CADERNO

DE

ESTUDO

FACULDADE

**Língua Portuguesa**

**Aula 1.1 – Teoria da comunicação: elementos da comunicação**

\*Comunicar é construir informações conjuntas entre quem fala e quem houve, utilizando-se da linguagem verbal ou não verbal.

\*6 elementos da comunicação – Compreender quais são os elementos

. Emissor , Receptor, Mensagem , Referente , Código e o Canal.

\*3 Pilares da teoria da comunicação de Roman Jakobson:

. Sempre existe um intenção por quem fala ou descreve , ou seja, por quem emite a mensagem;

. Todo evento comunicativo possui 6 elementos;

. O emissor dependendo de sua intenção, enfatiza alguns desses elementos, exercendo as funções da linguagem;

\*Ruídos da Comunicação são elementos que prejudicam a qualidade da comunicação.

**Aula 1.2 – Teoria da comunicação: Funções da linguagem**

Funções - Ênfase - Exemplo

Emotiva ou expressiva – Emissor,1ªPessoa – Um artigo de opinião

Conativa ou apelativa – Receptor,2ªPessoa – Uma propaganda

Poética – Mensagem – Um poema

Metalinguística – Código – Um termo de dicionário

Referencial – Contexto ou referente – Uma notícia

Fática – Canal – O contato inicial ao telefone “Alô!”

Elementos das funções da linguagem :

\*Que elemento enfatizar durante a comunicação;

\*O que são, como utilizá-las e como elas podem melhorar a nossa linguagem;

\*Identificar a função principal de um texto;

**Função Fática** – Centrada no elemento canal , Visa estabelecer, manter ou romper contato

**Função Referencial** – Centrada sobre o referente/contexto. Traz informações reais sobre o que acontece? Com quem? Onde ? Como ? Quando? . Usa a linguagem denotativa, objetiva. Visa descrever, narrar e informar sobre o mundo.

**Função expressiva ou emotiva** – Centrada no emissor – 1ª pessoa. Exprime atitudes, pensamentos, sentimentos, e posicionamentos do locutor em relação ao contéudo de sua mensagem e da situação. Visa demonstrar julgamentos, opiniões, exclamações, expressão de sentimentos.

**Função conativa ou apelativa** – Centra-se no destinatário/receptor ex: Textos publicitários, sermões, discursos políticos. Uso das formas verbais no imperativo, de pronomes pessoais e possessivos de 2ª pessoa, construindo uma relação dialogal e interpelativa. Visa fazer interpelações, solicitações, perguntas, convencer o interlocutor, dar ordens, sugerir...

**Função metalinguística** – Centrada sobre o código verbal . Visa estabelecer o código, evitando ambiguidades e certificando-se do seu sentido.

**Função Poética** – Centrada no formato do que se diz, mais do que na mensagem. Uso de recursos estilísticos literários e discursivos que trazem ao texto plurissignificados e ênfase nos fatores estéticos.

**Aula 2.1 – Estratégias de leitura – leitura textual ou literal**

Estratégias de Leitura : Visão Tradicional – Decodificar / Visão Moderna – Construir sentido

**Leitura Vertical :** Profunda, Reflexiva e analítica Ex: Textual/literal; contextual/entrelinhas; cultural /intertextual.

**Leitura Horizontal:** Superficial ( estrutura, títulos e subtítulos)

**Leitura textual/literal** : Identificar o gênero do texto, domínio discursivo, linguagem, veículo, informações literais etc.

**Leitura ascendente**: o ensino de leitura tradicional é fundamentado na concepção de leitura ascendente. De acordo com Kleiman (2002), alguns definem essa leitura como um processo de decodificação sonora das unidades linguísticas, e o sentido da leitura só pode sair da página impressa. Esse tipo de leitura também é conhecido como perspectiva do texto. Assim, o texto é, de acordo com Kleiman (2002), considerado um objeto completo.

**Leitura descendente:** essa perspectiva de leitura segue uma linha construtivista, segundo Figueiredo (1985). Nessa linha, a leitura é considerada um complexo processo psicolinguístico, e o leitor atinge o sentido do texto a partir de seu conhecimento de mundo e da criação de hipóteses.

**Leitura sociointeracionista:** essa perspectiva está relacionada com a psicolinguística, a teoria dos esquemas e a pragmática. Aqui, a leitura ocorre Estratégias de leitura – leitura textual ou literal 3 a partir dos dois movimentos anteriores: o ascendente e o descendente. Isso significa que ocorre uma integração entre a informação que o leitor encontra no texto impresso e o seu conhecimento de mundo, suas vivências. É o que se conhece por perspectiva moderna.

**Leituras verticais e Horizontais**

**Leitura horizontal :** \*Folear um jornal

**Leitura Vertical :** \*Leitura profunda – Textual=busca de informações literais. Contextual=busca construir informações nas pistas deixadas nas entrelinhas do texto.

**Leitura contemplativa, meditativa:** de acordo com o pesquisador (NASCIMENTO, 2009), é a leitura típica do livro. Nela, o leitor se dedica a uma leitura aprofundada, também chamada de vertical.

**Leitura movente, fragmentária:** para Nascimento (2009), essa leitura é típica da cidade, do leitor que recebe vários estímulos o tempo todo, como as pessoas que passam na rua, o outdoor, a buzina e o anúncio de carro de som.

**Leitura imersiva, virtual:** essa leitura se centra na era digital. Exige que o leitor faça seleções para não se perder na virtualidade.

**Leitura oral, dialógica:** Nascimento (2009) inclui, entre os tipos de leitura anteriores, citados por Santaella (2004), essa quarta classificação, que ele viu evidenciada à leitura contemplativa.

**Estratégias de leitura literal de um texto**

A compreensão literal se trata da reorganização de ideias, informações ou outros elementos do texto a partir das atividades de classificação, esboço, resumo e síntese**.**

**Classificação:** localização de categorias que aparecem no texto, como pessoas, lugares e ações.

**Esboço:** reprodução do texto em forma de esquema; usa frases, representações ou disposições gráficas.

**Resumo:** condensação do texto, que ocorre por meio de frases que narram os elementos ou fatos principais.

**Síntese:** conversão de diversas ideias, fatos ou elementos por meio de amplas formulações.

**Aula 2.2 – Estratégias de leitura – leitura texto e contexto**

Leitura contextual – **Procedimentos de análise**: responder a perguntas que mostrem o que há nas entrelinhas do texto.

**Perguntas:** Quem fala? Para quem? Como? O quê? Em que contexto?

Visa a interpretação, construção de sentido do texto, considerando informações implícitas e explícitas.

**Contexto e compreensão**

De acordo com Koch e Elias (2006), o contexto cognitivo dos interlocutores subsome os demais. Isso ocorre pois ele reúne todos os tipos de conhecimento arquivados na memória dos atores sociais que precisam ser mobilizados por ocasião do intercâmbio verbal. São eles:

O **conhecimento linguístico** propriamente dito;

O **conhecimento enciclopédico**, que pode ser declarativo (que se recebe pronto e é introjetado na memória “por ouvir falar”) ou episódico (adquirido por meio da convivência social e armazenado em “bloco” sobre as diversas situações e eventos da vida cotidiana);

O **conhecimento da situação comunicativa** e de suas “regras” (situacionalidade);

O **conhecimento superestrutural ou tipológico** (gêneros e tipos textuais);

O **conhecimento estilístico** (registros, variedades da língua e sua adequação às situações comunicativas);

O **conhecimento de outros textos** que permeiam a cultura (intertextualidade).

\***Leitura Contextual** – Visa a interpretação, construção de sentido do texto.

\*Considera informações explícitas e recupera as pistas deixadas no texto (informações implícitas).

**Analise do Texto** - \*Identificar marcas temporais , marcadores conversacionais, tempos verbais, pistas não verbais, advérbios, marcas de negação, etc.

\*Responder a pergunta que mostrem o que há nas entrelinhas do texto.

\***Quem fala** no texto? Que sujeitos sócio históricos são?

\***Para quem** fala?

\***O quê**?

\* **Como fala**?

\* **Por que fala**?

\* Em que **contextos restrito e amplo** fala?

# Aula 3.1– Estratégias de leitura - texto e intertextualidade

**Texto e intertextualidade**

\***Leitura cultural/intertextual** – Visa ao aprofundamento do sentido do texto, considerando o conhecimento prévio do leitor e o que há por trás das linhas do texto.

\***Leitura Cultural** – Análise pessoal, avaliação e julgamento do dito;

\***Procedimentos de análise** – Com quem os outros textos pode o leitor dialogar?

Que relação pode-se estabelecer entre esses textos ( paródia, paráfrase, alusão, citação...?)

Como o leitor se posiciona?

**Concepção de intertextualidade**

Nessa perspectiva, a intertextualidade é possível no processo do texto, e no ato de leitura, quando se pode notar o intertexto. Outro renomado teórico da intertextualidade, Gérard Genétte (1992), diz que a intertextualidade é um dos fenômenos da transtextualidade. Marcuschi (2008, p. 130) explica que fazem parte dessa transtextualidade:

A **intertextualidade**, que supõe a presença de um texto em outro (por citação, alusão, etc.);

A **paratextualidade**, que diz respeito ao entorno do texto propriamente dito, sua periferia (títulos, prefácios, ilustrações, encartes, etc.);

A **metatextualidade**, que se refere à relação de comentário de um texto por outro;

A **arquitextualidade**, bastante mais abstrata, que põe um texto em relação com as diversas classes às quais ele pertence (por exemplo, um poema de Baudelaire se encontra em relação de arquitextualidade com a classe dos sonetos, com a das obras simbolistas, com a dos poemas, com a das obras líricas, etc.);

A **hipertextualidade**, que recobre fenômenos como a paródia, o pastiche, etc.

Ao tratar os mecanismos da textualidade como critérios, Marcuschi (2008) ressalta que a intertextualidade é também um princípio constitutivo. Nesse sentido, ela compreende o texto como uma comunhão de discursos, e não como algo isolado ou apenas um simples critério de textualidade.

**Intertextualidade explícita e implícita**

A intertextualidade **explícita** ocorre quando se faz a citação da fonte do intertexto. Acontece, por exemplo, em discursos relatados, nas citações e referências, nos resumos, resenhas e traduções; e também nas retomadas de texto de parceiro para encadear sobre ele ou questioná-lo na conversação (KOCH; ELIAS, 2006). As teóricas explicam que a intertextualidade com explicitação da fonte aparece em diversos gêneros textuais. Porém, para que ocorra a produção de sentido, além da verificação do fenômeno, o leitor deve considerar a importância e a função da escolha realizada pelo autor.

A intertextualidade se constitui também de modo **implícito**. Pode ocorrer com alusões, na paródia, em certos tipos de paráfrases e ironias. Essa intertextualidade se dá sem a citação da fonte. Assim, é responsabilidade do interlocutor recuperar na memória a informação e construir o sentido do texto. Quando isso não ocorre, grande parte ou mesmo toda a construção do sentido fica prejudicada .

**Intertextualidade, leitura e produção de sentido**

A seguir, você pode compreender melhor algumas das categorias de intertextualidade. **Citação**: é identificável de modo imediato, tendo em vista o uso de marcas tipográficas específicas, como aspas, itálicos, separação do texto citado. Para Samoyault (2008, p. 49), “Basta uma dessas marcas para assinalar a citação, a ausência total de tipografia própria transforma a citação em plágio, cuja definição mínima poderia ser a citação sem aspas, a citação não marcada.”.

**Alusão**: remete a um texto anterior sem marcar a diferença da citação. De acordo com Samoyault (2008), às vezes não é intertextual propriamente dita, sendo exclusivamente semântica, como o enunciado “ele só pensa naquilo”, uma alusão erótica. Mas pode ser também uma alusão intertextual, como a realizada por James Joyce (apud SAMOYAULT, 2008, p. 50) em Ulysses, quando se refere à “Helena de Argos, a jumenta de Troia que não era de madeira e que alojou tantos heróis nos seus flancos.”. Aqui, há uma alusão mitológica e alegórica que não é plenamente visível. Esse tipo de intertextualidade depende muito do efeito de leitura. Ela é frequentemente subjetiva e raramente é necessário desvendá-la para compreender o texto.

**Plágio**: trata-se de uma retomada literal, porém sem marcas, o que torna a designação do heterogêneo nula. Quando ocorre a apropriação total, questões jurídicas devem ser levantadas a seu respeito, considerando que coloca em causa a propriedade literária, mais ou menos legitimada. Para a teórica, os termos de roubo e fraude são associados ao plágio e deslocam com mais frequência a questão do literário para o jurídico: “Introduzindo problemáticas ligadas à autoridade, à assinatura e à originalidade que ele anula, [...] o plágio merece assim ser mantido na tipologia, quando mesmo outras noções parecem poeticamente mais exatas ou mais eficazes para descrever certas operações de empréstimo.” (SAMOYAULT, 2008, p. 63).

**Paródia**: transforma uma obra precedente de modo a fazer uma caricatura ou reutilização de qualquer forma, transpondo-a. Sua construção visa à ludicidade, à subversão, de modo a desviar o hipotexto para zombar dele, e ainda à admiração. Possui caráter comum ao do patrimônio parodiado, o que possibilita aos leitores reconhecerem o hipotexto facilmente.

**Pastiche**: imita o hipotexto, remetendo “[...] menos a um texto preciso do que ao estilo característico de um autor e, para isso, o sujeito pouco importa.” (SAMOYAULT, 2008, p. 55). O pastiche admite variantes.

**Referência**: constitui-se também de intertextos ambíguos, assim como a alusão e o plágio. Para identificá-la, é necessário que o leitor possua determinada cultura e sagacidade, tornando a relação intertextual aleatória. Integração: seus operadores atuam nos textos que absorvem mais ou menos o texto anterior, em benefício da biblioteca no texto atual Estratégias de leitura – texto e intertextualidade 109 e, em seguida, de sua dissimulação, eventualmente (SAMOYAULT, 2008).

**Colagem**: nessas operações, o texto principal é colocado ao lado do intertexto e não o integra, o que valoriza o fragmentário e o heterogêneo. Elas podem aparecer acima do texto, como a epígrafe, e no meio do texto, como imagens colocadas no texto (SAMOYAULT, 2008).  Epígrafe: destacada do texto que ela antecede e introduz, a epígrafe é constituída, geralmente, por uma citação, com referência do autor e do texto do qual foi retirada. É uma colagem feita acima do texto, na sua abertura (SAMOYAULT, 2008).

**Leitura textual –** É a leitura das linhas, da superficialidade e materialidade do texto.

**Leitura Contextual** – É a leitura das entrelinhas das pistas deixadas no texto.

**Leitura cultural e intertextual –** É a leitura do que está por trás das linhas. – Visa ao aprofundamento do sentido do texto, considerando o conhecimento prévio do leitor e que há por trás das linhas do texto.

**Diálogos entre textos**

\*Paródia: Muda-se o conteúdo do texto utilizando a estrutura do texto original.

\*Paráfrase: Mantém-se o conteúdo, porém muda-se a estrutura.

**Aula 3.2– Tipos textuais – a descrição: elementos, estrutura e gêneros**

**Descrição**

\*Seu principal elemento é a Adjetivação que consiste em Identificar, Qualificar, Nomear, Quantifica, Localizar.

\* Pode ser Objetiva/Física – Verificação , Subjetiva/Psicológica- Percepção

\*Realiza-se em Gêneros como Anúncio, Relato, Reportagem, Catálogo, Guia Turístico

\*É utilizada para caracterizar Personagem, Espaço, Objetos, Pessoas, Lugares, Cenas

\*Tem o Efeito de levar o Receptor a produzir uma Imagem Mental

\*Utiliza como Recursos principais Os cincos sentidos, Percepção

**Descrição: concepções teóricas** A descrição é uma forma de apontar características de pessoas, seres, coisas, cenários, costumes e impressões. Ela se dá a partir de visão, tato, audição, olfato e paladar. O termo tem origem no latim descriptio, onis e significa figura, representação, escrever conforme o original, transcrever e copiar. De acordo com Vilela e Koch (2001, p. 549), a descrição “.

[...] consiste na exposição das propriedades, qualidades e características de objetos, ambientes, ações ou estados.”. A partir dela, o leitor pode visualizar mentalmente o objeto apresentado, que é concebido por meio de um processo linear de observação

**Descrição** : \*É caracterizar pessoas, cenas, objetos, lugares. \*É produzir uma imagem mental no interlocutor.

**Tipos de Descrição** – Objetiva ou Física – Verificação, uso dos sentidos. Subjetiva ou Psicológica – Sentimento e percepção.

**Objetivos da Descrição** – Nomear, identificar, Quantificar, Qualificar, Localizar, Para isto utilizamos como recursos os cinco sentidos e a percepção.

Os Gêneros em que se encontram sequências descritivas são: relatos de experiência e de pesquisas; reportagens; guias turísticos; catálogos; anúncios e diversos textos que caracterizam personagem e espaço narrativo.

**Aula 4.1– Composição Textual**

**Elementos da Narrativa**

I – **Apresentação** -Parte da narrativa, onde algumas informações das histórias são informadas: personagens, tempo, espaço, etc.

II – **Complicação** – Sucessão textual onde a trama e a ação começa a se desenvolver.

III – **Clímax** – Ponto crítico da história.

IV – **Desfecho** – Soluções para a resolução dos conflitos/dificuldades apresentadas.

V – **Tempo** - **\*Tempo Cronológico**: decorrer do tempo de forma cronológica, por meio de segundos, minutos, horas, dias, semanas, meses, anos, etc. É marcado por advérbios ou locuções adverbiais de tempo: ontem, há 10 anos, em 1990, etc.

\***Tempo Psicológico**: decorre independente do tempo cronológico. É marcado pelas impressões psicológicas dos personagens e revela informações sobre seus sentimentos. Ex: a saudade era infinita, o cárcere era infindável, o tempo passava voando, etc.

**VI – Espaço - \*Espaço Físico**: é o local onde ocorre a história, podendo ser imaginário( como no coração de uma pessoa), verossímil (como em um castelo) ou real ( como no Brasil, na Inglaterra, entre outros). **\*Espaço social**: É o espaço ocupado pelos personagens na esfera social: plebeus, monarcas, classe dos professores, etc. **\*Espaço psicológico**: É a conceitualização do espaço interno dos personagens, marcados por seus pensamentos, sentimentos, sensações, etc.

**VII – Personagem** - **\*Protagonista**: É o personagem principal da história, independente do seu caráter. **\*Antagonista**: É o personagem que se opõe ao protagonista, independente do seu caráter. **\*Secundário**: É o personagem que ocupa posições secundárias na história e serve apenas de apoio para o enredo.

**VIII – Narrador** - **\*Narrador-Personagem**: É, ao mesmo tempo, personagem e narrador. Conta a história sob a perspectiva de quem participa dela. **\*Narrador-Observador**: É um narrador neutro, que conta a história observada por uma perspectiva de fora. Tem conhecimentos limitados e não sabe todos os detalhes de todos os componentes da história. **\*Narrador – Onisciente Neutro**: é um narrador que sabe de todos os detalhes da história, sentimentos dos personagens, entre outros, e conta ao leitor o que é preciso saber para desenrolar da história, sem dar suas opiniões. **\*Narrador-Onisciente seletivo**: É o narrador que também sabe de tudo sobre a história, mas que emite suas opiniões a respeito de partes dela, induzindo o leitor.

**IX – Foco Narrativo** - **\*Foco Narrativo em Primeira Pessoa**: Ocorre quando a narrativa acontece sob a perspectiva de alguém que vivenciou a história. **\*Foco Narrativo em Terceira Pessoa**: Acontece quando a narrativa acontece sob a perspectiva de alguém que não vivenciou a história, mas que a contou observando de fora. Contada em terceira pessoa: Ele, ela, eles, elas, etc.

**TECNOLOGIA DA INFORMAÇÃO APLICADA À GESTÃO**

**Aula 3.2 – Alinhar as decisões da ti e do negócio**

**\***Impacto estratégico da carteira de desenvolvimento de aplicativos:

1. Nível do suporte: A Ti tem uma pequena influência nas estratégias atuas e futuras da empresa.

2. Nível Fabril : Aplicações de Ti contribui para o sucesso da empresa.

3 Nível de Transição : A Ti passa de uma posição discreta , para destaque da empresa.

4. Nível Estratégico: A Ti tem grande influência nas estratégias gerais da empresa.

**Aula 4.1 – Competindo com a tecnologia da Informação**

\*Estratégicas Básicas e uso estratégico da Tecnologia da Informação (TI)

Estratégicas organizacionais básicas

1.Diferenciação

2.Liderança em Custos

3.Crescimento

4.Inovação

5.Aliança

Estratégicas Básicas de uso empresarial da TI

1.Desenvolver novos atributos da TI para diferenciar produtos e serviços.

2.Utilizar a Ti para reduzir os custos dos ´processos empresariais.

3.Utilizar a TI para gerenciar a expansão regional e global da empresa.

4.Criar novos produtos e serviços que incluam componentes da TI

5.Utilizar a TI para cria parcerias virtuais.

\*Cinco Forças competitivas definidas por Michael Porter

1.Rivalidade dos concorrentes dentro do setor;

2.Ameaça de novos concorrentes;

3.Ameaça causa por produtos substitutos;

4.Poder de barganha dos clientes;

5.Poder de barganha dos fornecedores;

\*Cincos Estratégicas competitivas básicas

1.Liderança em custos;

2.Diferenciação de produtos ou serviços;

3.Inovação de novas maneiras de fazer negócios;

4.Crescimento afim de expandir para os novos mercados;

5.Aliança com clientes, fornecedores e até competidores;

**Aula 4.2 – Gerenciamento global e na empresa da tecnologia de informação**

Arquitetura da tecnologia da informação (TI)

**Plataforma da tecnologia**; a internet, as intranets, extranets e outras redes, e os sistemas de computadores fornecem uma infraestrutura de computação e de comunicação que apoia o uso estratégico da TI para os negócios corporativos.

**Recursos de dados**: Diversos tipos de banco de dados operacionais e especializados armazenam e fornecem dados e informações para os processos de negócios e apoio à tomada de decisão.

**Arquitetura de aplicativos**: aplicativos de TI são projetados como uma arquitetura integrada de sistemas empresariais que apoiam iniciativas estratégicas de negócios.

**Organização da TI**: a estrutura organizacional da função de sistemas de informação é projetada para alcançar as variáveis estratégicas de negócio.

**Direcionadores de negócios para a TI global**

Clientes globais. Clientes são pessoas que podem viajar a qualquer lugar ou companhias com operações globais. A TI global ajuda a fornecer serviços rápidos e adequados. • Produtos globais. Produtos são os mesmos em todo o mundo ou são montados por subsidiárias em todo o planeta. A TI global pode ajudar a administrar o mercado global e controlar a qualidade.

• Operações globais. Partes de uma produção ou processo de montagem são designadas a subsidiárias com base em condições econômicas ou outra qualquer. Apenas a TI global pode apoiar tal flexibilidade geográfica.

• Recursos globais. O uso e o custo de equipamentos comuns, instalações e pessoas são compartilhados por subsidiárias de uma companhia global. A TI global pode rastrear tais recursos compartilhados.

• Colaboração global. O conhecimento e a perícia dos colegas em uma companhia global podem ser rapidamente acessados, compartilhados e organizados para apoiar os esforços individuais ou do grupo. Apenas a TI global consegue apoiar tal colaboração empresarial

**Questões das comunicações de dados internacionais**

**Questões de administração de rede**

• Melhorar a eficiência operacional das redes • Operar com redes diferentes • Controlar a segurança de comunicação de dado

**Questões regulatórias**

• Lidar com restrições de fluxo de dados transnacionais • Administrar regulamentações de telecomunicação internacional • Manejar política internacional

**Questões da tecnologia**

• Gerenciar a infraestrutura de rede entre os países • Gerenciar a integração internacional de tecnologias

**Questões orientadas aos países**

• Reconciliar as diferenças nacionais • Lidar com estruturas tarifárias internacionais

**Como a TI deve ser gerenciada?**

A Ti deve ser gerenciada, para fortalecer o alinhamento estratégico.

Gerenciar o desenvolvimento e a implementação da TI.

Gerenciar o desenvolvimento e a implementação de novos aplicativos.

Gerenciar a organização e a infraestrutura da TI.

**Arquitetura de TI – É preciso se preocupar com:**

\*Plataforma de tecnologia – Internet, intranet, extranet, sistemas de computação.

\* Recursos de dados

Arquitetura de Aplicativos

Organização da TI

**Aula 5.1 – Gestão da tecnologia da informação e do conhecimento**

**Aplicação da gestão do conhecimento**

**Criação de canais de Discussão**; A criação de canais de discussão quebra alguns paradigmas.

**Reunião para coletar ideias**: Pode-se utilizar a técnica brainstorming, levantando questões, discutindo e analisando diferentes pontos de vista.

**Documentação das lições**: Todas as atividades realizadas pela organização devem ter suas lições registradas e discutidas.

**Transformação em conhecimento**: A organização deve encontrar alternativas para conhecer e utilizar junto ao colaborador essas boas ideias e concretizá-las, transformando-as em conhecimento.

**1.A gestão da informação e do conhecimento**

Um **dado** é qualquer elemento identificado na sua forma bruta que, por si só, não conduz a uma compreensão de determinada situação. Uma **informação** é o resultado do processamento e da manipulação de um conjunto de dados de forma a torná-los significativos e úteis. Um **conhecimento** pode ser visto como um conjunto de informações relacionadas entre si, que exploram as possibilidades dentro de um contexto.

Para Burstein e Holsapple (2016), o conhecimento tem características que o diferenciam dos outros ativos da organização, como você pode ver a seguir;

. **Alavancagem extraordinária e lucros crescentes:** o conhecimento não está sujeito à diminuição dos lucros, ou seja, quando é utilizado, ele não é consumido. Assim, os seus consumidores podem adicionar mais conhecimento àquele existente, aumentando o seu valor.

. **Fragmentação, dinamismo e necessidade de atualização**: à medida que o conhecimento aumenta, ele se ramifica e se fragmenta. O conhecimento é dinâmico; ele é informação em ação. Portanto, uma organização deve atualizar continuamente a sua base de conhecimentos para mantê-la como uma fonte de vantagem competitiva.

. **Valor incerto**: é difícil estimar o impacto de um investimento em conhecimento, uma vez que há muitos aspectos intangíveis.

. **Valor incerto do compartilhamento**: analogamente, é difícil estimar o valor do compartilhamento do conhecimento ou quem mais se beneficiará dele.

. **Conhecimento arraigado no tempo**: a utilidade e a validade do conhecimento podem variar com o tempo. Consequentemente, a disponibilidade imediata, o envelhecimento, a caducidade e a volatilidade desse conhecimento são atributos importantes.

. **Conhecimento explícito** está voltado para o conhecimento técnico, racional e objetivo (dados, procedimentos, políticas, software, etc.).

. **Conhecimento tácito** normalmente está no domínio da aprendizagem cognitiva subjetiva e experiencial, sendo altamente pessoal e difícil de formalizar.

As ferramentas de tecnologia que dão suporte à gestão do conhecimento são conhecidas como **knowware.** A maioria dos pacotes de sistemas de gestão de conhecimento contemplam ferramentas como computação colaborativa, servidores de conhecimento, portais corporativos de conhecimento, sistemas eletrônicos de gestão de documentos, ferramentas de coleta de conhecimento, mecanismos de busca e conjuntos de gestão do conhecimento.

# Aula 5.2 – Desafios éticos, sociais e de segurança da tecnologia de informação

# Crimes em informática

# Crimes cibernéticos são : Pirataria de software, Vírus de computador e worms Roubo Cinético, Fraudes digitais, Adware e spyware, Uso não autorizado no trabalho, Furto de propriedade intelectual, Ciberterrorismo – ( sabotagem de sistemas e infraestrutura), Hacking e Cracking – ( monitoramento de e-mail, invasão de computadores e redes).

**Aspectos éticos**

A **ética** trata dos comportamentos habituais da sociedade e de como são atribuídos os conceitos de bem e mal a esses comportamentos. O mau uso do acesso a um sistema é uma das ameaças mais difíceis de se identificar. Por exemplo, um funcionário de uma bempresa pode estar autorizado a acessar o sistema e, ainda assim, ser uma grande ameaça à segurança da informação.

A ética no tratamento de dados e informações se divide em quatro temas principais:

**Privacidade** — preservação da privacidade ou identidade de acesso às informações. A privacidade de dados muitas vezes está ligada à segurança individual, explicando os controles rígidos adotados pelas empresas para a guarda dos endereços de celebridades ou dos saldos de contas bancárias, por exemplo. Para manter a privacidade, empresas possuem documentos descrevendo suas políticas e suas ações no que se refere à privacidade e ao sigilo das informações dos usuários e dos clientes.

**Acuidade (precisão)** — as ações empresariais, como as ações de marketing, são essenciais nas corporações. Para que tais ações atinjam o objetivo determinado, é essencial que as informações disponíveis nos bancos de dados do sistema utilizado sejam precisas. Por exemplo, no caso de uma empresa desejar enviar um flyer de Dia da Mulher para todas as mulheres cadastradas no sistema, para que o marketing aconteça de forma correta, é necessário que as informações estejam precisas quanto ao sexo de todos os clientes cadastrados.

**Propriedade** — a propriedade intelectual dos dados, modelos, conceitos e documentos utilizados pela empresa deve ser sempre bem estabelecida, sendo respeitada e devendo ser tomados os devidos cuidados para que os dados sejam preservados do acesso e uso indevidos. Por exemplo, ao cadastrar um cliente, inserindo no sistema seus dados pessoais, a empresa será responsável por informar ao mesmo que está sendo efetuado um cadastro e que a empresa se manterá responsável por resguardar essas informações.

**Acesso** — para manter dados e informações em segurança, é necessário que a empresa estabeleça, claramente, quem pode ter acesso aos dados e às informações disponíveis

A manutenção de um comportamento ético envolve os seguintes aspectos:

**Conhecimento** — a empresa deve ter gerência e controle sobre os dados registrados em seus bancos de dados, e os clientes devem estar informados sobre a retenção desses dados.

**Consentimento** — a empresa somente deve usar os dados com o consentimento e a autorização dos clientes, parceiros e fornecedores a que esses dados se referem.

**Controle** — o cliente interessado deve poder consultar seus dados e modificá-los caso estejam incorretos.

**Notificação** — se houver uso dos dados para outras finalidades diferentes das originais, o cliente deve ser avisado previamente.

**Segurança da informação e estratégias**

A segurança da informação é primordial para que as informações sejam salvaguardadas de quaisquer desvios ou interferências que ocasionem a sua alteração.

As **ameaças à segurança da informação** são relacionadas diretamente à perda de uma das suas três principais características: a confidencialidade, a integridade e a disponibilidade. Vejamos o que acontece em caso de prejuízos a cada uma delas:

**Perda de confidencialidade** — há uma quebra de sigilo de uma determinada informação permitindo que sejam expostas informações restritas, as quais seriam acessíveis apenas por um determinado grupo de usuários.

**Perda de integridade** — determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.

**Perda de disponibilidade** — a informação deixa de estar acessível para quem necessita dela.

**Crimes relacionados com a tecnologia da informação**

Com a expansão do uso de tecnologias e o compartilhamento de informações, há um crescimento de crimes nas áreas em questão.

**Scan —** é um ataque que quebra a confidencialidade com o objetivo de analisar detalhes dos computadores presentes na rede (como sistema operacional, atividades e serviços) e identificar possíveis alvos para outros ataques. As principais formas de prevenção são a manutenção de um firewall na empresa e uma configuração adequada da rede.

**Fraude —** a fraude, ou o scam (com “m”), abrange uma quantidade ampla de tipos de ataque. Um dos mais comuns é o phishing, que, para obter informações do usuário, utiliza estratégias como a cópia da interface de sites famosos e o envio de e-mails ou mensagens falsas com links suspeitos. O principal meio de evitar fraudes é a conscientização dos usuários por meio de treinamentos sobre cuidados na rede

**Ataques ao servidor web** — os primeiros ataques de rede exploravam as vulnerabilidades relacionadas com a implementação de conjuntos de protocolos TCP/IP. O princípio básico durante qualquer desenvolvimento informático é que não se deve confiar nos dados enviados pelo cliente. Quase todas as vulnerabilidades dos serviços web estão relacionadas à negligência dos desenvolvedores, que não são cuidadosos o suficiente em relação ao formato dos dados inseridos pelos usuários. Os ataques contra os aplicativos web são sempre prejudiciais, porque denigrem a imagem da empresa.

**Worms** — são alguns dos malwares mais comuns e antigos. Malwares são softwares que têm como intuito 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 de se espalhar rapidamente pela rede e afetar arquivos sigilosos da empresa. Os principais meios de prevenção são a manutenção dos antivírus e os treinamentos de conscientização.

**DoS Attack** — é um ataque em que um computador denominado mestre pode ter sob o seu comando até milhares de computadores “zumbis”. Esse ataque consiste em fazer com que as máquinas infectadas e sob o comando do computador mestre se preparem para obedecer a um determinado recurso em um determinado servidor. Dependendo do recurso atacado, o servidor pode chegar a reiniciar ou até mesmo ficar travado.

Além dos incidentes de segurança da informação citados, vamos apontar os principais crimes cometidos na Internet:

**Injúria e difamação** — divulgar informações falsas em relação a uma pessoa ou a uma empresa é crime e pode levar a diversas penalidades. Quando esse crime ocorrer por meio da Internet, será considerado um crime virtual. Vale destacar que as vítimas podem acessar o poder judiciário e requerer indenização e reparação do dano. Para isso é essencial procurar uma delegacia especializada e registrar denúncia. Vejamos o que o Código Penal brasileiro dispõe sobre a injúria e a difamação nos arts. 139 e 140: “Art. 139. Difamar alguém, imputando-lhe fato ofensivo à sua reputação: […]”; “Art. 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro […]” (BRASIL, 1940, documento on-line).

**Utilização de softwares falsos** — alguns softwares, quando instalados em um computador, permitem acesso a todos os dados pessoais registrados na máquina. Com os dados em mãos, é possível falsificar cartões de créditos, realizar transações bancárias e muito mais. O crime de invasão e roubo de dados é mais comum do que pode parecer e está previsto no art. 154-A do Código Penal brasileiro, nos seguintes termos: Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: […] (BRASIL, 1940, documento on-line).

**Criação de perfis falsos** — ao criar contas utilizando nomes falsos, os usuários podem divulgar conteúdos mentirosos e gerar vários problemas, como a disseminação de fake news.

**Apologia ao crime** — é comum a criação de páginas e perfis que estimulem a prática de crimes como pedofilia, racismo, furtos, etc. Esses perfis geralmente possuem acesso privado, e os membros compartilham dicas e sugestões para a prática de atos ilícitos. ν

**Plágio** — é a cópia de informações veiculadas por terceiros sem a indicação da fonte. O crime está previsto na Lei nº. 9.610, de 19 de fevereiro de 1998, que dispõe sobre a proteção dos direitos autorais, e aquele que o comete pode sofrer pena de detenção e ser obrigado ao pagamento de multa.

# Aula 6.1 – Segurança em TI, Crimes, Conformidade e Continuidade I

**Principais ameaças à segurança da informação:**

**\***Divulgação/roubo de senhas

\*Erros e acidentes

\*Pirataria

\*Ataque de negação de serviço

\*Phishing

\*Roubos de notebooks

\*Falha na segurança física

\*Spywares

\*Fraudes

\*Spam

\*Vírus

Para gerenciar, primeiro conhecemos, depois, analisamos, implantamos e administramos o assunto, seguindo assim uma sequência lógica. A importância disso está relacionada ao fato de que os ataques a informação têm crescido nos últimos anos, ocasionando consideráveis prejuízos, por exemplo, ataques do tipo Denial of Service (DoS) (negação de serviço) que ocorrem quando um site recebe um grande número de solicitações, além de sua capacidade, fazendo com que ele falhe e não disponibilize as informações aos usuários. Uma forma de evidenciar esse conceito é utilizando o ciclo planejar, desenvolver, controlar e agir (PDCA, em inglês plan, do, check, act), encontrado na literatura da qualidade. Veja o Quadro1, que apresenta um resumo da ferramenta e dessa sequência.

**Planejar**- Nesta fase a empresa deve conhecer suas estruturas e informações, realizando uma análise para que, assim, possa dimensionar os sistemas de segurança capazes de dar o suporte necessário as suas atividades com segurança e confiança. Aqui serão identificados os riscos (probabilidade de uma ameaça explorar uma vulnerabilidade) e as ameaças (situação em que alguém ou algo poderá causar danos a um ou vários usuários dentro da organização).

**Desenvolver** - Nesta fase a empresa realiza a implementação dos atributos de segurança necessários a manter a informação ao alcance de todos os envolvidos no processo, realizando essa implementação nos equipamentos e sistemas de acesso e execução de programas para o desenvolvimento das atividades afins na empresa, como a utilização de contramedidas (recursos de segurança adotados para reduzir os riscos);

**Controlar** - Nesta fase a empresa controla a utilização e acessos às informações para a verificação das boas práticas e se essas rotinas estão sendo utilizadas para o crescimento da organização;

**Agir** - Nesta fase a empresa realiza ações de melhorias nos processos ou correções, para que cada vez mais a segurança da informação tenha aderência aos processos da organização;

**Conhecendo a segurança da informação**

A segurança da informação tem como meta a proteção da informação, seja ela impressa ou eletrônica, bem como os meios de armazenamento e utilização, por exemplo, os usuários que acessam esses equipamentos. Não basta proteger só os equipamentos se, por exemplo, os usuários liberarem informações sem as devidas permissões a pessoas fora do processo. A segurança da informação está diretamente relacionada com os riscos aos dados, aos sistemas de informação e as redes de comunicação.

**Pilares da Segurança da Informação**

**Integridade** vem do latim integritate, que significa a qualidade de alguém ou algo de ser íntegro, de conduta reta, pessoa de honra, ética, educada, cuja natureza de ação nos dá uma imagem de inocência, pureza ou castidade, o que é íntegro, é justo e perfeito.

**Confidencialidade** é a qualidade daquilo que é confidencial (que se diz ou que se faz com confiança e com segurança recíproca entre dois ou mais indivíduos). Para a segurança da informação, confidencialidade é a propriedade da informação que não estará disponível ou divulgada a indivíduos, entidades ou processos sem autorização.

O conceito de **disponibilidade** é utilizado em diversas áreas e esferas para fazer referência à possibilidade de que algo, um produto ou serviço, esteja disponível de ser realizado, encontrado ou utilizado. Para a segurança da informação, significa que a informação deve ficar disponível ao uso para quem tem autorização.

**Mecanismos de segurança**

**Mecanismos de segurança** são medidas que visam controlar o acesso às informações de forma física e lógica. Enquanto os controles físicos limitam o contato direto que um usuário pode ter com a informação e toda a estrutura que a envolve, os controles lógicos trabalham pela integridade da informação de modo que ela não seja acessada e manipulada. Alguns exemplos de mecanismos de segurança são (ALERTA SECURITY, 2016b):

**Criptografia:** um conhecido meio de converter os dados em um formato que seja impossível decifrá-lo. Imagine que para assegurar que os dados, em idioma português, não sejam compreendidos por meros falantes da língua, as informações sejam convertidas para o hebraico. O raciocínio é muito similar a isso, porém, criptografar é impedir completamente a interpretação das informações, e elas só voltam ao estado inteligível quando uma chave (senha) for inserida.

**Assinatura digital:** com a assinatura digital é garantida a integridade dos dados por meio de criptografia, ou seja, seu acesso pode ser irrestrito e seu conteúdo não pode ser modificado.

**Certificação:** uma certificação é como um atestado de autenticidade de um arquivo, uma garantia de que o mesmo é válido.

**Honeypot:** trata-se de um software que age como um antivírus em tempo real, cuja função é proteger os dados de invasores, aplicações maliciosas e estranhas ao sistema. A diferença é que, em vez de mantê-lo em quarentena, por exemplo, o honeyspot ludibria esse invasor, fazendo-o acreditar que está tendo acesso real às informações.

**Crimes em Informática**

Os crimes em informática estão crescendo muito, tanto pelo desconhecimento como pelo aumento de usuários na rede. As informações são preciosas para seu autor seja ele uma pessoa física ou uma organização que necessita de suas informações para planejamentos ou para rodar seus processos diariamente.

**Crimes de falsificação** - Trata-se de cópia de um software protegido por direitos autorais que é imitado em sua embalagem, etiqueta e demais informações, com visual muito próximo ao original para sua comercialização.

**CDROM pirata** - Também é um caso de falsificação, só que neste caso o usuário já sabe que está adquirindo uma cópia ilegal do que está procurando, por exemplo, um programa, um filme ou uma música, é encontrado normalmente em pontos de comércio popular, feito em uma mídia regravável, com valor bem abaixo do normal. Em uma única mídia é possível encontrar uma coletânea de mais de um original, por exemplo, todos os lançamentos de um músico.

**Revendas de hardware** - Acontece quando uma empresa ou pessoa vende um computador, seja em uma loja física ou virtual e entrega esse hardware com algum programa instalado pirata ou afirmando ser original, mas sem oferecer ao usuário a licença original ou a documentação técnica. Por exemplo, você compra um notebook já com o programa operacional instalado e não se preocupa em verificar se esse programa foi devidamente licenciado.

**Pirataria individual** - Ocorre quando uma pessoa, por amizade ou por não entender a gravidade do ato, oferta programas que comprou a colegas ou amigos, ela tem a licença de uso individual, mas realizando esse ato de compartilhar acaba por criar um problema grande não percebendo a gravidade e dimensão que isso pode ocasionar. Pirataria corporativa Parte do mesmo princípio da pirataria individual, ocorrendo em progressão geométrica. Imagine em uma empresa, ela compra licença de uso para um computador e instala nos outros 199 que possui. Nesse tipo de pirataria estão concentradas as maiores perdas do setor de software, pois são muitos hardwares funcionando com licenças copiadas. De fato, não são todas as organizações que cometem esse delito, há muitas que tem um rígido controle sobre o uso e adquirem corretamente as licenças para uso de programas.

**Pirataria cliente/ servidor** - Geralmente ocorre quando uma empresa entra em rede, ou seja, deixa de operar com estações separadas e utiliza um servidor com estações ligadas em rede. Nesse processo pode que ter, mesmo sem saber (quando faz o serviço com terceiros), instaladas cópias piratas ou acessos ilegais a programas compartilhados com um limite maior do que a licença permite, sendo essa prática um crime.

**Pirataria on-line** - Atualmente não há como ficar desconectado, seja em casa ou nos ambientes coorporativos. Com esse advento, a pirataria on-line vem crescendo na mesma proporção, os software são transferidos e instalados ilegalmente e anonimamente.

**Insegurança na internet**

A rede de computadores veio para o auxiliar a disseminação da informação e o acesso mais democrático delas pelas pessoas e empresas que antes não podiam ter acesso. Assim, além dos benefícios vieram também os malefícios da modernidade.

**Espionagem:** podem ser militares, de estado ou em empresas industriais, podem ser contratados por concorrentes ou inimigos para roubar ou destruir os dados de outros.

**Proveito próprio**: quando o ataque objetiva obter proveitos próprios, muitas vezes financeiros, por exemplo: transferências de numerário, resultados de concursos, uso de redes de telefonia ou dados sem os encargos.

**Vingança**: pessoas comuns, empresas ou até mesmo outro criminoso, pode até ser realizado por um não hacker, pode ser um ex-funcionário que está descontente com a antiga empresa, ou um ex-namorado que sai de um relacionamento e quer prejudicar a outra parte.

**Status,** **poder, necessidade de aceitação:** há nitidamente uma concorrência entre esses criminosos, eles querem sempre superar seus pares, sendo reconhecidos nesse submundo.

**Aventura:** esses criminosos, em maioria, são dotados da necessidade de aventura e desafios, partindo, por exemplo, do grau de dificuldade de invadir determinado sistema, os alvos mais cobiçados são plataformas de governos e instituições de segurança mundial.

**Maldade:** infelizmente o simples prazer de destruir faz parte do dia a dia desses criminosos, alguns deles têm o ego alto e para satisfazer esse ego cometem os crimes.