcionamento depende de computadores e também de outras opções de *hardware*, como *notebooks*, *smartphones* e *tablets*. Também são necessários *softwares* que irão rodar nesses *hardwares* – os aplicativos que servem para facilitar o cotidiano das funções, com a criação de planilhas, documentos e arquivos de dados. Requer-se também uma rede para conectar o trabalho realizado pelos funcionários da empresa, incluindo também seus clientes e fornecedores (Laudon; Laudon, 2014).

Além disso, se a empresa for de médio ou grande porte, também irá precisar de servidores: “um *data center*, como uma instalação que reúne sistemas computacionais e componentes associados, como sistemas de telecomunicações, armazenamento, segurança e fornecimento de energia de backup” (Laudon; Laudon, 2014, p. 146).

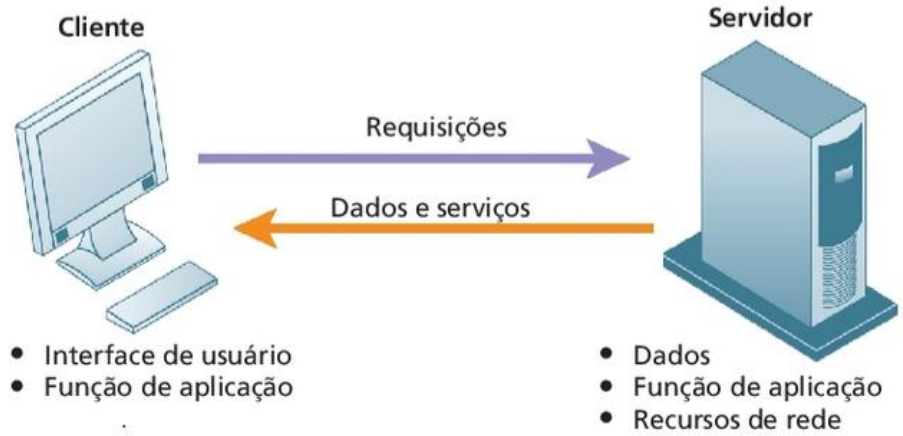
As empresas enfrentam muitos desafios e problemas que podem ser resolvidos por computadores e sistemas de informação. Para que este processo seja eficiente, precisam encontrar o *hardware* mais adequado. Nesse sentido, existem computadores de vários tamanhos, com diferentes recursos para o processamento de informação, desde os menores dispositivos de mão até *mainframes* e supercomputadores. Laudon e Laudon (2014, p. 148, grifo nosso) apresentam as categorias de computador:

> - **Computador pessoal** (pc): para o trabalho individual ou com algumas pessoas em uma pequena empresa, ocorre a utilização de um pc de mesa ou laptop; o indivíduo pode também utilizar um dispositivo móvel com considerável capacidade computacional, como um iPhone, iPad, Blackberry ou um dispositivo Android.
> - **Estação de trabalho** (*workstation*): para os trabalhos que exigem recursos gráficos ou computacionais poderosos, como engenharia ou projetos avançados, também se encaixa na categoria computador de mesa, mas possui capacidade de processamento matemático e gráfico superior à de um PC.
> - **Servidor**: computadores do tipo servidor são utilizados especificamente para suportar uma rede de computadores, permitindo aos usuários compartilhar arquivos, *software* e dispositivos periféricos, como uma impressora, ou outros recursos de rede. Às vezes é preciso um grande número de servidores conectados para suprir todas as necessidades de processamento de uma grande empresa.

- ***Mainframe***: é um computador de alto desempenho e grande capacidade, capaz de processar enorme quantidade de dados com extrema velocidade.
- **Supercomputador**: é um computador mais sofisticado de projeto especial, usado para executar tarefas que requerem cálculos complexos; é extremamente rápido, com milhares de variáveis, milhões de medidas e milhares de equações. Utilizado em análise de estruturas de engenharia, simulações, experimentos científicos, assim como em trabalhos militares, como pesquisas de armas de uso restrito e previsão do tempo.
- **Computação em grade** (*grid computing*): conecta em uma única rede computadores geograficamente distantes, criando assim um supercomputador virtual, que conta com a capacidade combinada de todos os computadores da rede.
- **Rede de computadores e computação cliente/servidor**: Para operacionalizar as funções de processamento são utilizados computadores em rede para a maioria das tarefas de processamento. Esta utilização de computadores conectados por uma rede de comunicação é chamada processamento distribuído. Um formato utilizado de processamento distribuído é a computação cliente/servidor, esse tipo de computação dividir o processamento entre clientes e servidores. Ambos fazem parte da rede, mas cada máquina desempenha a função específica que estiver mais apta a executar.

A Figura 2 apresenta o tipo mais simples de cliente/servidor sendo o processamento dividido entre as duas máquinas.

Figura 2 – Computação cliente-servidor



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

No exemplo da Figura 2 o processamento é dividido entre máquinas clientes e máquinas servidoras, conectadas por uma rede. O usuário interage com a interface das máquinas clientes:

> O cliente é o ponto de entrada do usuário para função requisitada; normalmente é um computador de mesa, um *laptop*, um *smartphone* ou *tablet*. O servidor provê serviços ao cliente, pois armazena e processa dados compartilhados e também executa funções, tais como gerenciar impressoras, armazenamento de *backup* e atividades de rede, como

> segurança, acesso remoto e autenticação de usuário. (Laudon; Laudon, 2014, p. 149)

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

1.1 Conceitos fundamentais de infraestrutura e segurança da informação

Caiçara (2015) aponta que existe uma crença de que os valores utilizados na segurança são *gastos*, enquanto o autor destaca que na verdade são *investimentos* que preservam a organização – considerando que há investimentos em sistemas relacionados à produtividade, qualidade do produto e eficiência, que podem ser comprometidos por uma sabotagem e até mesmo da falta de treinamento do pessoal.

Uma pesquisa na área de segurança da informação, realizada na Europa e nos Estados Unidos (Caiçara, 2015), indica que a atividade operacional de uma empresa cai em média 80% após 10 dias da ocorrência de um desastre na rede. Isso implica diretamente na sobrevivência da empresa, e em como fica a continuidade operacional se consideramos uma parada nos recursos de informática.

De acordo com Caiçara (2015, p. 158):

> 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 este cenário, o autor destaca a importância de medidas protetivas, trazendo uma relação com algumas questões às quais as empresas devem se atentar quando decidem sobre a implantação de medidas de segurança. Segundo Caiçara (2015, p. 158), é preciso realizar alguns questionamentos:

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?

Caiçara (2015) ressalta que, quando são definidas as medidas de segurança, o objetivo é minimizar os riscos e a vulnerabilidade nas organizações. Com isso, o autor ressalta que a segurança da informação deve primar por assegurar o que o autor define como *elementos da segurança da informação*, que são compostos por integridade, confidencialidade, autenticidade e disponibilidade das informações (Caiçara, 2015, p. 159, grifos do original):

> - **Integridade**: consiste da fidedignidade das informações, na conformidade dos dados armazenados com relação às inserções, alternações, processamentos autorizados efetuados e dos dados transmitidos. Parte-se da premissa de que manter a integridade das informações é garantia de não violação (acidental ou intencional) dos dados.
> - **Confidencialidade**: consiste em assegurar que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por algum meio. Com a manutenção da confidencialidade, busca-se assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou intencional sem que tenham autorização para este procedimento.
> - **Autenticidade:** consiste na garantia da veracidade da fonte de informações. Com a autenticidade, é possível identificar a pessoa ou entidade da qual se presta as informações.
> - **Disponibilidade**: consiste em assegurar que as informações estejam acessíveis às pessoas e aos processos autorizados em qualquer instante em que sejam solicitadas. A manutenção da disponibilidade de informações visa garantir a continuidade das transações e dos fluxos de informação sem interrupção.

A informação, nos dias atuais, passou a ser considerada como um recurso patrimonial – em alguns casos, o principal recurso. Assim, as medidas da segurança da informação serão tomadas de acordo com sua importância para empresa, pois a perda ou dano dessas informações podem implicar em prejuízos materiais e financeiros, os quais podem comprometer a imagem da organização, gerando impactos no mercado, que por sua vez podem resultar em quedas nas vendas e até mesmo em falência (Caiçara, 2015).

Nesse sentido, a segurança dos sistemas de informação é uma preocupação não apenas técnica, mas principalmente administrativa, levando em consideração tudo o que está envolvido nesses recursos. Afinal, além das instalações físicas e dos equipamentos, devem ser considerados os usuários,

compostos por executivos, acionistas, clientes, entre outros. Assim, Caiçara (2015, p. 160, grifos do original) afirma

> que as funções básicas de segurança dos sistemas de informação devem estar alinhadas com os seguintes passos: **dissuasão**: para que ocorra o desencorajamento à 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.

TEMA 2 – PRINCIPAIS VULNERABILIDADES DOS SISTEMAS DE INFORMAÇÃO

Ampliando os conceitos sobre a segurança da informação, Caiçara (2015) defende que os riscos ocorrem em qualquer ambiente organizacional. Eles podem ser oriundos de diversas naturezas, sendo decorrentes de vulnerabilidades comportamentais e operacionais. Por *vulnerabilidade* considera-se as fraquezas ou falhas que, ao serem conhecidas, podem resultar no vazamento ou perda de informação. Essas vulnerabilidades podem ser encontradas no âmbito pessoal ou de infraestrutura, ou seja, podem ocorrer na maneira de as pessoas se comportarem ou nos equipamentos, como *hardware* e *software*.

Caiçara (2015, p. 160) salienta que “todo negócio oferece riscos e está sempre suscetível ameaças, entretanto nem sempre uma empresa tem o pleno conhecimento desses riscos, uma situação é correr um risco e saber sua dimensão, outra é correr o risco sem conhecê-lo”. O conceito de *risco* é definido por Caruso e Steffen (2000, citados por Caiçara, 2015, p. 160):

> risco é tudo aquilo que pode afetar os negócios e impedir que os objetivos empresariais sejam alcançados, um risco existe quando uma ameaça com potencial que pode causar algum dano apresenta um alto índice de probabilidade de ocorrência no contexto dos sistemas de informação e um baixo nível de proteção.

Sendo assim, a verificação dos riscos deve ocorrer a partir de processos que indiquem as principais vulnerabilidades e ameaças. A partir disso é possível implementar controles e medidas de proteção capazes de reduzir a probabilidade de ocorrência dos riscos. Caiçara (2015) destaca que é necessário um gerenciamento contínuo dos riscos dentro de uma organização, pois este processo de análise não acaba com a implantação de medidas de segurança. Ele exige um contínuo monitoramento das ameaças que possam afetar o negócio da empresa, além de revisões periódicas dessa verificação.

Os processos de análise dos riscos existentes em sistemas de informação geram um mapeamento de ameaças principais. Caiçara (2015) apresenta um quadro com as principais ameaças (Figura 3), as quais, segundo o autor, “devem ser incluídas no mapeamento de riscos e na definição de política de segurança das informações” (Caiçara, 2015, p. 161).

Quadro 1 – Principais ameaças

Eventos	**Ameaças**
Integridade	• Ameaças físicas e ambientais (fogo, inundação, descargas atmosféricas, calor, poeira, falhas em equipamentos etc.). • Erros humanos. • Fraudes. • Erro de processamento e violação de sistemas. • Sabotagens físicas.
Disponibilidade	• Falhas em sistemas ou nos diversos ambientes computacionais. • Sabotagens lógicas.
Divulgação da informação	• Divulgação intencional de informações. • Divulgação não intencional de informações.
Alterações não autorizadas	• Alteração intencional. • Alteração não intencional.

Fonte: Caiçara, 2015, p. 161.

De acordo com Caiçara (2015, p. 162), quando ocorre a avaliação dos riscos em uma organização, uma das primeiras ações de quem realiza essa tarefa é fazer a análise de risco. O autor sugere uma sequência de etapas que podem ser desenvolvidas:

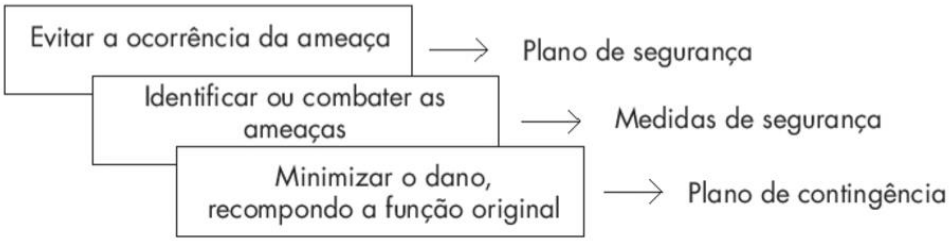
1. Identificação das principais informações estratégicas, dos bens patrimoniais, das pessoas que compõem a força de trabalho e das atividades e processos a serem protegidos;
2. Identificação de todos os tipos de riscos que envolvem as informações, as pessoas, os bens patrimoniais, as atividades e os processos a serem protegidos;
3. Estimativa da probabilidade de ocorrência de cada tipo de ameaça (riscos) no período de 1 a 2 anos, podendo ser considerado um tempo maior em função dos riscos inerentes ao ramo de atividade da organização;

4. Estimativa das consequências da ocorrência de cada tipo de ameaça, tanto dos danos e prejuízos tangíveis como dos intangíveis;
5. Cálculo estimativo da perda financeira anual para cada tipo de ameaça;
6. Cálculo da estimativa da perda financeira anual total para todas as ameaças;
7. Pesquisa e seleção de medidas e/ou alternativas de solução de segurança necessárias;
8. Cálculo de estimativa do custo de implementação e manutenção das medidas e/ou alternativas de solução de segurança necessárias;
9. Análise custo *versus* benefício (economia anual que poderá ser obtida com a implementação de medidas e/ou alternativas de solução de segurança).

Caiçara (2015, p. 162) defende que realizar a avaliação das ameaças é o ponto de partida para que ocorra o desenvolvimento ou a mudança no plano ou nas políticas de segurança da empresa. Quando uma organização não tem nenhum plano ou política de segurança, realizar a avaliação das ameaças se apresenta como uma oportunidade de obter uma visão estratégica das ameaças e riscos eminentes. Se já existir um plano de avaliação de ameaças, é pertinente que seja realizada uma nova inspeção no que já existe, para que sejam incluídas as novas ameaças e riscos que surgiram recentemente.

O autor aponta que a etapa final da análise de riscos é caracterizada pela necessidade de se gerar ou revisar o plano de segurança da organização, e que qualquer plano de segurança deve atender a preocupações básicas, com medidas necessárias para evitar, impedir ou minimizar as ocorrências, conforme ilustrado na Figura 3:

Figura 3 – Preocupações básicas



Fonte: Caiçara, 2016, p. 163.

TEMA 3 – SEGURANÇA DOS DADOS E DOS SISTEMAS

De acordo com Caiçara (2015), a segurança dos dados e dos sistemas envolve segurança física, ambiental e segurança lógica. Ao realizar o mapeamento dos riscos e a elaboração das políticas de segurança da informação, a empresa deve-se atentar ao local em que estão armazenadas essas informações, considerando a questão de segurança física e ambiental.

Além de se preocupar com a segurança dos computadores, é necessário realizar medidas para que as instalações e os equipamentos estejam seguros de ameaças – que podem ser fenômenos da natureza ou ações humanas, intencionais ou não. Nesse sentido, a segurança física e ambiental deve primar por definições de medidas que proporcionem "prevenção, detecção e reação", resultando no que Caiçara (2015, p. 67) define como "barreiras de segurança, em que os cuidados com a segurança física e ambiental sejam abordados com o mesmo cuidado que é realizada a segurança lógica".

Para realizar as definições quanto a medidas de proteção, é necessário considerar aspectos da segurança física e ambiental, que Caiçara (2015, p. 168) aponta como:

> localização, construção, controle de acesso, instalações elétricas e de telecomunicações, prevenção e combate a incêndio, condições ambientais, recursos humanos e padrões de trabalho. As principais ameaças quanto à segurança física e ambiental são decorrentes de incêndio, falhas em instalações elétricas e de equipamentos, poeira, umidade, acesso indevido às instalações, roubo, furto, falta de energia ou água, sabotagem, vandalismo, greves, descargas atmosféricas, inundações, ventos, vibração, efeitos químicos, radiação eletromagnética, explosões, entre outras.

Caiçara (2015) ressalta que o grau de rigidez na definição e avaliação dos riscos vai depender do porte e do ramo de atividade da empresa, bem como da criticidade das informações e do tipo de ambiente computacional. O autor especifica os aspectos de segurança física e ambiental (Quadro 2).

Quadro 2 – Segurança física e ambiental (localização)

Aspectos	Pontos que podem ser observados
Localização	• Evitar proximidade de instalações sujeitas a explosão, agentes químicos e radiações eletromagnéticas; • Evitar recursos computacionais críticos instalados em subsolos, próximos a grandes aglomerações ou manifestações públicas, últimos andares e estacionamentos; • Buscar proximidade de locais com fornecimento de energia elétrica estável; • Dar preferência a instalações de propriedade da própria empresa.

Fonte: Caiçara, 2016, p. 169.

Quadro 3 – Segurança física e ambiental (construção)

Aspectos	Pontos que podem ser observados
Construção	• Em ambientes de computadores de grande porte, também considerar como necessárias a construção em alvenaria e concreto, a ausência de janelas e a utilização de materiais resistentes a fogo; • Evitar piso com revestimento de materiais que proporcionem eletricidade estática, tais como carpete e/ou PVC; • Prever dutos para a distribuição de cabos elétricos e de comunicação de dados; • Prever reserva técnica de espaço para futuras ampliações que se fizerem necessárias; • Evitar construir instalações em níveis onde possa haver alagamentos ou inundações; • Utilizar salas-cofre, quando for o caso, para armazenamento de informações críticas, com vistas a manter a continuidade das operações em caso de desastre.

Fonte: Caiçara, 2016, p. 169.

Quadro 4 – Segurança física e ambiental (prevenção e combate a incêndio)

Aspectos	Pontos que podem ser observados
Prevenção e combate a incêndio	• Utilizar sistemática de detecção e combate a incêndio (uso contínuo, intermitente e eventual); • Sinalizar os equipamentos e locais de proteção e combate a incêndio; • Utilizar materiais resistentes ao fogo, quando for o caso; • Realizar treinamento da força de trabalho na utilização dos equipamentos de proteção e combate a incêndio; • Criar brigada de incêndio, quando for o caso; • Estabelecer procedimentos de emergência; • Definir critérios para manutenção dos dispositivos de proteção e combate a incêndio.

Fonte: Caiçara, 2016, p. 170.

Quadro 5 – Segurança física e ambiental (controle de acesso)

Aspectos	Pontos que podem ser observados
Controle de acesso	• Controlar o acesso de pessoas não autorizadas às áreas de alta criticidade, tanto em horário de expediente quanto fora do horário; • Monitorar o acesso de pessoas no perímetro externo da organização; • Definir níveis de acesso, de acordo com o grau de risco, a recursos computacionais e informações; • Controlar a entrada e a saída de equipamentos e materiais relativos aos recursos computacionais; • Definir os sistemas de controle de acesso a serem utilizados (manual, semi e automático); • Monitoramento e alarme para tomada de ações de prevenção ou correção.

Fonte: Caiçara, 2016, p. 170.

Quadro 6 – Segurança física e ambiental (RH)

Aspectos	Pontos que podem ser observados
Recursos humanos e padrões de trabalho	• Definir políticas de seleção, recrutamento e contratação de pessoas alinhadas com a política de segurança da informação; • Segregar funções da força de trabalho envolvida com recursos computacionais estratégicos; • Manter um plano de capacitação e desenvolvimento das pessoas que atenda aos aspectos da política de segurança da informação; • Monitorar as situações de risco quanto a férias, horas extras, doenças, greves, sobrecarga, estresse, ergonomia ou outra situação; • Definir um plano emergencial para situações de greve ou contingências, se for o caso; • Estabelecer acordos de confidencialidade e responsabilidades; • Estabelecer normativa de procedimentos quanto ao uso dos recursos computacionais e das informações.

Fonte: Caiçara, 2016, p. 171.

Quadro 7 – Segurança física e ambiental (instalações)

Aspectos	Pontos que podem ser observados
Instalações elétricas e de telecomunicações	• Garantir a alimentação alternativa de energia elétrica para a continuidade das atividades computacionais (uso de geradores de emergência ou nobreaks); • Assegurar a estabilidade do fornecimento de energia elétrica pela concessionária local; • Evitar acondicionar cabos elétricos em dutos de cabos de transmissão de dados; • Utilizar tomadas e plugues apropriados para conexão dos equipamentos computacionais; • Garantir a exclusividade dos circuitos elétricos para atender aos equipamentos computacionais, evitando-se, assim, sobrecargas, quedas ou elevações de tensão elétrica; • Assegurar o aterramento de todos os equipamentos computacionais e partes metálicas existentes no ambiente, visando evitar a danificação dos equipamentos e possíveis choques elétricos nas pessoas; • Instalar para-raios; • Adequar o nível de iluminação dos ambientes computacionais às tarefas a que se destinam; • Procurar efetuar blindagem de equipamentos ou dispositivos que gerem radiações eletromagnéticas; • Realizar manutenção elétrica periodicamente; • Adequar as instalações elétricas e de telecomunicações conforme as normas vigentes no país.

Fonte: Caiçara, 2016, p. 171.

Quadro 8 – Segurança física e ambiental (condições ambientais)

Aspectos	Pontos que podem ser observados
Condições ambientais	• Proporcionar ventilação e climatização adequadas para o funcionamento dos recursos computacionais; • Evitar o acúmulo de poeira e fumaça decorrente de cigarros; • Manter o nível de temperatura e umidade adequado para cada tipo de recurso computacional (computadores em rede do tipo servidor e estação de trabalho e computadores de grande porte); • Pintar paredes, teto e piso adequadamente, de acordo com a finalidade do ambiente; • Armazenar corretamente mídias de segurança (backups), tanto no interior quanto no exterior da organização; • Manter as condições de limpeza e conservação em dia.

Fonte: Caiçara, 2016, p. 171.

A segurança lógica é definida por Caiçara (2015, p. 171) como “um conjunto de métodos e procedimentos automáticos e manuais destinados à proteção dos recursos computacionais contra o seu uso indevido ou desautorizado, que compreende o controle de consultas alterações e inserções e exclusões de dados controle de uso de programas e outros recursos”.

Os principais problemas e ameaças com relação à segurança lógica estão ligados à possibilidade de acesso indevido e a erros, sejam eles intencionais ou não. Consideramos também perda de dados, falhas ou ações e programas clandestinos na rede, violações dos sistemas que ocasionem desvio das informações, fraudes e sabotagens. Também há relação de medidas de proteção, para a questão da segurança lógica adequadas a cada área, conforme o Quadro 9.

Quadro 9 – Medidas de proteção segurança lógica

Aspectos	Pontos que devem ser observados
SEGURANÇA DE REDES	O acesso às redes aumentou significativamente os riscos para a segurança das informações, não apenas da organização, como também na utilização remota de computadores de modo geral. À medida em que as transações via rede se sofisticam, aumentam as vulnerabilidades decorrentes das ameaças externas causadas por invasores criminosos que atuam pela internet. Isso pode ocorrer por conta de concorrentes na área da espionagem, de pessoas com o intuito de obter vantagem ou ainda por ameaças de funcionários insatisfeitos. A maioria das grandes ameaças contra a segurança das redes está no controle de acesso, que ocorre nas etapas de identificação, autenticação e autorização, além do recebimento de programas clandestinos conhecidos como vírus ou programas com a finalidade de rastrear dados de um computador.
SEGURANÇA DOS SISTEMAS	• Entrada dos dados: validação dos dados, verificação de duplicidade de registros, valores fora do limite estabelecido, caracteres inválidos, dados ausentes, incompletos ou excessivos, não autorizados ou inconsistentes. • Processamento dos dados: controle para minimizar os erros ou falhas de processamento, garantia da integridade dos dados, consistências e validação das datas e cálculos utilizados. • Saída dos dados: controle de qualidade dos dados de saída, período de arquivamento, critério de destruição de relatório impresso, controle sobre os impressos negociáveis, controle de acesso a relatório de acordo com o nível de autorização de acesso e condição de emissão de relatórios confidenciais. • Armazenamento dos dados: critérios para criação de cópias de segurança de *backups*, locais destinados a armazenamento, meios utilizados para transporte de mídias, protocolos de remessa, recepção e testes periódicos das cópias de segurança. • Transmissão dos dados: controles para identificar modificações não autorizadas ou comprometimento do conteúdo das mensagens, confirmação de recebimento e retransmissão, controle de erros e do fluxo e controle na transmissão de informações sigilosas.
SEGURANÇA DO USUÁRIO	A proteção do usuário exige, além das medidas de segurança, medidas aplicadas às redes e aos sistemas e, principalmente, aquelas relacionadas ao aspecto comportamental. O usuário não atua de forma isolada, pois compartilha as informações a todo instante, tanto interna quanto externamente. As medidas de proteção aplicáveis aos usuários incluem controles de segregação de acessos, verificação contra programas clandestinos (vírus e *spywares*), uso de programas de bloqueio e filtragem de acesso interno e externo, procedimentos de acesso e políticas de utilização de equipamento portáteis.

Fonte: Elaborado com base em Caiçara, 2015, p. 172.

TEMA 4 – POLÍTICAS DE SEGURANÇA E BOAS PRÁTICAS DE SEGURANÇA

Caiçara (2015, p. 163) define: “a política ou plano de segurança da informação é um conjunto de princípios que norteiam a gestão da segurança da informação e que devem ser observados pelas pessoas que compõem a força de trabalho (corpo técnico, gerencial e demais usuários internos e externos)”. Ou

seja, trata-se de normatizar os procedimentos institucionais e tornar claras e objetivas as regras relacionadas à segurança do ambiente, sendo um instrumento preventivo para proteger a organização de ameaças. Por ameaças à segurança consideramos elementos como confidencialidade, integridade, autenticidade e disponibilidade.

As diretrizes que norteiam as políticas de segurança são estabelecidas por Caiçara (2015 p. 163). Trata-se dos “referenciais a serem seguidos por todos na organização, de modo a assegurar a confiabilidade dos recursos computacionais; também define os direitos e responsabilidades das pessoas envolvidas no contexto computacional da organização e que manipulam as informações”. Nesse sentido, as políticas de segurança de uma empresa devem ser divulgadas e conhecidas por todos os trabalhadores da organização, assim como devem estar descritas as penalidades as quais estarão sujeitos os que contrariarem o que foi estabelecido.

Segundo Caiçara (2015, p. 164), há atributos fundamentais para um bom plano que contenha a política de segurança da informação, que são:

- Estar alinhado com as estratégias da organização;
- Buscar menos um enfoque técnico e mais um enfoque nos procedimentos e no aspecto comportamental;
- Estar sintonizado com as pessoas que se envolvem no contexto computacional da organização;
- Ser decorrente da sensibilização da alta direção da empresa, pois a falta de Patrocínio desse nível praticamente inviabiliza qualquer proposta de política de segurança,
- Ser divulgado sistematicamente para as pessoas envolvidas apresentando organização e planejamento,
- Ser monitorado constantemente e revisado periodicamente.

Caiçara (2015, p. 164) também defende que, antes de a empresa iniciar a política da segurança da informação, ela necessita realizar uma análise dos riscos, visando identificar os recursos que devem ser protegidos e verificar as ameaças e consequências destes, além das vulnerabilidades existentes na organização. As políticas de segurança devem ser realizadas por um corpo de profissionais habilitado para tal fim; pode-se ainda contratar uma consultoria para que, junto com os profissionais das áreas críticas, as etapas do plano sejam desenvolvidas.

A elaboração de políticas de segurança da informação, de acordo com Caiçara (2015), deve ser realizada de modo holístico, que possibilite abranger a missão, a visão, as diretrizes organizacionais, as estratégias do negócio, os

planos de ação e as respectivas metas institucionais. Para que isso ocorra, a elaboração deve abranger os aspectos listados no Quadro 10.

Quadro 10 – Aspectos para elaboração de políticas de segurança da informação

Aspectos	Pontos a serem definidos
PRELIMINARES	• Estão relacionados à abrangência e escopo de atuação da política, como identificação dos recursos críticos, classificação das informações críticas, ameaças e vulnerabilidades existentes na organização. • As definições fundamentais sobre a terminologia a ser empregada e a estrutura de gestão adotada para administrar as questões de segurança da informação. • As normas e regulamentos aos quais a política está subordinada, assim como a definição de pessoa com autoridade para sancionar, implementar e fiscalizar o cumprimento da política. • Os meios que serão utilizados na divulgação do plano que conterá a política de segurança da informação e a forma e periodicidade da revisão da política.
HUMANOS DA SEGURANÇA	Definições sobre a política de segurança pessoal adotada pela organização no que se refere aos processos de admissão, contratação e demissão, os requisitos de segurança com prestadores de serviço, os treinamentos em segurança pessoal, bem como as diretrizes de comportamento esperado em relação à utilização dos recursos computacionais disponíveis.
SEGURANÇA FÍSICA	Definição quanto à proteção dos recursos e instalações que contêm as informações críticas da organização e que estão sujeitos a violação, sabotagens, desastres, acidentes, danos, perdas de dados, acessos não autorizados ou interferências.
SEGURANÇA LÓGICA	• Definições para assegurar a proteção direta das informações críticas da organização quanto à operação correta, ao armazenamento e ao acesso autorizado das informações (confidencialidade e integridade). • Definição quanto à utilização de senhas, instalação e utilização de *softwares* e procedimentos para utilização da internet. • Direitos e responsabilidades dos usuários, bem como as penalidades.
SEGURANÇA DAS COMUNICAÇÕES	Definição para proteger os dados e as informações durante os processos de comunicação.
TRATAMENTO DAS OCORRÊNCIAS	Definições dos procedimentos a serem adotados em casos de identificação, notificação, identificação e tratamento das ocorrências de segurança das informações.
DESENVOLVIMENTO, AQUISIÇÃO, IMPLANTAÇÃO, OPERAÇÃO E MANUTENÇÃO DOS SISTEMAS	Definição para padronização de procedimentos e controles a serem utilizados nas diversas etapas de um sistema, com a criação de trilhas de auditoria e relatórios gerenciais que possam subsidiar o monitoramento dos sistemas mais críticos.
PROTEÇÃO JURÍDICA E ECONÔMICA	Definição dos aspectos que podem exigir assessoramento e proteção jurídica e os que exigem cobertura por seguro.

(continua)

(continuação do Quadro 10)

CONTINGÊNCIA (CONTINUIDADE)	Definição dos procedimentos a serem contemplados no plano de contingência, com recomendações para que a organização se previna quanto à possível paralisação das atividades que são suportadas pelos sistemas de informação e quanto a falhas ou desastres.
IMPLEMENTAÇÃO, MONITORAMENTO E REVISÃO	Definições e como serão viabilizados a aplicação das políticas de segurança da informação (material, pessoas e financeiro) e o acompanhamento sistemático da implantação da política e dos procedimentos a serem adotados na revisão periódica (recomenda-se periodicidade anual).

Fonte: Elaborado com base em Caiçara, 2015, p. 165.

TEMA 5 – AUTENTICAÇÃO, AUTORIZAÇÃO, AUDITORIA, PRIVACIDADE, INTEGRIDADE E DISPONIBILIDADE DE SISTEMAS

A premissa básica de segurança envolve o controle ao acesso dos sistemas, que Caiçara (2015, p. 174) define da seguinte forma: “controles de acesso lógico são um conjunto de procedimentos e medidas que se destinam a proteger os dados, os programas e sistemas contra as tentativas de acesso não autorizado”. O autor afirma que este controle pode ser visualizado a partir do recurso computacional e a partir do usuário. O principal objetivo de controlar o acesso lógico é garantir que

> somente os usuários autorizados acessem os recursos computacionais da organização a partir de um acesso que possibilita a execução das suas atividades, que os sistemas críticos sejam monitorados sistematicamente e restrito a poucas pessoas, e seja vedado aos usuários a execução de transação incompatível com a sua função ou estejam além de suas responsabilidades. (Caiçara, 2015, p. 174)

Os controles de acesso normalmente ocorrem após o processo de *login*, que concede acesso aos dados e aplicativos do sistema. Para que isso ocorra, são necessárias a identificação do usuário (ID) e a autenticação do usuário, geralmente por uma senha. Um sistema de *login* é eficiente desde que (Caiçara, 2015, p. 174):

> garanta que o sistema será acessado apenas por pessoas autorizadas, que libere as informações após a conclusão do procedimento de identificação e autenticação, que durante o procedimento de login não forneça ajuda que possa levar pessoas não autorizadas a completar o acesso, finalize o procedimento depois de validados todos os dados e limite o número de tentativas de acesso sem sucesso; recomenda-se o limite máximo de três tentativas.

Existem outros meios de autenticar o acesso lógico. A utilização da biometria é um exemplo, e vem fazendo diminuir a ocorrência de fraudes, visto que se vale de uma característica física única do indivíduo. Para utilizar a

autenticação a partir da biometria, é necessário que cada usuário valide a sua identidade a partir da captura de características por meio de dispositivos de sensores.

Figura 4 – Biometria digital

Fonte: Laudon; Laudon, 2014, p. 275.

O PC da figura tem um leitor de impressão digital biométrico para acesso seguro e rápido de arquivos e redes. Vários recursos de *hardware* estão equipados com identificação biométrica para autenticar seus usuários (Laudon; Laudon, 2014). Algumas das aplicações de biometria são definidas por Caiçara (2015, p. 175):

- Identificação por meio de scanner da íris;
- Impressão digital;
- Reconhecimento da voz;
- Reconhecimento por meio do mapeamento facial;
- Identificação da retina;
- Geometria da mão;
- Reconhecimento da assinatura.

De acordo com Belmiro (2014), para que exista um bom sistema de controle relativo aos sistemas de informação, também são necessárias auditorias abrangentes e sistemáticas. Segundo o autor (p. 87),

> uma auditoria é um sistema que identifica todos os controles que governam sistemas individuais de informação e avalia sua efetividade. As auditorias de segurança devem requerer tecnologias, procedimentos, documentação, treinamento e recursos humanos; além disso, listam e classificam os pontos fracos do controle e estimam a probabilidade de ocorrer erros nesses pontos, avaliando o impacto financeiro e organizacional de cada ameaça.

Vejamos o Quadro 11 para um exemplo de listagem feita por um auditor para deficiências de controle.

Quadro 11 – Diagrama do exemplo de listagem

Função: Empréstimos pessoais **Localização: Peoria, IL**	**Preparado por: J. Ericson** **Data: 16 de junho de 2014**		**Recebido por: T. Benson** **Data de revisão: 28 de junho de 2014**	
Natureza e impacto das deficiências	Chance de erro/uso indevido		Notificação à administração	
	Sim/Não	Justificativa	Data do relatório	Resposta da administração
Contas de usuários sem senhas	Sim	Deixa o sistema aberto para pessoas externas não autorizadas ou hackers	10/05/14	Eliminar contas sem senhas
Rede configurada para permitir apenas compartilhamento de arquivos do sistema	Sim	Expõe arquivos de sistemas críticos para partes hostis conectadas à rede	10/05/14	Garantir que apenas diretórios necessários sejam compartilhados e que sejam protegidos por senhas fortes
Patches de software podem atualizar programas de produção sem aprovação final do grupo de Padrões e Controles	Não	Todos os programas de produção exigem autorização da administração; o grupo de Padrões e Controles determina, para tais casos, um status de produção temporária		

Fonte: Laudon; Laudon, 2014, p. 275.

De acordo com Laudon e Laudon (2014), o diagrama representa uma página da lista de deficiências de controle que um auditor poderia encontrar em um sistema de empréstimos de um banco. Além de ajudar o auditor a registrar e avaliar as deficiências de controle, o formulário mostra os resultados das discussões sobre essas deficiências com a administração, bem como quaisquer medidas corretivas tomadas por esta.

Se alguma ameaça ou problema real existir, é necessário um plano de contingência que garanta a integridade dos sistemas. Caiçara (2015, p. 176) define plano de contingência ou plano de continuidade

> como um conjunto de estratégias e procedimentos que devem ser adotados quando uma organização ou uma determinada área se depara com problemas que comprometam a continuidade normal das atividades de negócio; o procedimento estabelecido em um plano de contingência deve minimizar os impactos causados pelas ocorrências.

O plano de contingência é um instrumento com medidas de ações preventivas ou corretiva que visam dar continuidade a operações e deve constar em um documento que sirva como um guia para atender às características e necessidades da organização. Caiçara (2015, p. 166) defende que esse documento deve conter "a descrição completa detalhada e atualizada dos critérios, recursos, alternativas, responsabilidades, atribuições, providências ações e procedimentos a serem adotados no início, durante, e depois de pequenas e grandes situações de emergência no ambiente computacional das organizações".

Laudon e Laudon (2014) complementam que o plano de continuidade dos negócios concentra-se no modo como uma empresa pode restaurar suas operações após um desastre. Nesse sentido, é importante garantir a disponibilidade dos sistemas, visto que são vitais para o funcionamento das organizações

FINALIZANDO

Nesta aula aprofundamos os conceitos relativos à infraestrutura e à segurança dos sistemas de informação. Destacamos que, mesmo com as principais ferramentas de segurança, os sistemas de informação serão confiáveis e seguros somente se os profissionais souberem como e onde utilizá-los. Para isso, é imprescindível conhecer onde a empresa corre risco e quais os controles necessários para proteger os sistemas de informação, assim como o desenvolvimento de políticas de segurança e planos para manter o negócio em funcionamento se ocorrer de os sistemas de informação não operarem adequadamente. As empresas contam com ferramentas e tecnologias para proteger seus recursos de informação.

REFERÊNCIAS

BELMIRO, N. J. (Org.). **Sistemas computacionais**. São Paulo: Pearson, 2014.

CAIÇARA, C. J. **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.