# Gestão de Tecnologia da Informação

## Segurança da Informação

**Profa. Ms. Fabiana A. Rodrigues**

EDUCAÇÃO METODISTA

# SEGURANÇA DA INFORMAÇÃO
# AULA 01

EDUCAÇÃO METODISTA

# EMENTA

Principais conceitos e objetivos de segurança da informação. Padrões de segurança da informação. Principais riscos em sistemas de informação. Tipos de ameaças e vulnerabilidades dos sistemas de informação. Aspectos especiais: Vírus, fraudes, criptografia e acesso não autorizados. Políticas de segurança em ambientes computacionais. Implantação de medidas de segurança.

# OBJETIVO GERAL

- ✔ Permitir ao aluno compreender os conceitos gerais de Segurança da Informação e os demais conceitos relacionados as estratégias para a proteção do conhecimento Organizacional.
- ✔ Permitir ao aluno compreender os princípios de Segurança da Informação que quando utilizado adequadamente, ajudam as organizações obterem melhores resultados.
- ✔ Conhecer os principais conceitos de Segurança da Informação.
- ✔ Conhecer Políticas de Segurança da Informação adequadas para o negócio.
- ✔ Planejar estratégias e identificar ferramentas que protejam os principais objetivos de segurança da Informação.

EDUCAÇÃO METODISTA

# OBJETIVOS ESPECÍFICOS

- ✔ Conceitos básicos que fundamentam os estudos sobre Segurança da Informação.
- ✔ Diferentes categorias de ativos existentes em uma empresa.
- ✔ Conceito de vulnerabilidade e ameaças dos ativos;
- ✔ Conceitos de integridade, confidencialidade e disponibilidade;
- ✔ Conceitos de análise de riscos;
- ✔ Conceitos de política de segurança da informação;
- ✔ Medidas de segurança;
- ✔ Normas de segurança da informação.

EDUCAÇÃO METODISTA

- **Dia da aula:** segunda-feira
- **Horário:** 19h30 às 21h10

## AVALIAÇÃO

| | Data | % |
|---|---|---|
| » Prova 1 | 25/09 a 29/09 | 35% |
| » Prova 2 | 27/11 a 01/12 | 35% |
| » Atividades | Durante a disciplina | 30% |
| Avaliação Substitutiva | de 04 a 08/12 | |
| Avaliação Suplementar | de 11 a 15/12 | |

# AVALIAÇÃO SUBSTITUTIVA

**Avaliação Substitutiva -** Substituirá a P1 ou P2, e deverá contemplar o conteúdo de todo o semestre, de forma temática/modular.

# AVALIAÇÃO SUPLEMENTAR

**Avaliação Suplementar - 100%**

Para quem: alunos com frequência mínima de 75% e nota menor que 6 e maior ou igual a 4.

# AULA 01

# Introdução e Conceitos Básicos de Segurança da Informação

EDUCAÇÃO METODISTA

# Introdução

- A segurança da informação é fundamental para empresas com informações valiosas e diferenciais competitivos.
- Seu papel é garantir confidencialidade, integridade e disponibilidade dos ativos de informação.
- As vulnerabilidades e ameaças devem ser conhecidas para proteger-se de ataques.

# INTRODUÇÃO

- Atualmente, as informações constituem o objeto de maior valor para as empresas. Por esse e outros motivos a segurança da informação é um assunto tão importante para todos, visto que afeta diretamente todos os negócios de uma empresa ou de um indivíduo.
- **Importância da Informação para o Negócio –** a informação é um elemento essencial para a geração do conhecimento, para a tomada de decisões, e que representa efetivamente valor para o negócio.

# INTRODUÇÃO

★ **Importância da Segurança da Informação**

- O armazenamento de informações evoluiu desde registros pré-históricos até os dias atuais.
- Informações tornaram-se valiosas para empresas, possibilitando estratégias personalizadas.
- A segurança da informação protege ativos em diversas formas de representação e armazenamento.

# INTRODUÇÃO

A internet possibilitou que pessoas e empresas cruzassem fronteiras de maneira fácil e rápida.

Os sistemas informatizados estão sendo amplamente utilizados para a realização das mais diversas atividades.

- O correio eletrônico tornou-se ferramenta indispensável às empresas e as pessoas
- Não apenas para comunicação, mas também para o marketing pessoal e comercial.

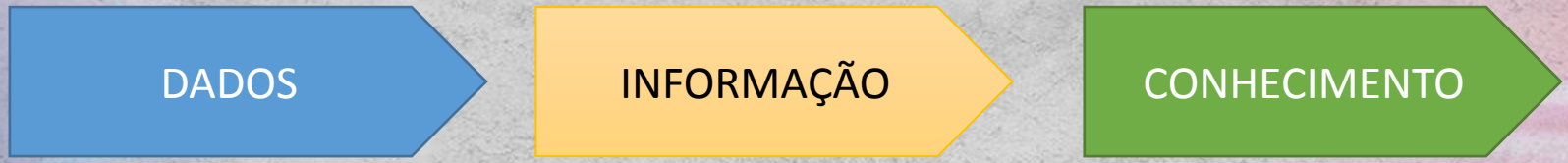
# Segurança da informação no contexto organizacional

- O armazenamento de informações surgiu da necessidade de registrar hábitos, costumes e intenções nos mais diversos meios, de forma que esses registros possam ser utilizados e compreendidos futuramente pelo autor da informação e por outras pessoas.

- No contexto organizacional, a informação pode estar relacionada, por exemplo, com os dados armazenados em software e o uso eficiente destes. Segundo Correa Junior (2011), estratégias de extração de dados podem ser utilizadas, por exemplo, para identificar um perfil de consumidor e, com isso, personalizar o negócio de uma empresa, estabelecendo um diferencial competitivo em relação à concorrência.

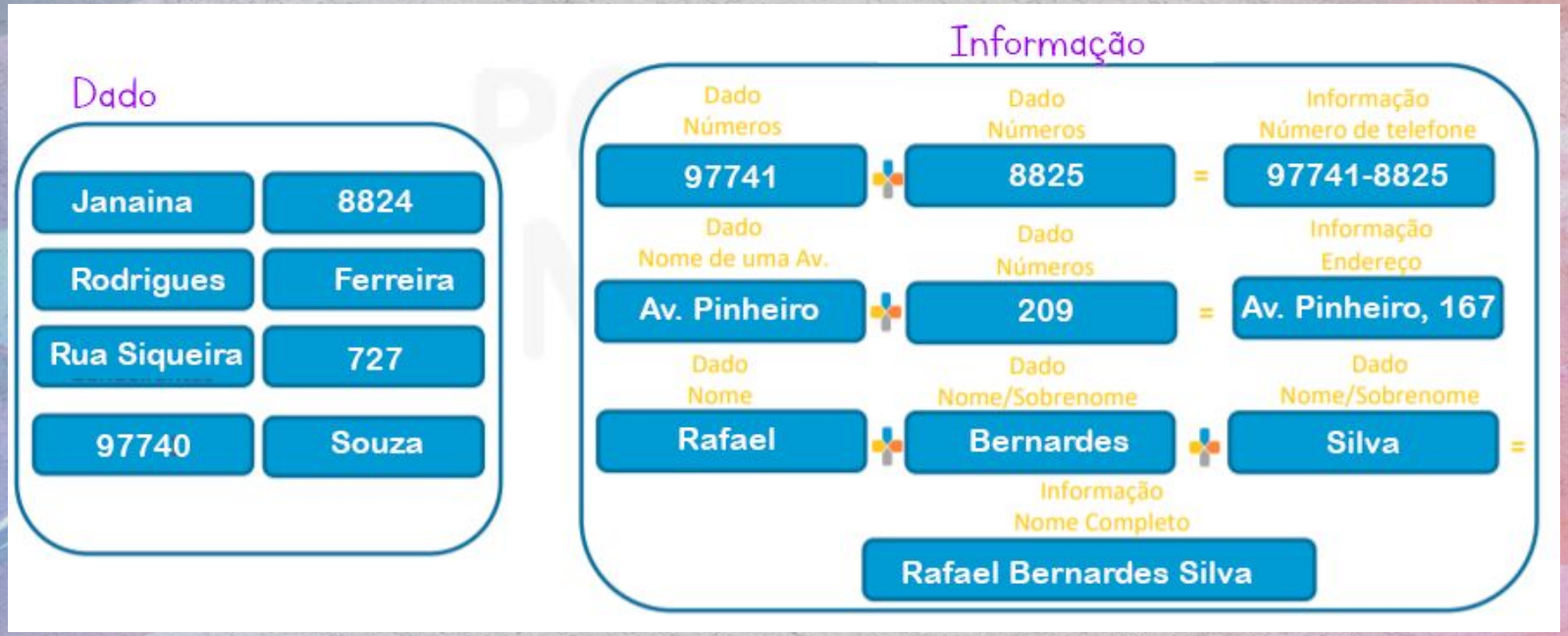
# Segurança da informação no contexto organizacional

- ★ O **conhecimento** e a **informação** são pontos-chave nas organizações, sendo necessário atentar para mecanismos que garantam a sua segurança.
- ★ A segurança da informação tem como propósito proteger os ativos de informação.
- ★ De acordo com Correa Junior (2011), um ativo de informação é qualquer objeto que retém partes da informação da empresa, nas suas mais diversas formas de representação e armazenamento: impressas em papel, armazenadas em discos rígidos de computadores, armazenadas na nuvem ou, até mesmo, retidas em pessoas.




- ★ A informação é algo que contém um significado e causa impacto em diferentes graus, tornando-a o elemento chave da extração e criação do conhecimento.
- ★ O conhecimento só poderá ser formado quando o indivíduo for exposto à informação, deste modo é possível afirmar que poderá até haver informação sem conhecimento, mas não conhecimento sem informação.

# INFORMAÇÃO, DADO E CONHECIMENTO



# O QUE É DADO?


✔Os dados são uma **coleção de fatos**, como números, palavras, medidas, observações ou apenas descrições de coisas.

EDUCAÇÃO METODISTA

# O que é INFORMAÇÃO?


✔Informação é o resultado do processamento, tratamento e organização de dados, de tal maneira que represente uma modificação no conhecimento do sistema (humano ou máquina) que a recebe.

EDUCAÇÃO METODISTA

# O QUE É INFORMAÇÃO?

✔Informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo.

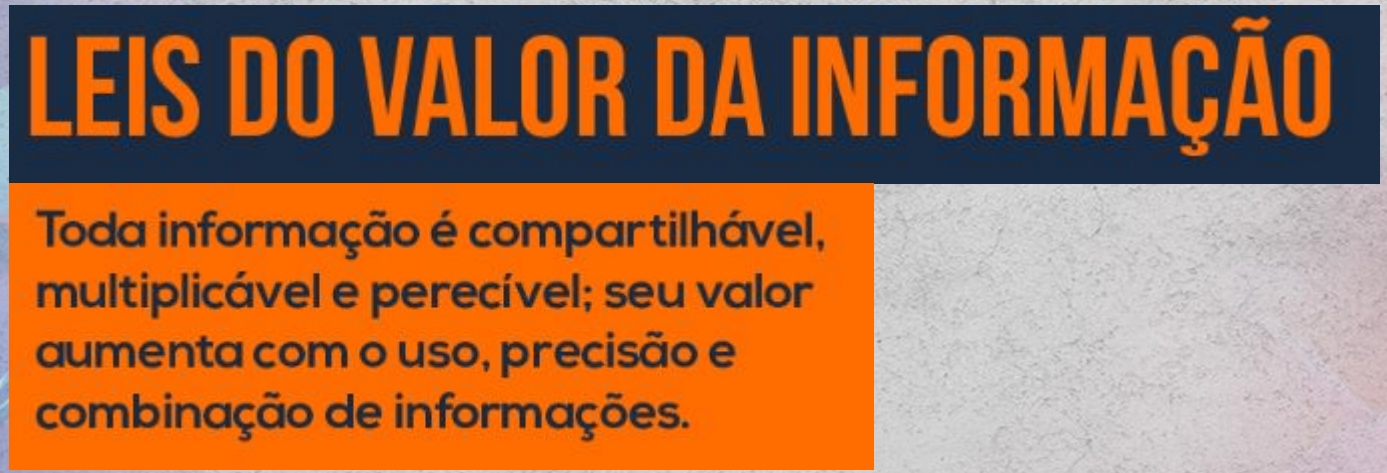
✔Trata-se de tudo aquilo que possibilita a aquisição do conhecimento

✔ A informação digital é um dos principais, senão o mais importante, produto da era atual. Ela pode ser manipulada e visualizada de diversas maneiras.

✔ Com a integração destes sistemas e de suas bases de dados por meio de redes, é um fato determinante da sociedade da informação.

# Segurança da informação no contexto organizacional

O valor da segurança da informação para as organizações é regido por sete leis, as quais destacam a sua importância.



# Segurança da informação no contexto organizacional

## CLASSIFICAÇÃO DA INFORMAÇÃO

Uma informação é classificada sempre em: pública, interna, confidencial e secreta.

# Segurança da informação no contexto organizacional

## CICLO DE VIDA DA INFORMAÇÃO

- Armazenamento
- Manuseio
- Transporte
- Descarte

EDUCAÇÃO METODISTA

# Segurança da informação no contexto organizacional

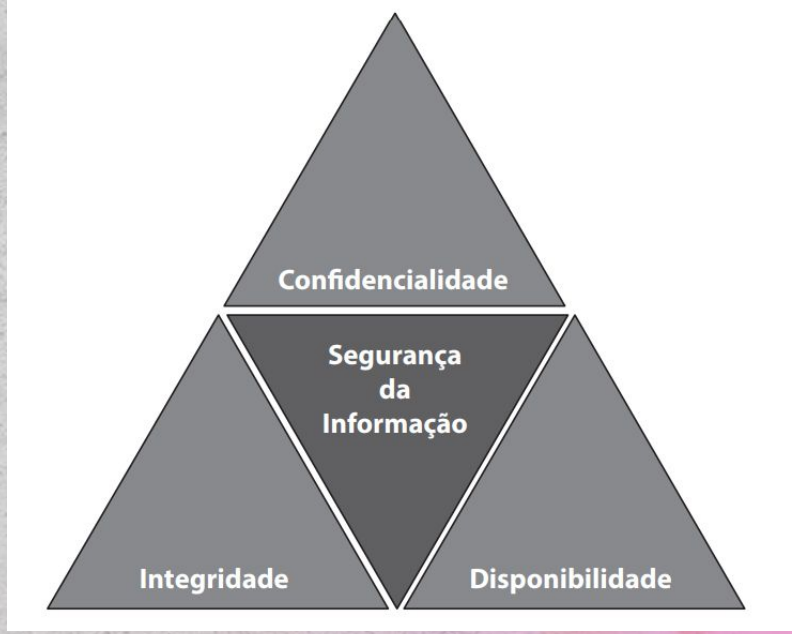
**Pilares da Segurança da Informação**

A segurança da informação compreende um conjunto de medidas que visam proteger e preservar as informações de um sistema.

# Segurança da informação no contexto organizacional

## Pilares da Segurança da Informação:

- **Confidencialidade (confidentiality):** capacidade de um sistema de impedir que usuários não autorizados “vejam” determinada informação que foi delegada somente a usuários autorizados a vê-la.
- **Integridade (integrity):** atributo de segurança que garante que a informação seja alterada somente de forma autorizada, sendo mantida, assim, correta e completa.
- **Disponibilidade (availability):** indica a quantidade de vezes que o sistema cumpriu uma tarefa solicitada sem falhas internas, para um número de vezes em que foi solicitado a fazer a tarefa.




EDUCAÇÃO METODISTA

# Por que se preocupar com a segurança da informação?

Existem diversos motivos para que as empresas se atentem à segurança de suas informações. Por exemplo:

**1. Roubo de dados e informações:** para muitas empresas, o seu maior capital é a regra de negócios da empresa, isto é, o conhecimento retido por ela quanto ao “fazer negócio”.

**2. Impacto na operacionalização da empresa:** muitas empresas dependem de seus sistemas computadorizados para o seu funcionamento. Imagine que uma invasão nos servidores de uma empresa tire seus sistemas do ar e faça com que a empresa pare de trabalhar por 24 horas.

**3. Sequestro de dados:** nos casos em que os dados dos servidores de uma empresa são vitais para o seu funcionamento, é preocupante o risco de sequestro de dados, em que um invasor captura as informações da base de dados da empresa e cobra valores significativamente altos pelo seu resgate.

# Por que se preocupar com a segurança da informação?

**4. Vazamento de dados confidenciais de clientes:** quando uma empresa armazena dados pessoais de clientes, por exemplo, documentação e dados financeiros, ela assume com o cliente um compromisso de responsabilidade com esses dados. Deixar o sistema vulnerável viola esse compromisso de responsabilidade, uma vez que os dados podem ser capturados direto do servidor se houver uma falha de segurança.

**5. Danos à imagem da empresa:** todos os problemas citados acima causam uma quebra de confiança entre a empresa e seus clientes, o que pode causar perda de clientes e graves danos financeiros para a empresa.

# SEGURANÇA DA INFORMAÇÃO
# AULA 02

EDUCAÇÃO METODISTA

# Ativos de uma empresa

Utiliza-se a palavra **ativos** para denominar tudo aquilo que possui valor para uma empresa e, por isso, precisa ser protegido (ABNT, 2005).

✔**Ativo** - a ISSO/IEC 13335-1/2004 caracteriza a informação como ativo qualquer coisa que tenha valor para a organização.

- Classificação de ativos:
  - Informações = equipamentos e sistemas / pessoas
  - Software / Hardware / Organização

# Ativos de uma empresa

Os ativos de informação podem ser divididos nas seguintes categorias:

- **Informações:** toda e qualquer informação que a empresa possui, digitalizada ou não.
- **Software:** esse grupo de ativos contém todos os programas de computador utilizados nos processos de acesso, leitura, transmissão e armazenamento das informações de uma empresa.
- **Hardware:** todos os elementos físicos que apresentam valor importante para uma empresa no que diz respeito à informação; por exemplo, computadores e servidores.
- **Organização:** nesse grupo, estão incluídos os aspectos que compõem a estrutura física e organizacional das empresas.
- **Usuários:** engloba os indivíduos que lidam com as informações no seu dia a dia de trabalho.

# Ativos de uma empresa

Exemplo: **Empresa de Tecnologia de Pagamentos Online**

Nesse caso, os ativos da empresa relacionados à Segurança da Informação incluiriam:

- ★ **Servidores e Infraestrutura de TI**
- ★ **Banco de Dados de Clientes**
- ★ **Criptografia e Chaves de Acesso**
- ★ **Firewalls e Sistemas de Detecção de Intrusão**
- ★ **Sistemas de Autenticação Multifator (MFA)**
- ★ **Políticas de Acesso e Controle de Privacidade**
- ★ **Monitoramento de Atividades Suspeitas**
- ★ **Plano de Resposta a Incidentes**
- ★ **Treinamento de Conscientização em Segurança**
- ★ **Backup e Recuperação de Dados**

# Ativos de uma empresa

Pensando em uma empresa de varejo, quais seriam os ativos mais importantes no que se refere à segurança da informação?

# Segurança da Informação

- Segundo a Associação Brasileira de Normas Técnicas: “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

- **A Segurança da Informação deve:**

# Segurança da Informação

## Prevenir

**Prevenir** se refere à adoção de medidas proativas para evitar que ameaças ou ataques ocorram. Isso envolve a implementação de controles de segurança, políticas e práticas que reduzem as vulnerabilidades e os riscos. A ideia é evitar que ameaças externas ou internas explorem pontos fracos nos sistemas, redes e processos da organização.

# Segurança da Informação

## Detectar

**Detectar** envolve o monitoramento constante de sistemas e redes para identificar atividades incomuns, suspeitas ou anormais que possam indicar um possível ataque. Isso pode incluir o uso de sistemas de detecção de intrusão, análise de logs de atividade e outras ferramentas que alertam os administradores sobre atividades potencialmente maliciosas.

# Segurança da Informação

## Deter

**Deter** refere-se a medidas que desaceleram ou impedem um ataque em andamento. Isso pode incluir a implementação de barreiras de segurança, como firewalls, sistemas de autenticação multifator (MFA) e controles de acesso rigorosos. O objetivo é dificultar o progresso dos atacantes e reduzir o impacto de um ataque em potencial.

# Segurança da Informação

## Documentar

**Documentar** envolve a criação de registros detalhados de atividades de segurança, incidentes, procedimentos e políticas. Isso é importante para análise posterior de eventos, investigações de incidentes, cumprimento de regulamentos e também para garantir a transparência e a comunicação eficaz dentro da organização.

# Segurança da Informação

A segurança da informação pode ser adquirida por meio da implantação de um conjunto apropriado de controles, que pode incluir:

- ✔ Políticas,
- ✔ Procedimentos,
- ✔ Estrutura organizacional,
- ✔ Funções de *hardware* e *software*.

# PROFISSÕES NA ÁREA DA SEGURANÇA DA INFORMAÇÃO

Gerente de segurança

Administrador de segurança

Consultor de segurança

Analista de segurança

Engenheiro de segurança ou arquiteto de segurança

DPO

https://seginfo.com.br/2019/04/12/dicas-de-como-iniciar-na-carreira-de-seguranca-da-informacao/

EDUCAÇÃO METODISTA

# FUNÇÕES DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

- Fazer cumprir a política de segurança da informação da empresa;
- Identificar e determinar o plano estratégico da segurança das informações;
- Definir regras e normas de conduta que protejam as informações;
- Analisar e identificar locais que coloquem em risco as informações;

# FUNÇÕES DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

- Monitorar os processos de segurança das informações em todas as áreas da organização;
- Implementar uma política de segurança global, com normas e diretrizes, para garantir a segurança das informações;
- Acompanhar todas as implantações de arquitetura e sistema da empresa para verificar se as regras pré-estabelecidas de segurança está sendo seguidas;

# FUNÇÕES DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

- Solicitar treinamentos em segurança da informação, quando necessário;
- Informar aos responsáveis de outras áreas a necessidade de novas normas de segurança da informação;
- Acompanhar os riscos, novos ou conhecidos, de origem interna ou externa;
- Observar todo o processo de auditoria de segurança realizada por organizações externas.

# Privacidade: escândalos de violação e vazamentos

## ✔Caso: Ashley Madison

- O caso Ashley Madison refere-se a um vazamento de dados que ocorreu em 2015, onde um grupo de hackers conhecido como "The Impact Team" roubou informações pessoais da base de usuários do Ashley Madison, um site que facilitava casos extraconjugais

- Os hackers ameaçaram divulgar os nomes e informações pessoais dos usuários se o Ashley Madison não fosse desativado.

- Eventualmente, o grupo vazou mais de 60 gigabytes de dados da empresa, incluindo detalhes dos usuários.

# Privacidade: escândalos de violação e vazamentos

✔ Caso: Facebook – Cambridge Analytica

- Vazamento de dados: A Cambridge Analytica, uma empresa de análise de dados, obteve informações pessoais de até 87 milhões de perfis do Facebook sem o consentimento dos usuários.

- Uso indevido de dados: A Cambridge Analytica usou esses dados para fornecer assistência analítica à campanha presidencial de 2016 nos Estados Unidos. A empresa também enfrentou investigações sobre seu possível papel no referendo do Brexit.

Segurança da Informação em: Brasil
2.654 resultados

Configurar alerta

**Consultor(a) Sênior em Segurança da Informação | Cloud Security | São Paulo**
Deloitte
São Paulo, São Paulo, Brasil (Presencial)
1 conexão trabalha aqui
Promovida

**Especialista de Tecnologia - Segurança da Informação (Sênior)**
Solutis Tecnologias
Salvador, Bahia, Brasil (Híbrido)
Recrutando agora
Promovida

**Coordenador de TI / Segurança da Informação**
Dataprom Equipamentos e Serviços de Informática
Curitiba, Paraná, Brasil (Presencial)
Recrutando agora
Promovida · Candidatura simplificada

**Analista de Segurança da Informação - Nível Pleno**
Microhard
Belo Horizonte, Minas Gerais, Brasil (Híbrido)
Recrutando agora
Promovida · Candidatura simplificada

**Analista de Segurança da Informação - Gestão de Vulnerabilidades & Governança AppSec - Vaga afirmativa para mulheres**
Ambev Tech

# OPORTUNIDADES DE TRABALHO

**Consultor(a) de Segurança da Informação - OT**
Accenture Brasil
São Paulo, São Paulo, Brasil (Híbrido)
Recrutando agora
Promovida

**Analista de Segurança em GRC Sr.**
UOL - Universo Online
São Paulo e Região (Presencial)
2 conexões trabalham aqui
Promovida

**Analista de Segurança da Informação Pleno**
Teletex IT Solutions
Blumenau, Santa Catarina, Brasil (Híbrido)
Promovida · 16 candidaturas

**Arquiteto de Segurança da Informação**
Aegea Saneamento
Canoas, Rio Grande do Sul, Brasil (Presencial)
Recrutando agora
Promovida

**Analista de Segurança da Informação**
Wipro
Fortaleza, Ceará, Brasil (Presencial)
Recrutando agora
Promovida · Candidatura simplificada

# OPORTUNIDADE DE TRABALHO

## Consultor Sênior – Privacidade de Dados

EY · São Paulo, São Paulo, Brasil

Anunciada há 2 meses · 124 visualizações

Candidatar-se | Salvar

**O que procuramos**

Um consultor com perfil de engenharia de privacidade de dados para se juntar à nossa equipe de Cybersecurity com foco em Data Protection and Privacy. Nesta função, você trabalhará para ajudar a implementar controles técnicos acerca do ecossistema de dados e conduzir assessments em projetos de diagnóstico ou implementação de soluções de privacidade em projetos de Implementação ou Operação, centradas em data discovery, orquestração, anonimização, DLP, CASB, com foco em data discovery. Você contribuirá diretamente para o sucesso de nossa estratégia de dados, trabalhando multidisciplinarmente com dados, jurídico e predominantemente Cybersecurity proteção de dados, governança, gestão de riscos e leis de privacidade, como exemplos LGPD, GDPR, CCPA, etc

**Responsabilidades**

- Levantar requisitos de projeto, escopo, interdependências, estimativas de esforço, tempo de duração e entregáveis de projeto.
- Desenvolver planos de projeto, planos de comunicação, status report, cronograma, reuniões e apoiar a gestão no controle financeiro dos projetos .
- Revisar as atividades dos membros da equipe de projeto.
- Responsabilizar-se pela qualidade técnica dos entregáveis de projetos e apoiar o desenvolvimento das pessoas do time e de outros membros, designados através da estrutura de gestão de pessoas, conhecido como Aconselhados.
- Elaborar especificações de arquitetura de segurança da informação, configurações de ambiente, documentação de processos, relatórios de diagnóstico e recomendação de conformidade de segurança da informação, proteção e privacidade de dados.
- Suportar a construção e/ou operação de processos de alta qualidade para controles regulatórios e de conformidade contínuos com leis ( LGPD, GDPR, CCPA e etc), bem como, com regulamentações adjacentes (PCI DSS, ISSO IEC 27701).
- Suportar a construção e/ou operação de programas de privacidade e proteção de dados por meio de controles automatizados, suporte à auditorias, suporte à certificações e programas de conformidade regulatória
- Implementar/configurar e/ou ter a vocação para a pesquisa de soluções em especial, no momento atual, para data discovery.

**Resquisitos da posição**

- Graduação em ciências exatas (engenharia, computação, sistemas) onde o pensamento lógico é desenvolvido na medida dos desafios que os projetos de cybersecurity exigem.
- Conhecimento no desenvolvimento e implementando controles de segurança como políticas, processos e tecnologias de proteção e privacidade de dados.
- Atuação em projetos baseados na ISO27001/ISO27701 e projetos que adotem frameworks de gestão de riscos de segurança da informação como o NIST e PCI DSS.
- Inglês intermediário para comunicações verbais e escritas com equipes EY, parceiros e clientes internacionais.
- Atuação em projetos de Data loss Prevention e Security Analytics Data Discovery.
- Vivência em projetos de adequação à LGPD/GDPR e similares e ferramentas de orquestração de privacidade.

**Desejável**

- Certificação profissional em domínios de privacidade e proteção de dados tais como as oferecidas pela IAPP (CIPM, CIPP), EXIN (DPO), ISACA (CDPSE), ISO27701 ou equivalentes.

**Setor**
Contabilidade , Serviços financeiros

**Tipo de emprego**
Tempo integral

**Funções de trabalho**
Recursos humanos

# AULA 03
# Vulnerabilidade e ameaças a ativos

EDUCAÇÃO METODISTA

# CURIOSIDADES E SUGESTÕES

**7 dicas para navegar com segurança na internet**

Disponível em: https://www.boavontade.com/pt/tecnologia/7-dicas-para-navegar-com-seguranca-na-internet

**GDPR Enforcement Tracker**

Disponível em: https://www.enforcementtracker.com/

**';--have i been pwned?**

Disponível em: https://haveibeenpwned.com/

EDUCAÇÃO METODISTA

# CURIOSIDADES E SUGESTÕES

**Cartilha de Segurança para Internet**

Disponível em:
https://nic.br/media/docs/publicacoes/13/fasciculo-internet-banking.pdf

**10 PASSOS PARA GARANTIR A SEGURANÇA DA CLOUD**

http://digital.br.synnex.com/pt/10-passos-para-garantir-a-seguranca-da-cloud

**TOP 10 MELHORES PRÁTICAS DE SEGURANÇA EM BIG DATA**

http://digital.br.synnex.com/pt/top-10-melhores-praticas-de-seguranca-em-big-data

# Vulnerabilidade e ameaças a ativos

O termo **vulnerabilidade** diz respeito à condição que torna um ativo um alvo mais predisposto a sofrer ameaças e invasões. Fazendo uma analogia, ao deixar a porta de sua casa aberta, você está deixando sua casa vulnerável a furtos e roubos. Isso não quer dizer que, obrigatoriamente, quando a porta estiver aberta, os ativos de sua casa serão furtados; contudo, indica que, com a porta aberta, o roubo ou furto é facilitado. O mesmo acontece em empresas com relação aos ativos de informação: ao não tomar os devidos cuidados com *hardware* ou *software*, os sistemas se tornam mais vulneráveis a ataques.

O termo **Ameaças** podem ser naturais, involuntárias ou intencionais. Causa potencial de um incidente indesejado, a qual pode resultar no  dano a um sistema ou organização.

# Vulnerabilidade

Alguns exemplos de vulnerabilidades são listados a seguir, com base em Dantas (2011):

**Área física e do ambiente:** diz respeito à vulnerabilidade na estrutura física da empresa; por exemplo, portas ou janelas desprotegidas, instabilidade da energia, localização em área susceptível à inundação.

**Hardware:** susceptibilidade a problemas que podem danificar os equipamentos; por exemplo, variação de voltagem, de temperatura, poeira, umidade, radiação eletromagnética, falta de controle de mudança de configuração.

# Vulnerabilidade

**Software:** diz respeito às falhas em um software que facilitam a invasão ou a danificação do software e dos dados; por exemplo, falta de mecanismo de identificação e autenticação, tabelas de senhas desprotegidas, alocação errada de direitos de acesso, falta de documentação, falta de backup.

**Comunicações:** linhas de comunicações desprotegidas, falta de identificação e autenticação de emissor e receptor, gestão inadequada da network, conexões de rede pública desprotegidas.

**Documentação:** arquivo desprotegido, falta de controle para cópias, falta de cuidado na disponibilização da documentação.

# Vulnerabilidade

**Pessoal:** falta de pessoal, treinamento de segurança insuficiente, ausência de conhecimento de segurança, utilização incorreta de software e hardware, falta de mecanismo de monitoramento, ausência de políticas para a utilização correta de mídia e de mensagens, procedimento inadequado para seleção.

# Ameaças a ativos

Ameaças podem ser **naturais**, **involuntárias** ou **intencionais**, conforme leciona Dantas (2011).

- Uma **ameaça natural** é aquela que se origina de fenômenos da natureza, como terremotos, furacões, enchentes, maremotos, tsunamis, *etc*.

- Uma **ameaça involuntária** é aquela que resulta de ações não intencionais, mas que causam algum dano; geralmente são causadas por acidentes, erros, ou pela ação inconsciente de usuários, como é o caso de vírus eletrônicos que são ativados pela execução de arquivos anexados às mensagens de e-mail.

- Já uma **ameaça intencional** é aquela que tem por objetivo causar danos, como ataques de hackers, fraudes, vandalismos, sabotagens, espionagem, invasão e furtos de informações, dentre outras.

# Ameaças a ativos

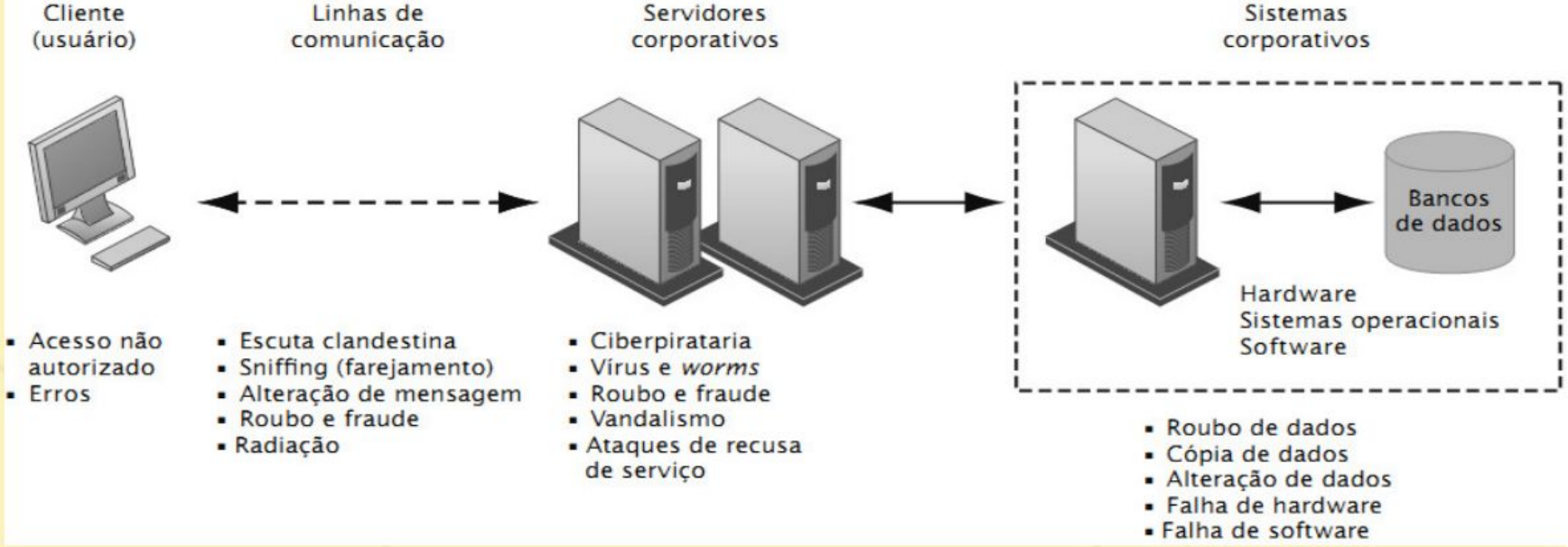
Dantas (2011) aponta as principais ameaças a ativos apresentadas em pesquisas sobre segurança da informação:

- vírus, worm, cavalo de tróia (trojan horse);
- phishing, pharming e spyware;
- adware, spam;
- roubo de dados confidenciais da empresa e de clientes, da propriedade da informação e da propriedade intelectual;
- acesso não autorizado à informação;

# Ameaças a ativos

- perda de dados de clientes;
- roubo de laptop, dispositivo portátil e hardware;
- má conduta e acesso indevido à network por funcionários e gerentes, bem como abuso de seus privilégios de acesso e utilização indevida da rede wireless;

# Vulnerabilidades e desafios de segurança contemporâneos




Normalmente, a arquitetura de uma aplicação baseada na Web inclui um cliente, um servidor e sistemas de informação corporativos conectados a bancos de dados. Cada um desses componentes apresenta vulnerabilidades e desafios de segurança. Enchentes, incêndios, quedas de energia e outros problemas técnicos podem causar interrupções em qualquer ponto da rede.

# Vulnerabilidade dos sistemas e uso indevido

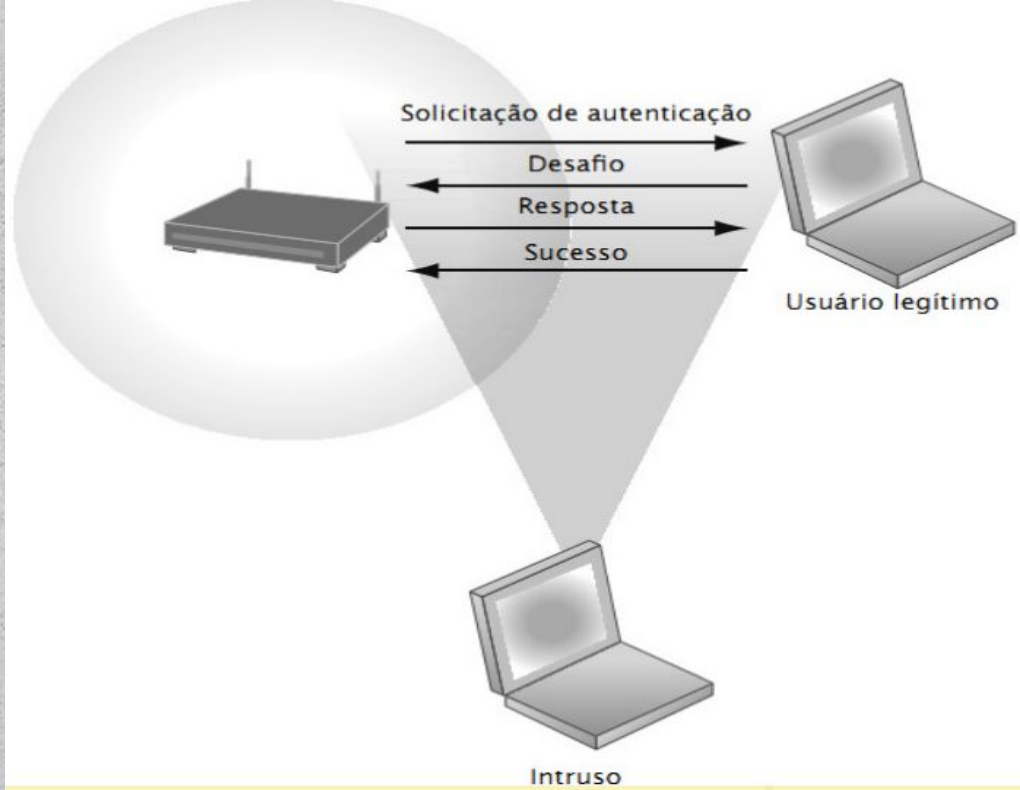
Vulnerabilidades da Internet

- Rede aberta a qualquer usuário
- O tamanho da Internet propicia que os abusos tenham um alto impacto
- Uso de endereços de Internet fixos com conexões permanentes à rede mundial facilita a identificação por hackers
- Anexos de e-mail
- E-mails usados para transmissão de segredos de negócios
- Mensagens instantâneas não são seguras e podem ser facilmente interceptadas

# Vulnerabilidade dos sistemas e uso indevido

Desafios de segurança em ambientes Wi-Fi

- Muitas redes Wi-Fi podem ser facilmente invadidas por intrusos. Eles usam programas sniffers para obter um endereço e, assim, acessar sem autorização os recursos da rede.



# Ferramentas para testar vulnerabilidade e ameaças

- **Greenbone** - O scanner de vulnerabilidades OpenVAS é a ferramenta de análise de vulnerabilidades que permite aos departamentos de TI verificar os servidores e dispositivos de rede, graças à sua natureza abrangente.

- **Tripwire IP360** - é uma das principais soluções de gerenciamento de vulnerabilidades do mercado, permitindo que os usuários identifiquem tudo em sua rede, incluindo ativos locais, na nuvem e em contêineres.

- **Nessus Vulnerability Scanner** - O Nessus Professional da Tenable é uma ferramenta para profissionais de segurança, cuidando de correções, problemas de software, remoção de malware, adware e configurações incorretas em uma ampla variedade de sistemas operacionais e aplicativos.

- **Software de Gestão de Vulnerabilidades grátis**

*Link*: https://www.capterra.com.br/directory/31062/vulnerability-management/pricing/free/software

# ATIVIDADE 1

A segurança da informação tem como base os seguintes aspectos, denominados pilares da segurança da informação: confidencialidade, integridade e disponibilidade dos dados; contudo, para que isso seja possível, é necessário se atentar às vulnerabilidades e às ameaças que surgem para os sistemas.

Você foi contratado por uma grande empresa prestadora de serviços em tecnologia da informação para garantir a segurança dos seus dados e informações. Pedro, o contratante, precisa se preocupar com as principais categorias de vulnerabilidades e ameaças, de modo a evitar que qualquer problema impacte no trabalho da empresa.

Analisando esse cenário, descreva as medidas que Pedro deve tomar para prevenir a vulnerabilidade:

**- Física** **- de hardware** **- de software**

**- de comunicação** **- de documentação** **- de pessoal**

EDUCAÇÃO METODISTA

# Como identificar um ataque

# Como identificar um ataque

***Principais formas de ataque***

- Ataques internos
- Vírus de computador

# Como identificar um ataque

## *Principais formas de ataque*

**Ataques internos**

- **Entradas Clandestinas:** Introdução deliberada de vulnerabilidades em softwares para explorar bugs de implementação.
- **Easter Eggs:** Características escondidas que podem ser usadas para explorar vulnerabilidades.
- **Bombas Lógicas:** Programas que executam ações maliciosas com base em condições do sistema.

# Como identificar um ataque

## *Principais formas de ataque*

**Vírus de computador**

- **Vírus de Macro e Boot Sector:** Infecções que afetam documentos e setores de inicialização.
- **Vírus Mutantes e Encriptados:** Variações do vírus que dificultam a detecção.

# Como identificar um ataque

## *Principais formas de ataque*

**Outros Tipos de Malware:**

- **Ransomware:** Criptografa dados e exige resgate para desbloqueio.
- **Cavalo de Troia:** Finge ser software legítimo e permite a entrada de outros malwares.
- **Spyware e Adware:** Espionam usuários ou exibem anúncios indesejados.
- **Rootkit:** Modifica utilitários do sistema para esconder ações maliciosas.

# Como identificar um ataque

**Invasões em Dispositivos IoT e Vulnerabilidades do BYOD:**

- Vulnerabilidades em dispositivos IoT podem ser exploradas por hackers.
- A incorporação do Bring Your Own Device (BYOD) pode aumentar as ameaças internas.

"Bring Your Own Device" (BYOD) é um termo usado para descrever a prática em que os funcionários de uma organização utilizam seus próprios dispositivos pessoais, como smartphones, tablets e laptops, para acessar e realizar atividades relacionadas ao trabalho.

# Como identificar um ataque

***Técnicas de invasão voltadas para equipamentos da Internet das Coisas***

Para garantir a segurança, é necessário conhecer as técnicas de invasão e os métodos de monitoramento.

Podemos utilizar sistemas de monitoramento para identificar vulnerabilidades, analisar logs e detectar possíveis falhas.

Ferramentas como firewalls e segurança endpoint são cruciais para proteger os nós de uma rede corporativa.

# Como identificar um ataque

"Ferramentas como firewalls e segurança endpoint" são componentes essenciais para fortalecer a segurança cibernética de sistemas, redes e dispositivos. Eles desempenham papéis fundamentais na proteção contra ameaças cibernéticas e na mitigação de riscos de segurança.

# Como identificar um ataque

***Formas de monitoramento de ataques***

- Monitorar ataques é crucial para prevenir invasões. Ferramentas como Cacti, Nagios e Zabbix permitem a análise constante da infraestrutura e a detecção de anomalias. Além disso, estratégias como a definição de políticas de acesso, inventário de dispositivos e inspeção de códigos contribuem para fortalecer a segurança.

# Como identificar um ataque

***Ataques autenticados e não autenticados***

- Entender a diferença entre ataques autenticados e não autenticados é essencial. Enquanto os ataques não autenticados exploram vulnerabilidades em contas de usuário comuns, os ataques autenticados buscam obter acesso a contas de administradores para comprometer sistemas inteiros. Diferentes métodos de autenticação, como conhecimento, tokens e biometria, podem ser usados para fortalecer a segurança.

# Atividade 2

- Você é um funcionário da empresa “Messias Atacadista” e, ao tentar acessar seu usuário no sistema, não consegue por haver incoerência em suas informações.


- Você então ao invés de solicitar apoio ao pessoal da TI, verifica que recebeu um e-mail, há alguns dias, perguntando se gostaria de resetar sua senha.

- No e-mail, não havia uma identificação do nome do sistema, nem um telefone de contato para auxílio e, mesmo assim, você resolveu respondê-lo, informando seu atual usuário e uma nova senha de acesso.

Você gostaria de mudar sua senha?
Informe a sua senha atual:

Nessa situação, havia um invasor aguardando que a senha fosse resetada através do e-mail, que o *cracker* elaborou ao funcionário.

O invasor, então, tem total acesso às informações guardadas no sistema.

Identifique qual foi o tipo de ataque efetuado pelo invasor e dê dicas de como se previnir nesse caso.

EDUCAÇÃO METODISTA

# AULA 04

EDUCAÇÃO METODISTA

# Como se prevenir?

- **Cabeçalhos suspeitos**
  - ✔ O cabeçalho do e-mail aparece incompleto, sem o remetente ou o destinatário, ou com apelidos ou nomes genéricos.

- **Opções para sair da lista de divulgação**
  - ✔ Existe *spams* que tentam justificar o abuso, alegando que é possível sair da lista de divulgação.

# Dicas para evitar spams

- Preservar as informações pessoais, como endereços de e-mail, dados pessoais e, principalmente, cadastrais de bancos, cartões de bancos, cartões de crédito e senhas.
- Ter sempre que possível, e-mails separados para assuntos pessoais, profissionais, para as compras e cadastros *on-line.*
- Procurar controlar a curiosidade de verificar sempre a indicação de um site em um e-mail suspeito de spam.
- Ter um filtro antispam instalado ou, ainda, usar os recursos antispams oferecidos pelo seu provedor de acesso.

# Recomendações gerais

- **Senhas:** complexidade, troca periódica, individualidade, mecanismos de recuperação.

Gerador de Senha: 11 melhores sites e apps para usar
*Link*:
https://www.tecmundo.com.br/seguranca/247875-gerador-senha-11-melhores-sites-apps-usar.htm

https://chrome.google.com/webstore/detail/bitwarden-free-password-m/nngceckbapebfimnlniiiahkandclblb?hl=pt-BR

# Criando uma senha forte

- Uma boa senha atenderá aos seguintes requisitos:

  - Um caractere inglês maiúsculo (A-Z)
  - Um caractere em caixa baixa do inglês (a-z)
  - Um número (0-9) e / ou símbolo (como!, # Ou%)
  - Dez ou mais caracteres no total.

# Criando uma senha forte

## Método A: converter uma frase em acrônimo

Escolha uma frase que você possa lembrar e reduza-a às primeiras letras de cada palavra, trabalhando em alguns números, letras maiúsculas e pontuação.

Exemplo Segunda Lei de Newton

Fr: força resultante
m: massa
a: aceleração

acronimo:

Fora Maria

**F.r = m.a**

## Método B: frase única

Escolha 4-5 letras e, em seguida, faça uma frase usando palavras que começam com cada uma dessas letras. Adicione um número ou pontuação, se fizer sentido.

Exemplo:

Viajar cidade ano / Independencia Financeira Meta

V!a6@rio2021

V!a6@euro22

1nF!@2024

1nF!@Mar21

EDUCAÇÃO METODISTA

# Gerenciadores de Senhas

- As senhas mais fortes são criadas por gerenciadores de senhas, software que gera e controla senhas complexas e exclusivas para todas as suas contas. Tudo que você precisa lembrar é a senha do gerenciador de senhas. Ao escolher um gerenciador de senhas, escolha um que ofereça suporte à verificação em duas etapas.

  - Site 2
  - Site 3
  - Site 4

# Verificação em duas etapas

- Quando você ativa a verificação em duas etapas, sempre que usar sua conta em um novo dispositivo, um código de autorização chegará ao seu telefone. Sem o código, um ladrão de senha não pode assumir o controle de sua conta. É a melhor maneira de proteger sua conta de criminosos cibernéticos. Duas etapas estão disponíveis para a maioria dos serviços de aplicativos.

# Recomendações gerais

**Conexões seguras, observância do cadeado**. Ao acessar um site, procure na barra de endereço do navegador o ícone do cadeado, que normalmente é exibido à esquerda do URL. O cadeado fechado indica que a conexão entre seu navegador e o servidor do site está criptografada e segura. Clique no cadeado para obter mais informações sobre a segurança do site e o certificado SSL.

**Características dos Browsers:**
Os navegadores modernos, como o Google Chrome, Mozilla Firefox e Microsoft Edge, possuem recursos de segurança que ajudam a identificar conexões seguras. Além do cadeado, eles podem exibir o nome da organização proprietária do *site*, certificando a autenticidade do mesmo. Além disso, eles alertam quando você está prestes a entrar em um site não seguro.

# Recomendações gerais

**Atenção aos Nomes de Domínio:**
É essencial observar atentamente o nome de domínio do site que você está acessando. Os golpistas frequentemente tentam enganar os usuários criando sites falsos com nomes semelhantes aos de sites legítimos. Isso é conhecido como ataque de phishing. Por exemplo, um site legítimo pode ser "minhaempresa.com", enquanto um site falso pode ser "minhaempresa123.com". Verifique sempre se o nome de domínio está escrito corretamente e se corresponde à empresa ou serviço que você espera acessar.

# Recomendações gerais

- **Antivírus:** importância, atualização e varreduras periódicas.


EDUCAÇÃO METODISTA

# Recomendações gerais

- **Firewall:** importância, atualização e funcionamento básico das regras.

Um firewall é uma barreira de segurança projetada para proteger redes de computadores e sistemas contra ameaças, monitorando e controlando o tráfego de dados que entra e sai de uma rede. Ele age como um filtro entre a rede local e a internet ou outras redes externas, permitindo apenas o tráfego autorizado e bloqueando ou filtrando o tráfego malicioso ou não autorizado.

# Recomendações gerais

## Atualizações de software

# Recomendações gerais

- **Backup:** importância, opções disponíveis, locais de armazenamento, quantidade de cópias, proteção das cópias.
- **Mensagens suspeitas:** características, canais por onde elas são entregues, como avaliar sua veracidade, onde denunciar atividades suspeitas.
- **Privilégio mínimo:** definição, objetivos, práticas para incorporação na rotina.
- **Mesa limpa:** definição, importância, dicas de implementação.

# Recomendações gerais

- **Descarte seguro:** importância, uso de fragmentadores e destruidores, informações que não devem ser descartadas sem tratamento.

- **Computação móvel:** riscos, criptografia, backup, senhas, rastreamento e localização de dispositivos.

- **Keylogger USB:** é um dispositivo capaz de gravar as teclas pressionadas pelas vítimas, sendo utilizado normalmente para descobrir senhas ou outras informações sensíveis. Ele tem um conector USB macho e fêmea, podendo facilmente ser colocado pelo invasor entre uma porta USB no micro do usuário e o cabo USB do teclado sem que este perceba.

# Material Complementar

- Os maiores ataques hackers da história

  https://www.tecmundo.com.br/seguranca/9971-os-maiores-ataques-hackers-da-historia.htm?v=1073158524

- Dez hackers que entraram para a história

  https://gizmodo.uol.com.br/dez-hackers-que-entraram-para-a-historia/?v=707441770

# Referências

DODT, C. **Transformando sua política de segurança da informação em um ativo estratégico.** 2011. Disponível em: <https://claudiododt.wordpress.com/2011/06/29/transformando--sua-politica-de-seguranca-da-informacao-em-um-ativo-estrategico/>. Acesso em: 14 jul. 2023.

# Conceitos de segurança lógica física

EDUCAÇÃO METODISTA

# Conceitos de segurança lógica física

"Conceitos de segurança lógica física" refere-se à combinação de dois tipos de segurança distintos: a segurança lógica e a segurança física. Ambos os conceitos são essenciais para proteger ativos e informações valiosas em uma organização ou sistema.

# Conceitos de segurança lógica física

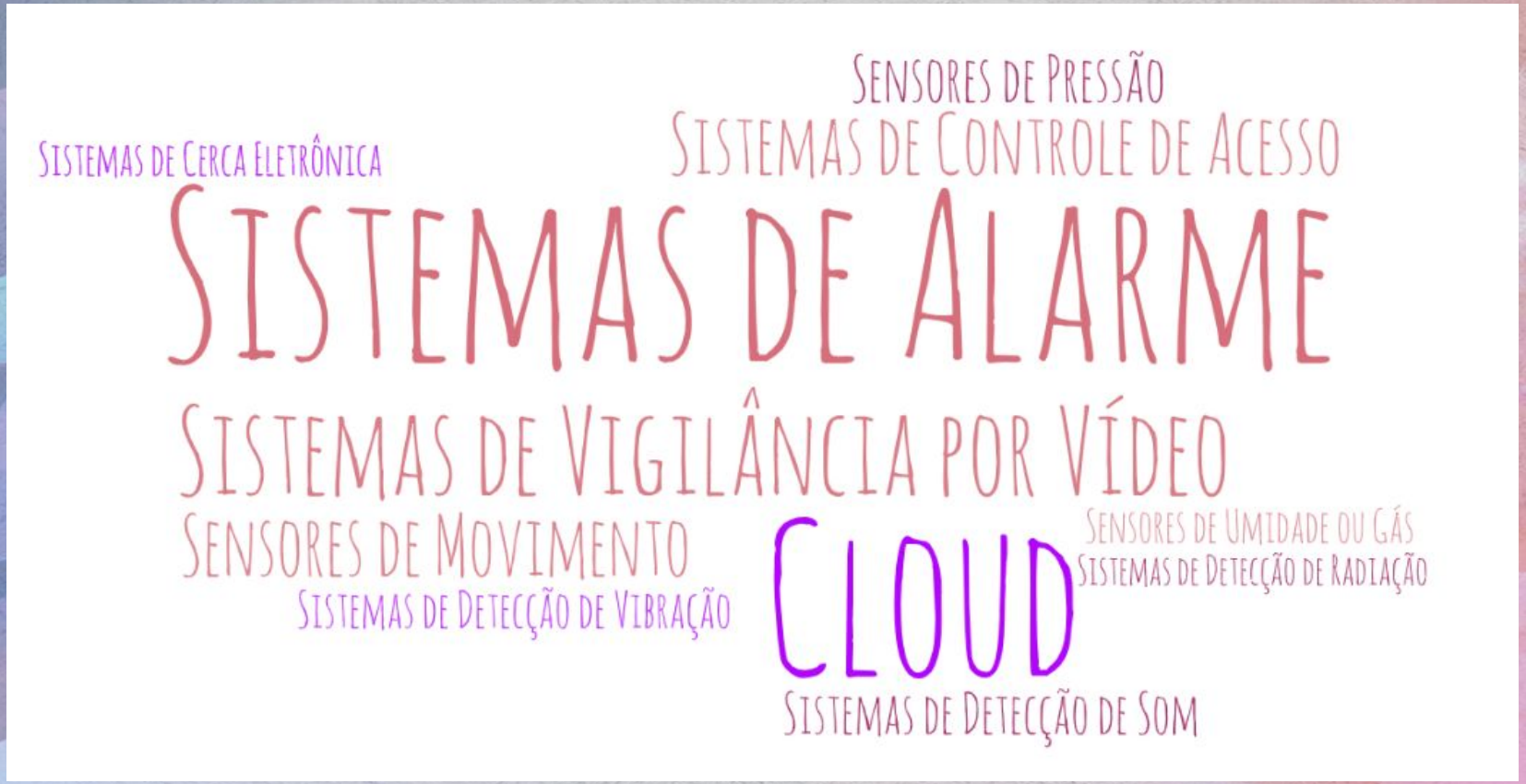
**Segurança Lógica:** Envolve a proteção de sistemas de informação, redes, dados e recursos digitais por meio de medidas tecnológicas e procedimentos. Isso inclui autenticação de usuários, autorização de acesso, criptografia, firewalls, detecção de intrusões, políticas de senhas, entre outros. A segurança lógica é voltada para a prevenção de ameaças cibernéticas, como hackers, malware e acessos não autorizados.

# Conceitos de segurança lógica física

**Segurança Física:** Refere-se à proteção dos ativos físicos de uma organização, como instalações, equipamentos, servidores e dispositivos. Isso pode incluir o controle de acesso físico por meio de fechaduras, sistemas de vigilância por vídeo, cercas, alarmes e medidas de prevenção de desastres naturais. A segurança física visa impedir a entrada não autorizada em espaços físicos e reduzir os riscos de roubo, vandalismo e interrupções.

Um exemplo clássico de ataque físico de interface é um cabo de rede em uma organização que, uma vez solto, oferece uma brecha para que o intruso possa conectar um dispositivo na rede e então promover o ataque desejado.

# Mecanismos de detecção de intrusão física




Educação Metodista

# Tecnologias para a implementação de segurança lógica física

A implementação de segurança lógica física envolve a utilização de uma combinação de tecnologias para proteger tanto os aspectos digitais quanto físicos de uma organização. Aqui estão algumas tecnologias comuns que são usadas para implementar essa abordagem de segurança abrangente:

# Tecnologias para a implementação de segurança lógica física

**Sistemas de Controle de Acesso Integrados:** Plataformas que combinam sistemas de controle de acesso físico (por exemplo, leitores de cartão, sistemas biométricos) com sistemas de controle de acesso lógico (autenticação em redes e sistemas). Isso garante que apenas pessoas autorizadas possam acessar áreas físicas e sistemas digitais.

# Tecnologias para a implementação de segurança lógica física

**Vigilância por Vídeo Inteligente:** Câmeras de segurança equipadas com recursos de análise de vídeo avançados, como detecção de movimento, reconhecimento facial, análise de comportamento e contagem de pessoas. Essas tecnologias podem identificar atividades suspeitas ou comportamentos anormais.

# Tecnologias para a implementação de segurança lógica física

**Sistemas de Gestão de Identidade e Acesso (IAM):** Plataformas que gerenciam a autenticação e autorização de usuários para sistemas, aplicativos e recursos digitais, bem como o acesso físico a instalações. Isso inclui gerenciamento de senhas, autenticação multifator (MFA) e provisionamento de contas.

# Tecnologias para a implementação de segurança lógica física

**Biometria Avançada:** Utilização de características únicas dos indivíduos, como impressões digitais, íris, reconhecimento facial e até mesmo padrões de voz, para autenticação e controle de acesso tanto a sistemas digitais quanto a áreas físicas.

# Tecnologias para a implementação de segurança lógica física

De acordo com Goodrich e Tamassia (2013), para uma biometria ser considerada um recurso de identificação a partir de determinada característica (impressão digital, por exemplo), existem diversos requisitos a serem atendidos, listados a seguir:

1. **Universalidade:** quase todas as pessoas precisam ter alguma característica que seja comum a todos, sendo a mais conhecida a impressão digital.

# Tecnologias para a implementação de segurança lógica física

2. **Distinção**: as características de cada pessoa devem apresentar diferenças notáveis, sendo, por exemplo, o DNA e a retina inconfundíveis.

3. **Permanência**: a característica biométrica não deve se alterar de forma significativa com o tempo.

4. **Coletável**: a biometria precisa ser determinada e quantificada de forma efetiva.

# Tecnologias para a implementação de segurança lógica física

**Sistemas de Detecção de Intrusão:** Combinação de sensores físicos (como sensores de movimento e de abertura) com sistemas de monitoramento e alerta para detecção precoce de atividades intrusivas em espaços físicos.

# Tecnologias para a implementação de segurança lógica física

**Sistemas de Prevenção de Intrusões (IPS):** Ferramentas que monitoram e analisam o tráfego de rede em busca de atividades maliciosas, detectando e bloqueando tentativas de intrusão em sistemas e redes digitais.

# Tecnologias para a implementação de segurança lógica física

**Firewalls Físicos e Virtuais:** Barreiras de segurança que controlam o tráfego de rede, permitindo ou bloqueando o acesso com base em regras predefinidas. Firewalls podem ser implementados tanto em nível físico (dispositivos) quanto em nível lógico (software).

# Tecnologias para a implementação de segurança lógica física

**Encriptação de Dados:** A aplicação de algoritmos de criptografia para proteger dados confidenciais em trânsito e em repouso, garantindo que apenas as partes autorizadas possam acessar e compreender as informações.

# Tecnologias para a implementação de segurança lógica física

**Sistemas de Gestão de Incidentes:** Plataformas para rastrear e responder a incidentes de segurança, tanto físicos quanto lógicos, com fluxos de trabalho definidos para lidar com ameaças em tempo real.

# Tecnologias para a implementação de segurança lógica física

**Monitoramento de Integridade:** Ferramentas que monitoram e verificam a integridade dos sistemas, aplicativos e arquivos, alertando sobre quaisquer alterações não autorizadas ou suspeitas.

# Saiba Mais…

**Proteção de dados pessoais em redes sociais**

*Link*: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Danilo-Doneda_FINAL.pdf.pdf

**Desenvolvimento em segurança da informação**

*Link*: https://www.youtube.com/embed/69ZdfDlC5fw

# PRÁTICAS RELACIONADAS A APLICAÇÕES DO USO DE DADOS, MARKETING E MÍDIAS SOCIAIS

# USO DE DADOS, MARKETING E MÍDIAS SOCIAIS

A economia atual é movida a partir de um importante ativo: **Informações**
Obter informações sobre uma quantidade grande de possíveis clientes tornou-se atividade diárias dentro de várias organizações:

- Que tipo de produto ou serviços o potencial consumidor está mais propenso a comprar?
- Como se comporta nas mídias sociais?
- Como se comporta na internet ou em lojas físicas?
- Quanto estão dispostos a gastar?
- Que tipo de propaganda mais o atrai?
- A construção destes perfis necessita de muitos dados sobre pessoas e seu comportamento. Como obter essas informações?

# USO DE DADOS, MARKETING E MÍDIAS SOCIAIS

## COOKIES

Um cookie, no âmbito da Internet, é um **pequeno arquivo texto de computador ou pacote de dados enviados por um site da Internet para o navegador do usuário, quando esta visita o site.**

Cada vez que o usuário visita o site novamente, o navegador envia o cookie de volta para o servidor para notificar atividades prévias do usuário.

EDUCAÇÃO METODISTA

# USO DE DADOS, MARKETING E MÍDIAS SOCIAIS

**Tipos mais comum de Cookies**

**Cookies de sessão**

Ao sair do site, e fechar o navegador, o cookie da sessão é apagado da memória do computador do usuário e, como resultado, ele é apagado

O exemplo mais comum é o recurso de carrinho de compras de qualquer loja virtual. Sempre que os itens são selecionados, a seleção é armazenada no cookie da sessão

**Cookies persistentes**

Os cookies persistentes permanecem no disco rígido do usuário até serem apagados pelo usuário ou até expirarem..

Por exemplo, para manter a seleção de idioma do usuário.

**Cookies de rastreamento**

Geralmente é chamado de cookie de terceiros. Ele é colocado no disco rígido de um usuário por um site de um domínio diferente daquele que o usuário está visitando.

Definidos por redes de publicidade nas quais um site pode se inscrever.

EDUCAÇÃO METODISTA

Analise os ***cookies*** do *site*

# Criptografia, Assinatura Digital e Certificados

O termo **criptografia** vem do grego e é uma combinação das palavras **“kryptós”, que significa “escondido”, e “gráphein”, que significa “escrita”.**

Existem diferentes sistemas de criptografia, que podem ser usado para vários propósitos, como garantir :

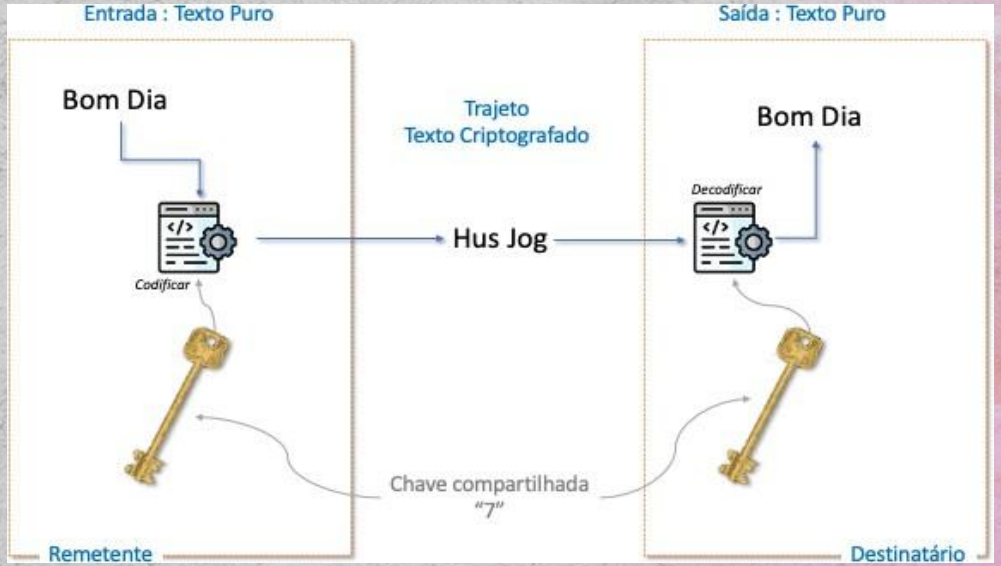
- Integridade de dados,
- autenticidade de dados,
- mecanismos de autenticação e não repúdio à informação.

# Criptografia, Assinatura Digital e Certificados

## Tipos de Sistemas

**Criptográficos** Sistema

Simétrico



# Criptografia, Assinatura Digital e Certificados

**Tipos de Sistemas Criptográficos - Sistema Assimétrico**

A criptografia assimétrica é caracterizada pela existência de um par de chaves:

**a chave privada e a chave pública**.

Uma mensagem encriptada com a chave privada só poderá ser decriptada com a chave pública correspondente, assim como uma mensagem encriptada com uma chave pública só poderá ser decriptada com a chave privada correspondente. Para executar a criptografia assimétrica com intuito de autenticação, a mensagem enviada é criptografada com a chave privada do remetente. Ao receber a mensagem, ela deverá ser decriptografada pelo destinatário utilizando a chave pública do remetente. Se for possível decriptá-la com esta chave pública, é garantida a autenticidade do remetente.

Para garantir a confidencialidade e a integridade do conteúdo de uma mensagem, o remetente deverá criptografar a mensagem com a chave pública do destinatário. Desta forma, apenas o destinatário terá acesso ao conteúdo da mensagem, uma vez que apenas ele possui a chave privada relacionada àquela chave pública.

# Criptografia, Assinatura Digital e Certificados

**Assinaturas digitais e certificados**

Uma assinatura digital é um método para confirmar se a informação digital foi produzida ou enviada por quem reivindica ser a origem, são criadas utilizando criptografia assimétrica.

É também possível verificar a assinatura digital utilizando um certificado, o que deve ser feito de forma segura, tal como, por exemplo, um token ou smartcard.

# Software malicioso – Malware & Cia

- Malware é a combinação das palavras inglesas “malicious” e “software” e se refere a softwares indesejados, tais como vírus, worms, cavalos de Troia e spyware.

- Um tipo de fraude na internet que tem como objetivo “pescar” suas informações, principalmente dados de documento e bancários.

- Spam : Mensagens indesejadas. O termo é normalmente usado para e-mails indesejados, mas as mensagens publicitárias indesejadas em websites também são consideradas spam.

- Hacking : Atividades que têm como objetivo comprometer dispositivos digitais como computadores, smartphones, tablets e até mesmo redes inteiras.

# Ao acessar o site bancário

- certifique-se de usar computadores e dispositivos móveis seguros

- digite o endereço do site bancário diretamente no navegador Web

evite seguir ou clicar em links recebidos via mensagens eletrônicas (e-mails, mensagens SMS, redes sociais, etc.)

não utilize sites de busca para localizar o site bancário

geralmente o endereço é bastante conhecido

- sempre acesse sua conta usando a página ou o aplicativo fornecido pelo próprio banco

# Ao acessar o site bancário

- antes de instalar um módulo de proteção, certifique-se de que o autor do módulo é realmente a instituição em questão

- evite usar dispositivos móveis e computadores de terceiros (como lan houses, e Internet cafés)
não há garantias de que os equipamentos estejam seguros

- sempre acesse sua conta usando a página ou o aplicativo fornecido pelo próprio banco

- evite usar redes Wi-Fi públicas

- utilize um endereço terminado em “b.br”, caso seu banco ofereça essa opção domínios terminados em “b.br”, além de serem de uso exclusivo de instituições bancárias, também oferecem recursos adicionais de segurança

# Ao acessar o site bancário

- certifique-se de usar conexões seguras. Alguns indícios desse tipo de conexão são:

- o endereço do site começa com “https://”
- o desenho de um “cadeado fechado” é mostrado na barra de endereço, ao clicar sobre ele, são exibidos detalhes sobre a conexão/certificado digital em uso

- um recorte colorido (branco ou azul) com o nome do domínio do site é mostrado ao lado da barra de endereço (à esquerda ou à direita) ao passar o mouse ou clicar sobre ele, são exibidos detalhes sobre conexão/certificado digital em uso
- a barra de endereço e/ou o recorte são apresentados na cor verde e no recorte é colocado o nome da instituição dona do site

# ANONIMIZAÇÃO& PSEUDONIMIZAÇÃO

## Anonimização

“Utilização de meios técnicos razoáveis e disponíveis no momento do processamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”

## Exemplo Dado Anonimizado

| ID | Nome | Gênero | Nascimento | Partido |
|---|---|---|---|---|
| xxxxxx | xxxxxxx | Masculino | 1959-1970 | A |

| Quantidade Pessoas | Gênero | Nascimento | Partido |
|---|---|---|---|
| 3 | Masculino | 1959 - 1970 | A |

# ANONIMIZAÇÃO & PSEUDONIMIZAÇÃO

**Pseudonimização**

Artigo 4º, 5 - “processamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular dos dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa física identificada ou identificável”

EDUCAÇÃO METODISTA

## Exemplo PseudoAnonimizado

| Nome | E-mail | Referência | Gênero | Idade |
|---|---|---|---|---|
| Daniel | Daniel@email | 1234 | Masculino | 50 |

| Nome | E-mail | Referência | Referência | Gênero | Idade |
|---|---|---|---|---|---|
| Daniel | Daniel@email | 1234 | 1234 | Masculino | 50 |