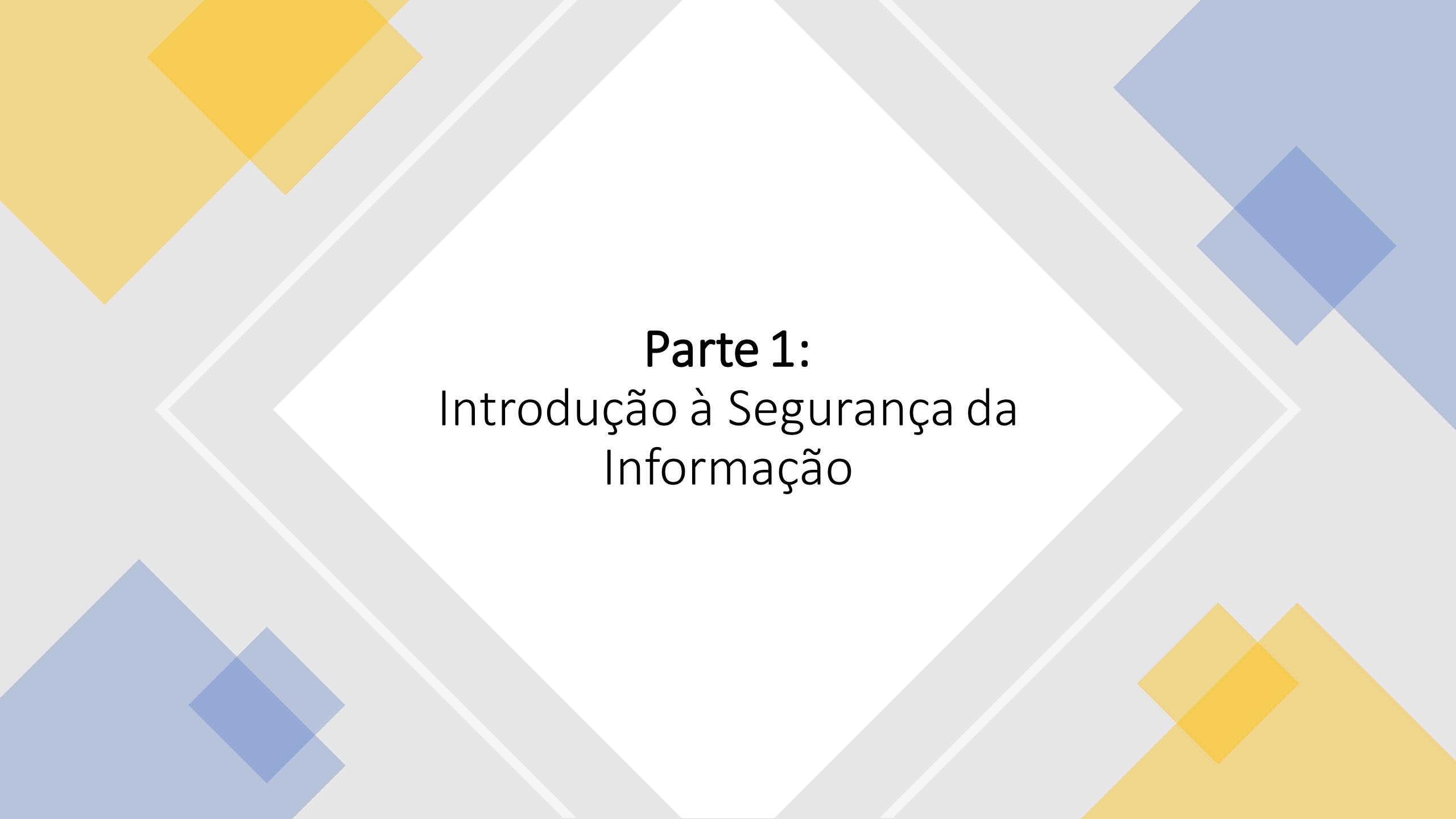


# Redes e Segurança


---

Universidade de Mogi das Cruzes (UMC)



# **Parte 1:**

## Introdução à Segurança da Informação



## Ciência da Informação: Pirâmide do conhecimento



# Importância da Informação

Informações são um ativo da empresa

- Devem ser protegidas!
  - Garantir continuidade dos negócios
  - Maximizar o retorno de investimentos/oportunidades
  - Minimizar transtornos.

# Ativos Empresariais

- Exemplifiquem ativos empresariais...

# Importância da Informação

Informações estão em constante risco

- Em especial porque muitas são “sensíveis”
  - Proteção dos negócios
  - Lei Geral de Proteção de Dados

# Importância da I nformação

- Objetivo: garantir
  - Confidencialidade
  - Integridade
  - Disponibilidade

# Segurança da Informação

- Um conjunto de medidas que se constituem basicamente de controles e política de segurança, tendo como objetivo a proteção das informações dos clientes e da empresa (ativos/bens), controlando o risco de revelação ou alteração por pessoas não autorizadas.



# RISCO? QUE RISCO?

Definindo alguns termos...

- **Ameaça**
  - Qualquer ocorrência que possa provocar perda. Evento ou atitude indesejável que potencialmente remove, desabilita, danifica ou destrói um recurso;

# RISCO? QUE RISCO?

Definindo alguns termos...

- **Vulnerabilidade**
  - Elementos que expõem às ameaças.
  - Característica de fraqueza de um bem;
  - Características de modificação e de captação de que podem ser alvos os bens, ativos, ou recursos intangíveis de informática, respectivamente, software, ou programas de bancos de dados, ou informações, ou ainda a imagem corporativa.

# RISCO? QUE RISCO?

Definindo alguns termos...

- **Desastre**
  - Impacto de uma força externa que ocasiona perda ou prejuízo; não precisa ser destruidor!

# RISCO? QUE RISCO?

- **Ameaças**
  - Existência de potenciais invasores com interesse nas informações que mantemos
  - Funcionários insatisfeitos com acesso ao banco de dados
- **Vulnerabilidades**
  - Uma versão antiga de webserver com falha conhecida
  - Código PHP mal elaborado que permita injection
- **Desastres**
  - Furto das informações confidenciais de nosso banco de dados
  - Deleção do banco de dados como um todo

# RISCO? QUE RISCO?

Definindo alguns termos...

- **Risco**
  - A probabilidade da ocorrência de uma ameaça em particular.
  - A probabilidade que uma ameaça explore uma determinada vulnerabilidade de um recurso.

# RISCO? QUE RISCO?

Risco é uma probabilidade de:

- Ameaças e vulnerabilidades...
- Levarem a desastres!

Em geral, define-se risco como sendo:

***risco** = ameaças . vulnerabilidade*

Em outras palavras:

- Se não houver ameaças ou vulnerabilidades...
- Não haverá riscos.

# Inevitabilidade dos Riscos

Riscos são inevitáveis

- Investidores comprando ações
- Cirurgiões realizando operações
- Engenheiros projetando pontes
- Empresários abrindo negócios
- Etc...

# Inevitabilidade dos Riscos

Mas gerenciá-los é estratégico:

- Precisam ser minimizados ou mitigados...
- Já que não temos como eliminá-los totalmente



# Política de Segurança da Informação

- Um conjunto de diretrizes (normas) que definem formalmente as regras e os direitos dos usuários, visando à proteção adequada dos ativos da informação.

# Princípios da Política de Segurança

- **Integridade:** Condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas.
- **Confidencialidade:** Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização prévia do seu dono.
- **Disponibilidade:** Possibilidade de acesso à informação por parte daqueles que a necessitam para o desenvolvimento de suas atividades.

# Ameaças à Política de Segurança

- **Integridade:** Ameaças de ambiente (fogo, enchente...), erros humanos, fraudes, erro de processamento.
- **Confidencialidade:** Divulgação premeditada ou acidental de informação confidencial.
- **Disponibilidade:** Falhas de sistemas, remoção de arquivos por falha humana ou sem autorização.

# Mecanismos de Segurança

- **Controle físico:** Barreiras que limitam o contato ou acesso direto à informação ou a estrutura que a suporta.
  - Ex: Porta, paredes, trancas, blindagem, guardas, etc.
- **Controle lógico:** Barreiras que limita o acesso à informação em ambiente eletrônico.
  - **Mecanismos de criptografia**
    - Modificar a informação de forma que seja impossível que pessoas não autorizadas a decodifiquem.
  - **Mecanismos de controle de acesso**
    - Senhas, Firewall, Sistemas biométricos

# Gestão de Riscos

Processo para identificar, mensurar e planejar passos para reduzir um determinado risco a níveis aceitáveis pela organização.

# Gestão de Riscos

## **Informação é estratégica!**

- Fundamental realizar análise de riscos voltada aos ativos de informação
- Determinar quais riscos podem afetar a entrega de produtos ou serviços
- É preciso conhecer os requisitos de negócio!

# Avaliação de Riscos: Identificação das Ameaças

- Históricos de incidentes de segurança.
  - Estatísticas da empresa ou fontes externas.
- Tipos de ameaças:
  - Naturais (terremoto, enchente, incêndio etc...)
  - Humanas (dolosos, imperitos, imprudentes ou negligentes)
  - Ambientais (falta de energia, poluição etc...)

# Avaliação de Riscos: Identificação de Vulnerabilidades

Falhas ou fraquezas de segurança.

- Listas de verificação:
  - Falhas de software e hardware
- Outros métodos:
  - Testes e simulações
  - **Teste de invasão de sistemas**
  - Auditoria de código



# Avaliação de Riscos: Análise de Probabilidades

- Produção de índice indicativo da chance de uma ameaça se tornar um desastre
  - **Alta:** existe uma ameaça evidente e nenhum controle preventivo efetivo.
  - **Média:** existe uma ameaça evidente, mas há controles efetivos em ação.
  - **Baixa:** a ameaça é desmotivada e há controles efetivos em ação.
- Considerar experiências passadas
  - Estatísticas históricas de ocorrências.
  - Fatores climáticos e geográficos.
  - Situações que poderiam levar a erros humanos.

# Avaliação de Riscos: Análise de Impactos

Determinar impacto e valor do sistema para a organização

- Inicia-se com:
  - Missão do sistema
  - Criticidade do sistema de dados
  - Sensibilidade dos dados do sistema
- Identificar o impacto...
  - Caso a ameaça “tenha sucesso”
  - Integridade, disponibilidade e confidencialidade
- Qualitativa x Quantitativa

# Avaliação de Riscos: Determinação do Risco

Avaliar:

- A possibilidade de exploração da vulnerabilidade
- O impacto ao negócio devido a evento adverso
- Efetividade de controles para reduzir os riscos.
- Tabela conforme ABNT (notas 0 a 8)

# Avaliação de Riscos: Recomendações de Controle

Sugerir novos controles para mitigar riscos

- Considerar:
  - Efetividade de opções recomendadas
  - Legislação e regulamentação
  - Política organizacional
  - Impacto operacional
  - Segurança e confiabilidade.

# Avaliação de Riscos: Documentação dos Resultados

- Documentação e armazenamento
  - Estabelecer uma base de conhecimento
  - Apoiar novas políticas e procedimentos
- Não se busca apontar erros
  - Indicar os riscos inerentes
  - Justificar investimentos
  - Reduzir potenciais perdas e danos

# LIDANDO COM OS RISCOS

Há dois tipos principais de abordagem:

- Reativa
- Proativa

# LIDANDO COM OS RISCOS: **Abordagem reativa**

- Agir quando ocorre um incidente
  - Sempre que ocorrer um incidente...
  - Verificar e agir para não voltar a acontecer
- Envolve:
  - Auditoria
  - Análise e pesquisa
  - Documentação
  - Implementação de medidas.

# LIDANDO COM OS RISCOS: Abordagem proativa

- Agir para que não haja incidentes
  - Prática diária, agir antes de acontecer
  - Para evitar que incidentes venham a acontecer
- Envolve:
  - Pesquisa de falhas
  - Análise de logs
  - Documentação
  - Implementação de medidas



# Abordagens de Segurança

Não são excludentes!

- Ambas: mitigação de riscos futuros
  - Proativa é efetiva também para o presente
  - Reativa tende a ser mais cara no longo prazo.

# Normas Regulamentadoras de Segurança da Informação

ISO é a abreviação ou sigla referente a International Organization for Standardization, que em português significa Organização Internacional para Padronização, e foi criada em 1947 na Suíça.

# Normas Regulamentadoras de Segurança da Informação

- **ISO/IEC 27000** - é a norma básica que inclui o vocabulário, glossário que trata sobre a Gestão da Segurança de Informação.
- **ISO/IEC 27001** - trata sobre os requisitos para que um Sistema de Gestão de Segurança da Informação esteja correto.
- **ISO 27001** - se a empresa quiser obter um certificado de segurança, essa norma é a que deve, em primazia, ser observada, ela é considerada uma ISO aditável, a única que quando falamos das normas aditáveis que definem requisitos de SGSI.

# Normas Regulamentadoras de Segurança da Informação

- **ISO/IEC 27002** - recomendável que seja feito o seu uso junto com a ISO 27001, essa norma trata das políticas que auxiliam a gestão e a colocação de um Sistema de Segurança da Informação. Essa norma é a única em que você poderá tirar certificados profissionais.
- **ISO/IEC 27003** - enquanto a ISO 27001 dita apenas os requisitos para um sistema de segurança de informação, a ISO 27003 trata das diretrizes, isto é, dá o “passo a passo” para a criação de um SGSI.

# Normas Regulamentadoras de Segurança da Informação

- **ISO/IEC 27004** - define métricas, isto é, metas para o alcance da segurança da informação e de sua gestão, por isso ela é tão importante quando uma empresa deseja acompanhar de perto os seus resultados.
- **ISO/IEC 27005** - trata da gestão de riscos, e pode ser comparada com a seção 4 da ISO 27001.
- **ISO/IEC 27006** - define o que uma empresa de auditoria deve levar em consideração quando deseja validar o sistema de gestão de segurança da informação de uma empresa X.

# Normas Regulamentadoras de Segurança da Informação

- **ISO/IEC 27007** - deve ser usada em conjunto com a ISO 27006, já que trata dos padrões que a auditoria deve seguir.
- **ISO/IEC 27008** - trata do controle de segurança.
- **ISO/IEC 27009** - foca nas indústrias que desejam trabalhar com essa adequação.
- **ISO/IEC 27011** - refere-se especialmente ao rito de segurança que deve ser feito por empresas que trabalham com telecomunicações, isto é, call-center dentre outros.

# Normas Regulamentadoras de Segurança da Informação

- **ISO/IEC 27013** - trata da integração das normas 27001 e 27002, tratando como deve ser a implementação delas de maneira conjunta.
- **ISO/IEC 27015** - pode ser considerada uma norma que complementa a 27002, e trata da segurança no mercado financeiro.
- **ISO/IEC 27016** - aborda os pontos de segurança da informação no que concernem a economia em um todo.

# Normas Regulamentadoras de Segurança da Informação

- **ISO/IEC 27017** - trata especificamente sobre a segurança em computação na nuvem, ou cloud computing.
- **ISO/IEC 27018** - é uma norma complementadora da 27017, e trata basicamente sobre a PII, a privacidade quando se trata de cloud computing, ou computação na nuvem.
- **ISO 27031** - trata de conceitos da segurança de informações no TIC.



# Normas Regulamentadoras de Segurança da Informação

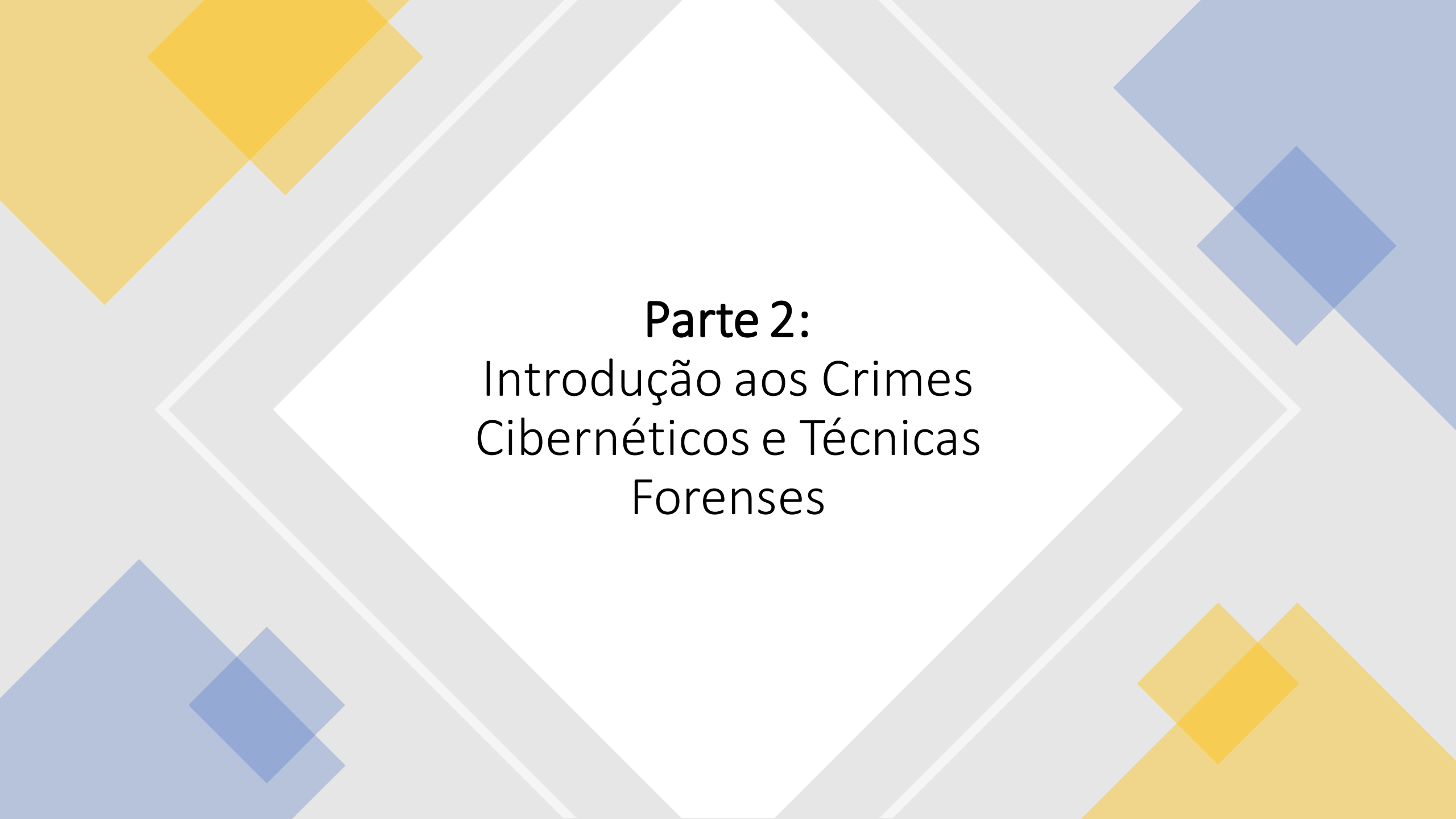
- **ISO 27033-1** - é a parte introdutória das ISO que tratam sobre redes e ela fala basicamente os conceitos e definições utilizadas.
- **ISO 27033-2** - é o guia que trata desde o planejamento até a execução da segurança de redes.
- **ISO 27033-3** - foca nas técnicas que tratam da segurança de redes, e buscam definir conceitos e riscos.

# Normas Regulamentadoras de Segurança da Informação

- **ISO 27033-1** - é a parte introdutória das ISO que tratam sobre redes e ela fala basicamente os conceitos e definições utilizadas.
- **ISO 27033-2** - é o guia que trata desde o planejamento até a execução da segurança de redes.
- **ISO 27033-3** - foca nas técnicas que tratam da segurança de redes, e buscam definir conceitos e riscos.

# Normas Regulamentadoras de Segurança da Informação

- **ISO 27033-4** - trata de ameaças de segurança no que se relacionam a gateways e informações no que concerne a segurança de redes.
- **ISO 27033-5** - fala sobre a proteção de redes utilizando VPN.
- **ISO 27033-6** - trata sobre as técnicas e desenhos no que concernem a redes sem fio e sinais e frequências de rádio.



## **Parte 2:**

# Introdução aos Crimes Cibernéticos e Técnicas Forenses

## Conceitos: Hacker

- Os hackers são indivíduos com habilidades avançadas em computação, que usam suas habilidades para encontrar vulnerabilidades em sistemas de computador. Eles podem ser classificados em diferentes categorias, dependendo de suas motivações e objetivos.

## Conceitos: Hacking

- Termo geral usado para descrever a ação de explorar vulnerabilidades de segurança em sistemas e redes para obter acesso não autorizado ou realizar atividades maliciosas.

## Conceitos: Cracker

- Os crackers são indivíduos que usam suas habilidades em computação para violar a segurança de sistemas de computador e redes. Eles geralmente têm motivações criminosas ou maliciosas.

## Conceitos: Cracking

- Os crackers são indivíduos que usam suas habilidades em computação para violar a segurança de sistemas de computador e redes. Eles geralmente têm motivações criminosas ou maliciosas.



## Conceitos: **White Hats**

- Os white hats são hackers éticos que usam suas habilidades para encontrar e corrigir vulnerabilidades em sistemas de computador e redes. Eles geralmente trabalham para empresas de segurança cibernética ou agências governamentais.

## Conceitos: Gray Hats

- Os gray hats são hackers que usam suas habilidades para encontrar vulnerabilidades em sistemas de computador, mas não necessariamente com intenções maliciosas. Eles podem alertar os proprietários dos sistemas sobre as vulnerabilidades encontradas.

## Conceitos: **Black Hats**

- Os black hats são hackers que usam suas habilidades para violar a segurança de sistemas de computador e redes com intenções maliciosas. Eles podem roubar informações pessoais, infectar computadores com malware ou realizar ataques DDoS.

## Conceitos: **Lammers**

- Os lammers são indivíduos com poucas habilidades em computação que tentam se passar por hackers. Eles geralmente não têm intenções maliciosas e podem se tornar uma fonte de problemas de segurança para seus próprios sistemas.

## Conceitos: **Script kiddies**

- São indivíduos que usam ferramentas de hacking pré-fabricadas para realizar ataques cibernéticos, geralmente sem muito conhecimento técnico. Eles usam programas de hacking automatizados para explorar vulnerabilidades conhecidas e comprometer sistemas sem entender completamente o que estão fazendo.

## Conceitos: Spammers

- São pessoas ou empresas que enviam spam em massa. Eles podem ser motivados por razões comerciais, políticas ou outras.

## Conceitos: Spam

- É o envio de e-mails em massa não solicitados, geralmente para fins de marketing ou propaganda. O spam pode ser enviado por pessoas físicas ou empresas.

## Conceitos: Spammers

- São pessoas ou empresas que enviam spam em massa. Eles podem ser motivados por razões comerciais, políticas ou outras.



## Conceitos: Scams

- São golpes cibernéticos que visam enganar as pessoas para que forneçam informações pessoais, financeiras ou outras informações valiosas. Os scams são geralmente realizados por meio de engenharia social e podem incluir falsos e-mails de phishing, sites fraudulentos e outras táticas.

## Conceitos: Scammers

- São indivíduos ou grupos que realizam scams. Eles podem usar várias técnicas de engenharia social e falsificação de identidade para enganar as pessoas e obter informações valiosas.

## Conceitos: **Malwares**

- Um termo genérico para programas maliciosos que podem incluir vírus, trojans, backdoors e spywares. Eles são projetados para danificar, controlar ou roubar informações dos sistemas infectados.

## Conceitos: Vírus

- Um programa malicioso que se espalha por meio da inserção de cópias de si mesmo em outros programas executáveis ou arquivos de dados. O objetivo principal dos vírus é danificar ou interromper o funcionamento normal dos sistemas infectados.

## Conceitos: Keyloggers

- São programas maliciosos que são usados para capturar as teclas digitadas em um dispositivo. Eles são frequentemente usados por criminosos cibernéticos para roubar senhas e informações confidenciais.

## Conceitos: Trojans

- Programas maliciosos que se disfarçam como software legítimo e são instalados pelos usuários sem o conhecimento de que eles estão infectando seus sistemas. Os trojans podem ser usados para roubar informações pessoais, como senhas ou dados bancários, ou para permitir que hackers acessem o sistema infectado remotamente.

## Conceitos: Backdoors

- Programas maliciosos que permitem que hackers acessem sistemas infectados remotamente, sem o conhecimento dos usuários. Eles geralmente são instalados por meio de trojans ou exploração de vulnerabilidades de software.

## Conceitos: Exploits

- É uma técnica que aproveita uma falha de segurança em um sistema ou software para executar um código malicioso ou obter acesso não autorizado. Os exploits são frequentemente usados em ataques de hacking.



## Conceitos: Rootkits

- É um tipo de malware que se oculta em um sistema operacional e permite que um invasor tenha acesso de root (ou seja, acesso completo) ao sistema. Os rootkits são frequentemente usados em ataques avançados de hacking, pois podem ocultar as atividades maliciosas do invasor e evitar a detecção pelos programas antivírus.

## Conceitos: **Spywares**

- Programas maliciosos que coletam informações pessoais dos usuários sem o seu conhecimento ou consentimento. Eles podem ser usados para coletar informações sobre hábitos de navegação, senhas, dados bancários e informações de identificação pessoal.

## Conceitos: **Worms**

- Programas maliciosos que se espalham por meio de redes de computadores, sem a necessidade de serem anexados a outros programas. Eles geralmente se espalham rapidamente e podem sobrecarregar redes, causando interrupções no funcionamento normal dos sistemas.

## Conceitos: **Adwares**

- Programas maliciosos que exibem anúncios invasivos nos sistemas infectados, geralmente sem o consentimento do usuário. Eles podem ser usados para direcionar os usuários para sites maliciosos ou para coletar informações sobre seus hábitos de navegação.

## Conceitos: **Bots**

- Programas maliciosos que permitem que hackers controlem remotamente sistemas infectados. Eles podem ser usados para lançar ataques DDoS, coletar informações pessoais ou instalar outros programas maliciosos.

## Conceitos: **Ransomwares**

- Programas maliciosos que criptografam os dados dos usuários e exigem o pagamento de um resgate para desbloqueá-los. Eles podem ser usados para extorquir dinheiro de empresas ou indivíduos.

## Conceitos: Sniffers

- Programas maliciosos que capturam e analisam o tráfego de rede em sistemas infectados. Eles podem ser usados para roubar informações pessoais, como senhas ou dados bancários.

## Conceitos: **MITM**

- Sigla para "Man-in-the-middle" ou "Homem-no-meio", é um tipo de ataque em que um hacker se posiciona entre duas partes que estão se comunicando, interceptando e manipulando as informações trocadas entre elas.



## Conceitos: **Brute force**

- Um método de ataque em que um hacker tenta adivinhar senhas ou chaves criptográficas por meio de tentativa e erro. Eles usam programas automatizados para testar combinações de senhas até encontrar a correta.

## Conceitos: DDoS (Distributed Denial of Service)

- Um ataque em que um grande número de solicitações é enviado para um servidor, tornando-o incapaz de responder a outras solicitações legítimas. Este ataque é realizado por meio de um grande número de dispositivos infectados (bots), que são controlados remotamente para enviar as solicitações ao mesmo tempo. O objetivo do ataque DDoS é derrubar o serviço ou sistema alvo.

## Conceitos: SQL Injection

- Um ataque que explora vulnerabilidades em aplicativos da web que utilizam bancos de dados para armazenar informações. O ataque ocorre quando um invasor insere códigos SQL maliciosos em campos de entrada do aplicativo, como um formulário de login, e faz com que o aplicativo execute esses códigos. Isso permite que o invasor acesse, modifique ou exclua informações do banco de dados.

## Conceitos: Cross-site Scripting (XSS)

- Um ataque que explora vulnerabilidades em aplicativos da web que não validam adequadamente os dados de entrada do usuário. O ataque envolve a inserção de código malicioso em uma página da web, que é então executado pelo navegador do usuário. O código malicioso pode ser usado para roubar informações de sessão, como cookies, ou redirecionar o usuário para um site falso.

## Conceitos: **Phishing**

- Um método de engenharia social em que os hackers criam sites falsos ou enviam e-mails fraudulentos para induzir os usuários a revelar informações pessoais, como senhas ou dados bancários.

## Conceitos: Phreaking

- Uma técnica que envolve a exploração de vulnerabilidades em sistemas de telefonia para fazer ligações ou obter acesso a recursos de rede sem autorização.
- Historicamente, o phreaking era usado para fazer ligações gratuitas ou de longa distância, mas hoje em dia é usado para realizar ataques a sistemas de telefonia e roubar informações pessoais dos usuários.

## Conceitos: Carding

- Uma técnica que envolve a compra, venda e uso de informações de cartão de crédito roubadas ou falsificadas. Os carders usam técnicas de hacking para obter acesso a informações de cartão de crédito, como números, datas de validade e códigos de segurança, e depois vendem essas informações a terceiros ou as usam para fazer compras fraudulentas..

## Conceitos: Engenharia reversa

- É o processo de desmontagem de um software ou dispositivo eletrônico para descobrir seu funcionamento interno e encontrar possíveis vulnerabilidades ou falhas de segurança. A engenharia reversa é legal quando realizada para fins de pesquisa ou desenvolvimento, mas pode ser ilegal se usada para atividades maliciosas.



## Conceitos: Descompilar

- É o processo de converter o código compilado de um software de volta para sua forma original, de código-fonte. A descompilação é frequentemente usada para fins legítimos, como entender como um software funciona ou realizar engenharia reversa para compatibilidade com outras plataformas. No entanto, também pode ser usada para fins maliciosos, como roubo de propriedade intelectual ou criação de versões piratas de software.

## Conceitos: **Descompilador**

- É um programa de computador que realiza o processo de descompilação. Os descompiladores geralmente exigem um conhecimento avançado de linguagem de programação e são projetados para converter o código compilado em um código-fonte legível e editável.

## Conceitos: Descriptografia

- É o processo de decodificar informações que foram previamente criptografadas, de modo que possam ser lidas e interpretadas. A descriptografia só é possível com o uso de uma chave específica, que deve ser conhecida apenas por pessoas autorizadas.

## Conceitos: Engenharia social

- Uma técnica que envolve a manipulação psicológica de usuários para obter acesso a informações confidenciais ou sistemas de computador. Os engenheiros sociais usam a persuasão, a intimidação, a lisonja e outros métodos para enganar os usuários e obter informações que podem ser usadas em ataques.
- Exemplos incluem phishing, pretexting, baiting e quid pro quo. A engenharia social é frequentemente usada em conjunto com outras técnicas de hacking, como malware ou exploração de vulnerabilidades, para maximizar o sucesso dos ataques.

## Conceitos: Pretexting

- Uma técnica de engenharia social em que o invasor se passa por outra pessoa para obter informações confidenciais. Isso pode envolver a criação de uma história falsa ou uma identidade falsa para ganhar a confiança da vítima e obter acesso a informações sensíveis.

## Conceitos: **Baiting**

- Técnica de engenharia social que envolve a oferta de algo atraente, como um dispositivo USB ou um download gratuito, para induzir a vítima a fornecer informações ou acessar um sistema comprometido.

## Conceitos: Quid pro quo

- Uma técnica de engenharia social em que o invasor oferece algo em troca de informações confidenciais ou acesso a um sistema. Isso pode incluir ofertas falsas de serviços ou suporte técnico em troca de informações de login ou outras informações confidenciais.

## Conceitos: Macros

- Ataques com macros são uma técnica comum de engenharia social usada por criminosos cibernéticos para disseminar malware. Macros são pequenos programas que podem ser executados dentro de aplicativos como o Microsoft Office. Ao abrir um documento infectado que contenha macros maliciosos, o usuário pode inadvertidamente ativar um código que instala malware em seu computador.



# Medidas de Defesa

- **Mantenha o software atualizado:**
  - É importante manter o sistema operacional e o software atualizados, pois as atualizações geralmente incluem correções de segurança.

# Medidas de Defesa

- **Use senhas fortes e diferentes para cada conta:**
  - Use senhas fortes e complexas, e evite reutilizar senhas para várias contas.

# Medidas de Defesa

- **Use autenticação de dois fatores:**
  - A autenticação de dois fatores adiciona uma camada adicional de segurança exigindo uma segunda forma de verificação, como um código enviado por SMS ou gerado por um aplicativo.

# Medidas de Defesa

- **Cuidado com phishing e e-mails suspeitos:**
  - Verifique sempre o remetente e o conteúdo dos e-mails antes de clicar em links ou fazer download de anexos. Nunca forneça informações confidenciais ou senhas por e-mail.

# Medidas de Defesa

- **Use software antivírus e anti-malware:**
  - Instale e mantenha atualizado um software antivírus e anti-malware.

# Medidas de Defesa

- **Não confie em dispositivos desconhecidos:**
  - Evite usar dispositivos USB ou outros dispositivos desconhecidos, pois eles podem conter malware ou outras ameaças.

# Medidas de Defesa

- **Mantenha backups regulares:**
  - Faça backups regulares dos seus dados para evitar a perda de informações em caso de ataque.

# Medidas de Defesa

- **Educação e treinamento:**
  - Eduque-se e treine sua equipe e familiares em práticas seguras de computação e em como identificar e evitar técnicas de engenharia social.



# Medidas de Defesa

- **Educação e treinamento:**
  - Eduque-se e treine sua equipe e familiares em práticas seguras de computação e em como identificar e evitar técnicas de engenharia social.

## Conceitos: Firewall

- Sendo uma solução conjunta de hardware e software, o firewall é um mecanismo de segurança que trabalha analisando e filtrando o fluxo de informações trocadas pela rede, é um mecanismo que serve como barreira para evitar comunicações não autorizadas.
- O objetivo básico do firewall é bloquear troca de informações indesejadas.

## Conceitos: **Firewall**

- Com base nos dados disponibilizados pelo usuário que cuida das redes, o firewall tanto de software quanto de hardware, trabalha realizando permissões ou bloqueios de conteúdos que vem das redes externas.

# Conceitos: Firewall

- Os firewalls possuem três tipos básicos de atuação, são eles:
  - Firewalls de filtragem de dados ou packet filtering.
  - Firewall de proxy.
  - Firewall de inspeção de estados.

## Conceitos: Firewall

- **Firewall em rede**
- Eles agem como um firewall de inspeção de dados, observando as trocas e criando registros para que eles sejam posteriormente vistos, se necessário. Normalmente eles são usados pela união do hardware com o software, o que gera uma proteção maior, onde todos os dados são observados com relação as duas facetas, eles observam diferentes tipos de conexão ou tentativa de conexão.

## Conceitos: Firewall

- **Firewall local**
- Conhecidos também como local firewalls, esse tipo de proteção trabalha com base em configurações previamente instaladas, onde, através delas, o acesso à rede local é limitado.
- Ele é utilizado, normalmente, em conjunto com o firewall de rede, já que este protege toda uma área enquanto o firewall local protege individualmente os computadores.

## Conceitos: VPN

- A sigla VPN significa, Virtual Private Network, ou, em português, Rede Privada Virtual, é mais um tipo de proteção quando tratamos de segurança na troca de dados. Ela trabalha com protocolos previamente definidos, chamados de “protocolo padrão”, os quais podem contribuir para a segurança ou não.

## Conceitos: VPN

- A sigla VPN significa, Virtual Private Network, ou, em português, Rede Privada Virtual, é mais um tipo de proteção quando tratamos de segurança na troca de dados. Ela trabalha com protocolos previamente definidos, chamados de “protocolo padrão”, os quais podem contribuir para a segurança ou não.



# Alguns Dados

**59,5%**

**População Mundial**

Com acesso à Internet (em 2021)

**53,4%**

**Dos utilizadores da Internet**

Estão localizados na Ásia, seguindo-se a Europa (14,3%), África (11,5%), América Latina (9,6%) e América do Norte (6,7%).

**65%**

**Taxa de penetração da Internet**

Sendo a América do Norte onde a taxa é maior (93,9%)..

**Tempo online?**

O utilizador médio da Internet (valores globais) passa 6h58 online todos os dias.



## Conceitos: Cibercrime

- Cibercrime é atividade criminosa cometida com computadores e/ou através de uma rede ou da Internet.
- Toda a atividade criminosa em que se utiliza de um computador ou uma rede de computadores como instrumento ou base de ataque.

## Conceitos: Ciberataque

- Ciberataque é qualquer tentativa de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um dispositivo.
- Um ataque cibernético é qualquer tipo de manobra ofensiva voltada para sistemas de informação de computadores, infraestruturas, redes de computadores ou dispositivos de computadores pessoais.

## Conceitos: Ciberguerra

- Modalidade de guerra em que a conflitualidade não ocorre com armas físicas, mas via meios eletrônicos e informáticos no chamado ciberespaço.

# Conceitos: Ciberterrorismo

- Ciberterrorismo é o uso da Internet para realizar atos violentos que resultam em, ou ameaçam, perda de vidas ou danos corporais significativos, a fim de obter ganhos políticos ou ideológicos por meio de ameaça ou intimidação.

# Conceitos: Computação Forense

- Computação forense é um ramo da ciência forense digital pertencente às evidências encontradas em computadores e em mídias de armazenamento digital.
- O objetivo da computação forense é examinar a mídia digital de uma maneira forense, com o propósito de identificar, preservar, recuperar, analisar e apresentar fatos e opiniões sobre a informação digital.

# Conceitos: Computação Forense

- Computação forense é um ramo da ciência forense digital pertencente às evidências encontradas em computadores e em mídias de armazenamento digital.
- O objetivo da computação forense é examinar a mídia digital de uma maneira forense, com o propósito de identificar, preservar, recuperar, analisar e apresentar fatos e opiniões sobre a informação digital.

## Conceitos: Pentest

- O teste de intrusão (do inglês "Penetration Test" ou pentest"), também traduzido como "teste de penetração", é um método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de uma fonte maliciosa.
- O processo envolve uma análise nas atividades do sistema, que envolvem a busca de alguma vulnerabilidade em potencial que possa ser resultado de uma má configuração do sistema, falhas em hardwares/softwarewares desconhecidas, deficiência no sistema operacional ou técnicas contramedidas.



# Conceitos: Pentest

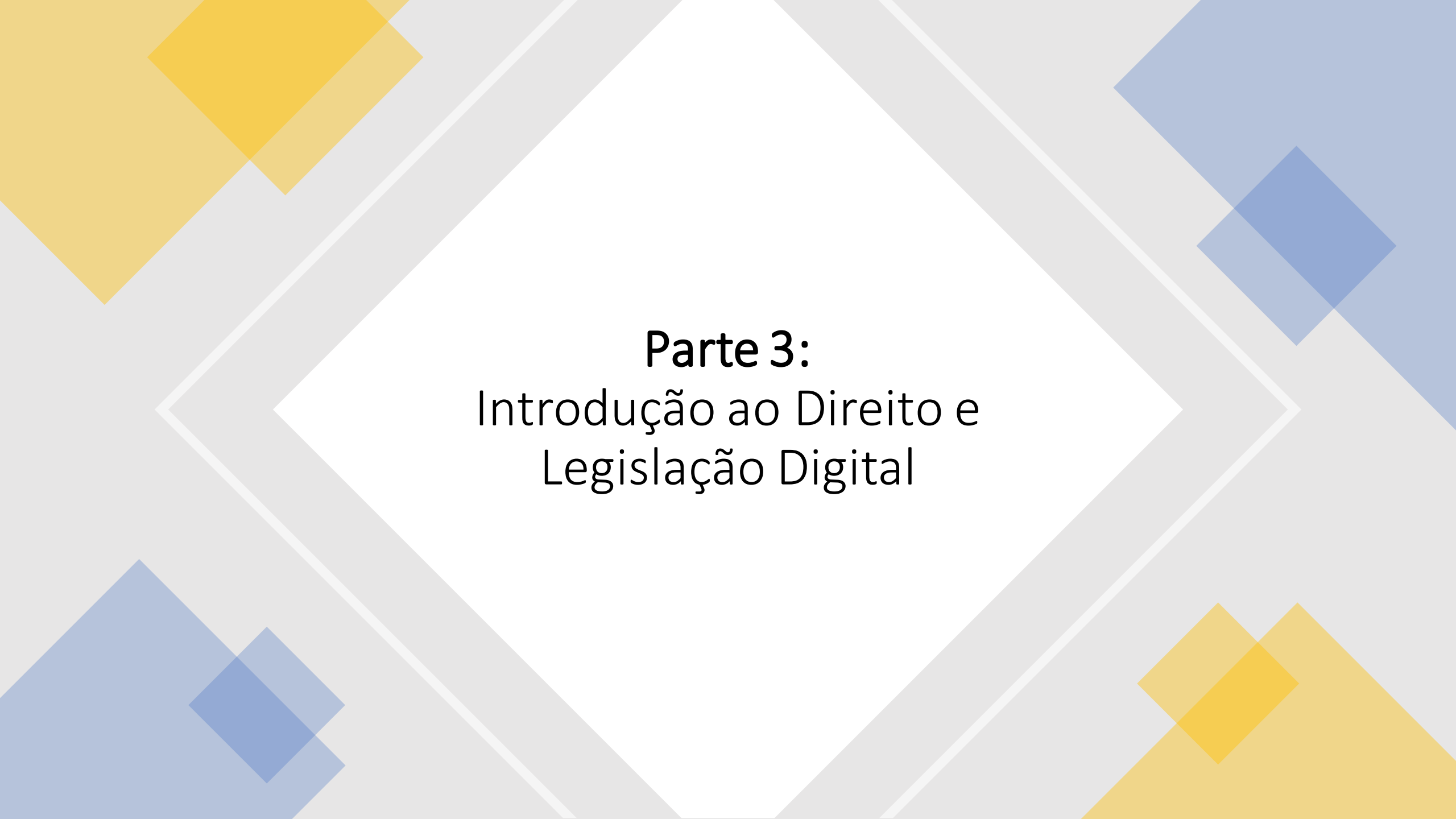
- **Teste da Caixa Branca**
  - Assume que o testador possui total conhecimento da infraestrutura a ser testada, incluindo o diagrama da rede, endereçamento IP e qualquer informação complementar.

# Conceitos: Pentest

- **Teste da Caixa Preta**
  - Assume que não existe qualquer conhecimento prévio da infraestrutura a ser testada. Sendo que o primeiro teste deve determinar a localização e extensão dos sistemas antes de iniciar a análise.
  - Simulam um ataque de alguém que esteja familiarizado com o sistema, enquanto um teste de caixa branca simula o que pode acontecer durante o expediente de um trabalho ou depois de um "vazamento" de informações, em que o invasor tenha acesso ao código fonte, esquemas de rede e, possivelmente, até mesmo de algumas senhas.

## Conceitos: **Pentest**

Testes de caixa preta simulam um ataque de alguém que esteja familiarizado com o sistema, enquanto um teste de caixa branca simula o que pode acontecer durante o expediente de um trabalho ou depois de um "vazamento" de informações, em que o invasor tenha acesso ao código fonte, esquemas de rede e, possivelmente, até mesmo de algumas senhas.



# **Parte 3:**

## Introdução ao Direito e Legislação Digital



Fim do Módulo