# INTRODUÇÃO

No mundo digital em constante evolução, a segurança da informação tornou-se um tema essencial e uma preocupação fundamental para empresas, organizações e indivíduos. A rápida expansão da tecnologia e a interconexão global aumentaram a quantidade de informações e dados transmitidos e armazenados eletronicamente. No entanto, essa crescente dependência da tecnologia também trouxe consigo uma série de ameaças cibernéticas cada vez mais sofisticadas.

A segurança da informação refere-se à proteção dos dados, informações e sistemas contra acessos não autorizados, uso indevido, alteração, destruição ou qualquer outra forma de comprometimento. O objetivo é garantir a confidencialidade, integridade e disponibilidade das informações, bem como a proteção da privacidade e dos direitos dos indivíduos e organizações.
As ameaças à segurança da informação são diversas e constantemente em evolução. Hackers, crackers, malware, phishing, ransomware e ataques de engenharia social são apenas algumas das ameaças que podem comprometer a segurança dos sistemas e dos dados. Além disso, fatores humanos, como negligência, erro ou má conduta, também podem representar riscos significativos.

Para garantir a segurança da informação, é necessário adotar uma abordagem holística que engloba várias camadas de proteção. Podemos incluir aí a implementação de políticas e procedimentos de segurança, o uso de tecnologias avançadas de criptografia, adoção de práticas seguras de desenvolvimento de software, realização de testes regulares de segurança e a conscientização e treinamento dos usuários.

A segurança da informação não se limita apenas às organizações, inclusive é uma responsabilidade individual. Cada pessoa que utiliza a tecnologia deve estar ciente dos riscos e adotar medidas para proteger suas informações pessoais e digitais.

Nesta era digital, em que a informação é um ativo valioso, a segurança da informação é essencial para garantir a confiança, privacidade e confidencialidade. É uma área em constante evolução, impulsionada pelo avanço tecnológico e pela crescente sofisticação das ameaças cibernéticas. Assim sendo, este módulo possibilitará conhecer os conceitos fundamentais da segurança da informação, e abrange, entre outros assuntos, o acesso a ferramentas e sistemas que facilitarão iniciar o técnicas para garantir a segurança e integridade da informação no âmbito digital.

# TEMA 1
# Segurança da Informação e suas características

## Habilidades:

- Identificar os fundamentos da segurança da informação.
- Entender a importância da informação e dados.
- Operar mecanismos de segurança da informação.

A segurança da informação é um conjunto de medidas e práticas adotadas para proteger os dados, informações e sistemas contra ameaças, dessa forma, garante-se a confidencialidade, integridade e disponibilidade das informações. Essa disciplina visa preservar a segurança dos ativos de informação, sejam físicos ou digitais, e envolve a implementação de políticas, procedimentos, tecnologias e treinamentos. A Segurança da Informação é padronizada pelas **normas da família ISO/IEC 27000**, que abordam exclusivamente este tema (Sistema de Gestão e Segurança da Informação).

## Cyber Security

A Segurança Cibernética (Cyber Security) contempla a proteção dos dados e informações que transitam através de um local informatizado, ou seja, é focada na defesa dos dados e informações em meios digitais. Cyber Security é uma das facetas da Segurança da Informação, já que os dados e informações não necessariamente estarão em meios físicos, como contratos físicos (papel), documentos e cartas, por exemplo, mas também em ambientes informáticos.

Tanto a Segurança da Informação quanto a Segurança Cibernética transitam não somente no meio organizacional e corporativo, assim como na nossa rotina. Compartilhamos dados a todo momento e/ou dependemos de serviços externos para requisitar ações em diversos ambientes informatizados no nosso dia a dia. Cabe a nós, da mesma forma, aprendermos a nos prevenir e a remediar os riscos.

## Conceitos-base

Para prosseguirmos, é de extrema importância entendermos alguns conceitos.

### Dados:

- Os dados são fatos brutos, que podem ser quantitativos ou qualitativos, como números, palavras, símbolos ou valores. Não têm contexto ou significado intrínseco - significação por si próprio.
- São tipicamente representados de forma objetiva e podem ser coletados, armazenados e processados em diferentes formatos, como planilhas, bancos de dados ou arquivos digitais.
- Podem ser estruturados, como dados organizados em tabelas, ou não estruturados, como textos livres, imagens, áudio e vídeos.

### Informação:

- A informação é o resultado do processamento e interpretação dos dados. Tem significado e contexto atribuídos a ela, o que a torna relevante e útil para as pessoas.
- É o produto da análise, organização, contextualização e interpretação dos dados. Fornece conhecimento, *insights* ou respostas a perguntas específicas.
- É comunicada de forma compreensível e utilizada para tomar decisões, obter entendimento ou fornecer suporte a determinadas ações.

Em resumo, os dados são elementos brutos e objetivos, enquanto a informação é o resultado do processamento dos dados, transformando-os em significativos e úteis para as pessoas. São os componentes básicos a partir dos quais a informação é derivada, por meio da aplicação de contextos, análises e interpretações. A transformação dos dados em informação envolve a atribuição de significado, o estabelecimento de relações e a extração de *insights* para gerar conhecimento.

## História da Informação

Na Antiguidade, a informação era transmitida principalmente de modo oral, por meio de narrativas e histórias contadas de geração em geração. Com o surgimento da escrita, por volta de 3500 a.C., a informação pôde ser registrada e preservada de forma mais duradoura. As primeiras formas de escrita incluíam pictogramas e hieróglifos, usados pelos antigos egípcios, sumérios e outros povos.

A invenção do papel, na China, por volta do século II d.C., foi um marco importante na história da informação, o que permitiu a produção em massa de livros e documentos escritos. A imprensa, inventada por Johannes Gutenberg no século XV, revolucionou a disseminação da informação ao permitir a produção rápida e em grande escala de livros impressos. Isso desempenhou um papel

crucial no avanço da Renascença e disseminação do conhecimento científico durante o Iluminismo.

No século XIX, a telegrafia e o telégrafo foram introduzidos, o que possibilitou uma forma rápida de comunicação à distância. Esse desenvolvimento foi seguido pelo telefone, no final do século XIX, e rádio, no início do século XX, e isso ampliou ainda mais as oportunidades de comunicação em tempo real.

Entretanto, a verdadeira revolução na história da informação ocorreu com o advento dos computadores e da internet no século XX. A criação dos primeiros computadores eletrônicos, como o ENIAC, na década de 1940, permitiu o processamento rápido e automatizado de informações. A internet, desenvolvida na década de 1960, conecta computadores em rede e viabilizou a troca de informações em uma escala global.

Desde então, a tecnologia da informação tem avançado rapidamente, com o surgimento de dispositivos cada vez menores e mais poderosos, como smartphones e tablets. A digitalização de informações tornou possível o armazenamento e a transmissão de grandes quantidades de dados de maneira eficiente e acessível.

Atualmente, vivemos na chamada "era da informação", na qual o acesso à informação é amplamente disponível e a comunicação ocorre em tempo real em diferentes plataformas. A inteligência artificial, realidade virtual e computação em nuvem são apenas alguns exemplos das tecnologias que estão moldando o futuro da informação.

Em suma, a história da informação é uma jornada que **abrange milênios de desenvolvimento humano**, desde a comunicação oral até as tecnologias digitais modernas. Essa evolução tem desempenhado um papel principal na disseminação do conhecimento, avanço científico e transformação da sociedade como um todo.

## Pilares da Segurança da Informação

A segurança da informação é um conjunto de medidas e práticas adotadas para proteger os dados, informações e sistemas contra ameaças, e garantir a **confidencialidade, integridade e disponibilidade das informações**. Essa disciplina visa preservar a segurança dos ativos de informação, sejam físicos ou digitais, e envolve a implementação de políticas, procedimentos, tecnologias e treinamentos.

Existem algumas características fundamentais da segurança da informação que ajudam a moldar sua abordagem e estratégia:

- **Confidencialidade:** É a garantia de que as informações estejam **acessíveis apenas para pessoas autorizadas**. Isso envolve a proteção contra o acesso não autorizado, o uso indevido e a divulgação não autorizada de informações sensíveis. A **criptografia e autenticação** são mecanismos normalmente usados para garantir a confidencialidade dos dados.

- **Integridade:** Refere-se à proteção das informações contra alterações não autorizadas ou acidentais. O objetivo é **garantir que as informações permaneçam completas, precisas e consistentes ao longo do tempo**. Mecanismos de controle, **como assinaturas digitais e controle de versões**, são usados para verificar a integridade dos dados.

- **Disponibilidade:** Diz respeito à garantia de que as informações e **sistemas estejam acessíveis quando necessário**. Isso envolve proteger os sistemas contra interrupções, falhas técnicas,

desastres naturais e ataques maliciosos que possam afetar a disponibilidade dos serviços e dados. Estratégias de backup, redundância de sistemas e planos de recuperação de desastres são adotados para garantir a disponibilidade dos recursos de informação.

● **Autenticidade:** Remete à validade e origem das informações. É importante garantir que as informações sejam **provenientes de fontes confiáveis e que não tenham sido adulteradas**. Mecanismos como certificados digitais e assinaturas eletrônicas são usados para verificar a autenticidade das informações.

● **Não repúdio:** Tem o objetivo de evitar que uma pessoa negue a autoria de uma ação realizada. Isso é especialmente importante em transações eletrônicas, nas quais **é necessário ter provas irrefutáveis de que uma ação foi realizada por um determinado indivíduo**. Uma medida para evitar que uma pessoa negue a autoria de uma ação realizada é o uso de assinaturas digitais. As **assinaturas digitais** são métodos criptográficos que garantem a autenticidade e a integridade de um documento ou mensagem digital, proporcionando uma prova matemática de que o documento não foi alterado desde que foi assinado e que a assinatura pertence à pessoa que a criou.

Além dessas características, a segurança da informação também envolve a implementação de **controles e mecanismos de proteção, como firewalls, antivírus, detecção de intrusões, políticas de acesso e controle de privilégios**.

**OBS:** Uma tecnologia usada para detectar e responder a tentativas de intrusão em sistemas é a **detecção de intrusões**. Este é um conjunto de técnicas e tecnologias que monitoram atividades suspeitas ou maliciosas em redes e sistemas computacionais. Ela pode incluir a análise de logs, o uso de sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS) para identificar padrões de comportamento que possam indicar uma possível violação de segurança.

A conscientização e a educação dos usuários também desempenham um papel fundamental na segurança da informação. Todos os envolvidos no uso de informações devem estar cientes dos riscos, conhecer as melhores práticas de segurança e **adotar comportamentos seguros, como o uso de senhas fortes, a não divulgação de informações confidenciais e a atualização regular de software e sistemas**.

**OBS:** O **phishing é uma técnica maliciosa** utilizada por cibercriminosos para enganar os usuários e obter informações confidenciais, como senhas, números de cartões de crédito ou outras informações pessoais. A palavra "phishing" deriva de "fishing" (pesca, em inglês), indicando que os criminosos estão "pescando" informações valiosas dos usuários.

Aqui está uma explicação mais detalhada:

**1. Engenharia Social:** O phishing utiliza técnicas de engenharia social para manipular psicologicamente os usuários. Isso pode envolver criar e-mails, mensagens de texto, ou até mesmo páginas da web que se parecem legitimamente com comunicações de empresas conhecidas, bancos, redes sociais, etc.

**2. Isca:** Os criminosos geralmente oferecem uma isca tentadora, como um aviso falso de segurança, uma promoção imperdível, uma notificação de conta bloqueada, entre outros pretextos convincentes.

**3. Ação do Usuário:** Os usuários são induzidos a tomar uma ação rápida e impulsiva, como clicar em um link, baixar um arquivo anexado, preencher um formulário ou fornecer informações pessoais.

**4. Captura de Informações:** Ao clicar no link ou interagir com a página falsa, os usuários são levados a inserir suas informações confidenciais, que são então capturadas pelos criminosos.

**5. Consequências:** As consequências do phishing podem variar desde o roubo de identidade até fraudes financeiras graves, dependendo das informações obtidas e da capacidade dos criminosos de explorá-las.

Para se proteger contra o phishing, é essencial estar atento a sinais de alerta, como URLs suspeitos, erros gramaticais ou ortográficos em e-mails, solicitações inesperadas de informações pessoais, entre outros. Além disso, é recomendável usar autenticação de dois fatores sempre que possível e manter os softwares e sistemas atualizados para mitigar vulnerabilidades que os criminosos poderiam explorar.

**RESUMO:**

A Segurança da Informação estuda, defende e garante a proteção dos dados e informações, de modo a preservá-las e manter o valor que lhes foi imposto. Cyber Security, ou Segurança Cibernética, tratará desta mesma defesa, porém exclusivamente em meios digitais, ou seja, protegerá as informações e dados armazenados em sistemas, estudando maneiras de prevenção de interrupções de serviços informáticos, ataques hackers, entre outros. A S.I. é baseada em pilares, que são a confidencialidade, integridade, disponibilidade, autenticidade, legalidade e determinam a organização e padronização do ambiente organizacional.

**ATIVIDADES:**

**1.** O que é confidencialidade na segurança da informação?
a) A proteção contra alterações não autorizadas de dados.
b) A garantia de que as informações estejam acessíveis apenas para pessoas autorizadas.
c) A validação da origem das informações.
d) A proteção contra interrupções e falhas técnicas.

**2.** O que é um firewall e qual é sua função na segurança da informação?
**3.** Qual a diferença entre dados e informação?
**4.** Descreva as principais etapas envolvidas na implementação de um programa abrangente de segurança da informação em uma organização.
**5.** Explique o que é criptografia e como ela é utilizada para proteger as informações na comunicação eletrônica.

## Atividade em grupo:

Pesquise na internet, ou outra mídia que preferir, uma notícia que envolva um crime cibernético recente no Brasil. Aponte as características deste ataque e qual ou quais pilares da Segurança da Informação foram afetados.