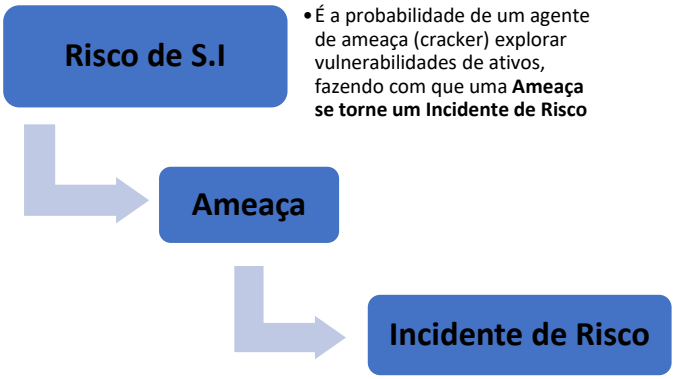
- # Segurança da Informação

- **S.I** → envolve **Identificação, proteção, detectação, resposta e recuperação** e atendem os princípios do CID
- **Norma ABNT ISO/IEC 27002** → Define toda Segurança da Informação. É a única certificada.
- A proteção de três pilares/princípios é a razão da segurança da Informação → **CID** ← **Família ABNT NBR ISO/IEC 27000**
- **CONFIDENCIALIDADE** → Proteção de uma informação com acesso apenas a determinadas pessoas. (Incidente é percebido só depois)
- **INTEGRIDADE** → Informações devem se manter integras do início ao fim, não podem sofrer qualquer tipo de modificação. (Incidente é percebido só depois)
- **DISPONIBILIDADE** → A garantia de que estará à disposição dos usuários sempre que eles precisarem. (Incidente é percebido na hora)

  Outros pilares tão importantes quanto.

- **Autenticidade** → Garantir que determinada pessoa ou sistema é, de fato, quem ela diz ser.
- **Não-Repúdio (Irretratabilidade)** → Busca-se garantir que o usuário não tenha condições de negar ou contrair o fato de que foi ele quem gerou determinado conteúdo ou informação.
- **Legalidade** → O aspecto de legislação e normatização.

- # Elementos do risco




**Ativo** → É quem possui elementos de riscos, quem deve ser protegido

**Agente de ameaça** → Quem explora a vulnerabilidade (ponto fraco). Ex.: cracker

**Agente de ameaça** → Pode ser também uma situação/método que acidentalmente ficou vulnerável devido a um erro de configuração do adm. ao servidor, por exemplo.

**Vulnerabilidade** → Falha / Fraqueza em procedimentos de segurança. **Porta aberta** para ameaças.

**Vulnerabilidade Tecnológica** → Ataque feito por **Exploits** que são softwares que utilizam dados ou códigos próprios que exploram as fraquezas de ativos.

**Shellcode** → Código malicioso escrito em assembly injetado em um programa para realizar ações maliciosas. Quando uma Shell é aberta ela dá total acesso do sistema ao invasor.

**Controles de segurança ou Mecanismos de defesa** ➔ aplicados em vulnerabilidades para evitar do agente de ameaça explorar.

**Ameaça** → Algo que pode acontecer -- **é o potencial de um agente de ameaça explorar uma vulnerabilidade** específica, acidental ou interinamente. Exemplo de ameaças: Negação de Serviço e Vazamento de Informações.

**Incidente de segurança** ➔ Quando a ameaça de fato ocorre.

Cálculo da probabilidade de isso tudo ocorrer representa o risco.

**Risco = Probabilidade x Impacto**

- ## Controles de Segurança

**Mecanismo de defesa e Segurança de Rede ->** São definições e implementações de controles de segurança que visam a proteção e prevenção contra riscos identificados, analisados e avaliados.

**Conjunto de controles de segurança** ➔ Parte da estratégia de segurança para prevenção e pode ser composto por processos, como **Gestão de Identidade e Acessos** ➔ Gerenciamento de contas e senhas dos usuários, controle essencial, pois ocorrem muitos incidentes de segurança para obtenção de dados.

**Controles de Segurança, podem ser** → **Físicos =** Câmeras de vigilância, Alarmes, Guardas || **Tecnológicos =** Antivírus, firewall, criptografia, etc... || **Processos =** Políticas de Segurança, conscientização de segurança e privacidade...

**CERT.br** ➔ Grupo de Resposta a Incidentes de Segurança para internet no Brasil, é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à internet.

**Definição para os incidentes de seguranças reportados ao CERT.br**

- **Worm** → Processo automatizado de propagação de códigos maliciosos na rede
- **DoS** → Ataque de negação de serviço, deixa o servidor/usuário com sistema indisponível
- **Invasão** → Ataque bem sucedido, acesso não autorizado a um computador ou rede
- **Web** → Comprometimento de servidores Web ou desconfigurações de páginas
- **Scan** → Varreduras em redes com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles e suas vulnerabilidades.

- **Fraude** → Qualquer ato enganoso, de má-fé com o intuito de lesar outrem. Incidentes em que ocorre uma tentativa de se obter vantagem.
- **Outros** → Qualquer notificação que não se enquadra nas categorias anteriores

** Como tudo passa pela rede e a aplicação está na camada 7 da pilha de protocolos TCP/IP, o portal de fornecedores está sujeito às vulnerabilidades de rede e de hardware.**

Pontos do ataque que devem ser avaliados de acordo com o ESTADO DA INFORMAÇÃO.

- **Dados em processamento (DIU – Date-In-Use) ->** Ataques mais sofisticados
- **Dados em transmissão (DIM – Date-In-Motion) ->** Ataques à rede
- **Dados Armazenados (DAR – Date-At-Rest) ->** Ataques a banco de dados.

**LGPD – Lei Geral de Proteção de Dados** ➔ Dados pessoais devem ser protegidos para a garantia da privacidade. Ataques para vazar dados pessoais e comprometer a privacidade, ataques podem ocorrer com DIU, DIM, DAR.

**SEGURANÇA – AGENTES DE AMEAÇA, AMAEAÇAS E TÉCNICAS DE ATAQUES**

**Agentes de ameaças** ➔ elementos importantes para o entendimento dos riscos e da segurança ➔Mais comuns são **pessoas** (crackers); **Agentes de ameaça naturais** (terremotos, tempestades, inundações de datacenter – instalação que abriga servidores ou equipamentos de computação, etc); Os **Malwares ou Código malicioso** (programa malicioso) também são agentes de ameaça bastante crítico, vírus e worms são exemplos.

**Vírus** → Código malicioso que contamina um sistema a partir de uma ação do usuário. Ex.: Clique em um link contaminado; instalação de um software suspeito.

**Worm** → Código malicioso que se propaga nas redes em busca de vulnerabilidades do sistema operacional, contaminando e se espalhando SEM a necessidade de ação humana.

**Cavalo de Tróia** → Disfarçado de programa ou arquivo legítimo, engana os usuários e infecta seus sistemas, como **KEYLOGGER** captura o que o usuário digita e envia os arquivos para o cracker.

**Keylogger** → Malware que registra TUDO que é digitado, ataque bastante comum que rouba credenciais de acesso a bancos.

**Backdoor** → Código malicioso que permite o acesso remoto não autorizado ao sistema, muitas vezes sem ser percebido. Ele explora vulnerabilidades como firewall ou softwares desatualizados, pela abertura de portas de um servidor, do roteador e firewall.

**MALWARE CRÍTICO - Ataque de Ransomware** → Sequestram dados de servidores e usuários com o uso de criptografia e exige resgate. O criminoso cifra os arquivos ou o disco e exige o pagamento de um resgate em troca da chave criptográfica que decifra as informações originais.

- **Princípio da Segurança comprometido:** Disponibilidade
- **Possível controle de segurança:** Backup

**Ataque – DoS e DDOS** ➔ Deixam indisponível o servidor/sites → Negação de serviço que torna um sistema indisponível. Exemplo: ataque feito por meio do bombardeamento de solicitações, impossibilitando usuários de utiliza-los. Ambos comprometem a **Disponibilidade da Informação**

- **DoS** → Ataque feito por apenas um invasor que envia vários pacotes.

- **DDoS** → Ataque distribuído e coordenado, que parte de várias máquinas contra um alvo. No DDoS um hacker comanda máquinas chamadas de **Masters**, essas Masters comandam outras máquinas chamadas de **Daemons,** são elas que realizam efetivamente o ataque a vítima.

**SYN Flooding (Técnica típica de DoS) ->** causa o **overflow** (transbordamento – quando um valor que precisa ser guardado é maior do que o espaço que temos) da pilha de memória e **Smurf ->** envio de pacotes específicos.

**MITM (Ataque do homem do meio)→** Sequestro de conexões e é ativo, acontece em tempo real, com a gente de ameaça controlando e redirecionando as conexões TCP para determinada máquina, esse ataque compromete a CID. Muito usado com o protocolo HTTP, com o HTTPS é mais complicado.

- **Ataque de Dos e DDoS** comprometem a Disponibilidade da Informação
- **Ataque envolvendo Malware ou MITM** comprometem além da disponibilidade, a confidencialidade e a integridade da informação – CID

Problema de autenticação dos usuários -> Descoberta de senhas com o uso de técnicas como **ATAQUE DE DICIONÁRIO** (palavras de dicionários são testadas) e **ATAQUE DE FORÇA BRUTA – BRUTE FORCE** (Diferentes combinações de caracteres são testadas) e para evitar podemos usar o mecanismo de segurança que trava as tentativas de acesso depois de um determinado número de tentativas de senhas inválidas.

- **<u>Controles de segurança e Proteção</u>**

Melhor local para controles de segurança é no **fluxo da informação** → uma boa estratégia de segurança é analisar qual a estrutura de rede mais segura considerando um pedaço dessa rede, uso de **zonas desmilitarizadas (DMZ) -> controle de acesso de rede e detectação de ataques.** → técnica usada entre a rede pública e a rede interna, camada de segurança que ajuda a proteger a rede interna, mantendo os serviços públicos em uma rede separada e isolada.

**DMZ** é proteger a rede privada, mantendo serviços públicos como servidores de e-mail, web e FTP fora da rede principal. Esses serviços são colocados na DMZ para que os usuários da internet possam acessá-los sem ter acesso à rede privada.

**Firewall (guarda)** → Controle de segurança mais famoso responsável pelo controle de acesso à rede, ele filtra tudo aquilo que não é permitido. C<u>omeçou funcionando na camada de rede e hoje atua também na aplicação</u> contra ataques e trabalha junto com o WAF (Web Application Firewall), o **firewall** filtra o tráfego de rede baseado nos cabeçalhos dos pacotes e o **WAF** filtra e monitora o tráfego entre os usuários e a Web, na camada e aplicação HTTP.

- Principais desafios do uso do firewall é a sua configuração, composta por regras que consideram, pelo menos **diferentes segmentos de rede, serviços disponibilizados pela empresa** e os **serviços que podem ser acessados pelos usuários internos.**
- Aplicação Microsoft Terminal Services – **REMOTE DESKTOP PROTOCOL** →Serviço disponibilizado pelo Windows para acesso remoto. O firewall libera a porta TCP 3389 para que o RDP funcione.
- **Scan de portas** → Técnica usada para encontrar portas abertas e, dessa forma, uma vulnerabilidade na rede ou sistema.

**IDS (Sistemas de Detectação de Intrusão)** → controle de segurança que analisa diferentes informações, como conexões, logs e os fluxos de dados para detectar ataques em andamento, em tempo real. **É o complemento ideal para o firewall.**

- Monitora e Detecta ataques em andamento
- Emite um alerta
- Sua análise é baseada em assinaturas de ataques conhecidos

**IPS (Sistemas de Prevenção de Intrusão)** → Evolução do IDS, bloqueia atividades maliciosas em tempo real, ideal para quem deseja uma camada adicional de segurança para bloquear atividades maliciosas em tempo real.

- Monitora o tráfego de rede em busca de atividades suspeitas
- Quando detecta, bloqueia/derruba a atividade
- Atual de forma in-line, similar ao firewall
- Utiliza técnicas de IA para diminuir a quantidade de alarmes falsos e ataques não detectados

**Endpoints** → Qualquer dispositivo móvel ou não, conectado a uma rede privada ou corporativa, que transmite e recebe dados e informações

**Antimalware** → Busca códigos maliciosos, evita que sejam instalados na máquina.

**OBS.** Cada medida de proteção **sozinha não funciona**, é preciso fazer uma **camada** delas.

**Autenticação** → Um dos principais controles de segurança ao validar a identidade dos usuários, a fim de que possam ter acesso aos recursos.

**3 Fatores da Autenticação/ Validação de ID** → Algo que o usuário **sabe**, **possui** e **é**.

**Autenticação de Duplo Fator ou Múltiplo Fator** → Quando dois fatores diferentes de autenticação são usados. Ex.: Senha e SMS

Em segurança é preciso considerar aspectos de **USABILIDADE** e o **NÍVEL DE SEGURANÇA REQUERIDOS PARA CADA CASO.**

**Controle de conteúdo** → Controle de segurança para filtrar o acesso a conteúdo impróprio ou que levam a perda de produtividade.

## • Criptografia

- É ocultar o significado de uma mensagem.
- Evoluiu de uma arte para uma ciência
- Arte de escrever ou resolver códigos
- **Antes** era pra comunicação secreta e **Hoje** é para autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas.....
- A criptografia básica pode ser simétrica ou de chave privada, são de chave secreta (única chave para cifrar/decifrar) e possuem cifragem com algoritmos matemáticos (Mais seguro).

- **<u>Objetivos da Criptografia</u> – C.I.A.N**

**Sigilo** → Proteção dos dados contra divulgação não autorizada

**Autenticação** → Garantia de verificação da identidade do remetente ou da fonte de um dado

**Integridade** → Garantia de que as informações não sejam alteradas durante a transmissão

**Não-Repúdio** → Garantia que não se pode negar a autoria de uma mensagem

**Anonimato** → Garantia de não rastreabilidade de origem de uma mensagem

- **Confidencialidade** → Só o destinatário pode/deve ter acesso aos dados da mensagem
- **Integridade** → O destinatário deve saber se a mensagem foi alterada na transmissão
- **Autenticidade** → O destinatário deve ter a certeza de que foi o remetente quem realmente enviou a mensagem
- **Não-Repúdio** → O remetente não pode negar o envio/autoria da mensagem

**Cifra de César** → Consiste na substituição simples de letras do alfabeto por letras avançando algumas letras na sequência. Ex. Em uma troca de 3 -> **A** seria **D**, **B** seria **E, C** seria **F**

A **Segurança dos sistemas criptográficos** se dá pela →

- geração aleatória de trocas de chaves, quanto maior a frequência da troca, maior segurança terá.
- O tamanho das chaves são diferentes para criptografia de chave privada ou simétrica e para a criptografia de chaves públicas ou assimétricas.
- A criptografia é baseada em técnicas que incluem a cifragem, funções de hash e assinaturas digitais e a escolha delas depende de critérios de nível de segurança, métodos de opção dos algoritmos, desempenho, facilidade de implementação.

- **Para criptografar/descriptografar precisamos de** → Algoritmo, chave - Um algoritmo é utilizado com várias chaves (não ao mesmo tempo). As chaves devem ser mudadas com frequência para uma maior segurança.

- **Tipos de Criptografia**

  - **Criptografia de chave privada / Simétrica →**

    - A chave usada para cifrar a mensagem é a mesma utilizada para decifrar
    - A chave deve ser mantida secreta pelo remetente e destinatário
    - Um canal seguro deve ser utilizado para transmissão da chave
    - Algoritmo de Chave simétrica -> DES
    - É mais rápida

- **Criptografia de chave pública ➔**

    - remetente tem chave pública e destinatário tem chave privada
    - Sempre que uma chave privada é gerada, uma pública correspondente também descer ser criada
    - Algoritmo de Chave Assimétrica -> RSA
    - É mais lenta

**Criptografia RSA ➔** A criptografia RSA baseada em números primos (fatoração), é considerada uma das mais seguras e seu algoritmo foi o primeiro a possibilitar a assinatura digital.

**Esteganografia ➔** Técnica que oculta uma mensagem dentro de outra ou de uma imagem

**Criptografia ➔** Técnica que oculta o significado de uma mensagem

**Assinatura Digital ➔** conjunto de chaves, algoritmos de assinatura digital, hashs que fazem verificação a autenticidade e integridade de documentos e mensagens eletrônicas. É baseada em um processo matemático que usa chaves públicas e privadas para gerar e verificar a assinatura.

**Criptografia Hash ➔** Criptografa os dados quando enviados para poder ser comparado com os dados recebidos e garantir a integridade dos dados.

---

A criptografia hash é uma técnica que converte dados de qualquer tamanho em uma sequência de caracteres de comprimento fixo, chamada de hash. **O objetivo principal dessa técnica é garantir a integridade dos dados, permitindo verificar se houve alterações nos mesmos.**
Um algoritmo de hash recebe os dados de entrada e aplica uma série de cálculos matemáticos complexos para produzir o hash resultante. Esse hash é único para cada conjunto de dados, o que significa que até a menor alteração nos dados de entrada resultará em um hash completamente diferente.

- A criptografia hash possui algumas características importantes:

    - **Integridade dos dados:** Se qualquer parte dos dados originais for modificada, o hash resultante será completamente diferente, permitindo detectar alterações não autorizadas.
    - **Tamanho fixo:** O tamanho do hash é sempre o mesmo, independentemente do tamanho dos dados de entrada. Isso é útil, pois permite comparar hashes rapidamente, mesmo para grandes quantidades de dados.
    - **Irreversibilidade:** É computacionalmente inviável reverter o processo de hashing para obter os dados originais a partir do hash. Isso significa que não é possível reconstruir os dados originais apenas com o hash.

A criptografia hash é amplamente utilizada em várias aplicações, como segurança de senhas, verificação de integridade de arquivos, autenticação de mensagens e autenticação de identidades digitais. Alguns exemplos de algoritmos de hash populares incluem **o MD5, SHA-1, SHA-256 e o bcrypt.**

---

- **POLÍTICA E CULTURA DA SEGURANÇA**

**CYBERSECURITY, CIS CONTROLS E FAMÍLIA NBR ISO/IEC 27.000**

- Família **NBR ISO/IEC 27000**
  NBR ISSO/IEC 27002 -> Foca nos objetivos de controle de segurança. Única certificada.
- **Cybersecurity Framework** do National Institute of Standards and Technology (**NIST** - Instituto Nacional de Padrões e Tecnologia) ➔ Abordagem integrada de diferentes aspectos de segurança
- **CIS Controls** do Center for Internet Security (CIS – Controle de Segurança da Internet) ➔ Estabelece forma mais prática de trabalho

Conjunto de frameworks e normas que guiam as ações de Segurança da Info. ➔ São aspectos normativos e de cultura da segurança da informação que tratam de forma integrada.

A segurança é um conjunto de **Pessoas + Processos + Tecnologia**

Segurança da informação é direcionada também por **aspectos legais, regulatórios e contratuais**

- Segurança da informação é crucial para proteger dados sensíveis.
- Aspectos legais, regulatórios e contratuais **são relevantes** para a segurança da informação.
- No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) é uma lei importante nesse contexto.
- A lei Carolina Dieckmann e o Marco Civil da Internet também são relevantes para a segurança da informação no país. Essas leis estabelecem diretrizes e responsabilidades para proteger dados pessoais e regular o uso da internet.

## Certificação do SGSI

- **A ABNT NBR ISO/IEC 27001** é a norma que regula a certificação do Sistema de Gestão de Segurança da Informação (SGSI) de uma empresa. A norma tem como objetivo estabelecer os controles de segurança necessários para garantir a proteção dos dados. **Única norma que possui certificação → 27001**
- **Cybersecurity Framework ➔** é uma abordagem integrada que abrange diversos aspectos da segurança
- **CIS Controls ➔** oferece uma forma mais prática de trabalho.

**Cybersecurity Framework, do NIST**

- Ferramenta para organizar e melhorar seu programa de segurança cibernética. É um conjunto de diretrizes e práticas recomendadas para ajudar as organizações a criar e melhorar sua postura de segurança cibernética.
- Descreve a postura da segurança cibernética atual, descreve objetivos, identifica oportunidades, avalia os progressos, comunica os riscos, faz uma avaliação de tudo que está acontecendo dentro da empresa, o que pode melhorar, revisto, evoluído, ele faz um retrato total.
- Organiza diferentes elementos da segurança da informação e tem foco no uso de direcionadores de negócios para guiar atividades de segurança cibernética considerando os riscos. Ele se baseia em foco e ações em TODOS os níveis de segurança da empresa.

Gestão de Risco – CYBERSECURITY FRAMEWORK

- **Nível Executivo / Alta Gestão**

Foco → Riscos organizacionais
Ação → Expressa prioridade, aprova implementações, decisões sobre riscos

- **Nível Negócios / Processos**

Foco → Gerencia riscos do ambiente
Ação → Nomina implementações, desenvolve perfis, aloca orçamentos

- **Nível Implementação / Operações**

Foco → Implementa a segurança no ambiente
Ação → Implementa o que foi definido e aprovado

- As três partes do Cybersecurity Framework são:
  - **Núcleo (Framework Core)→** Representa os resultados desejados de segurança cibernética organizados em uma hierarquia e alinhados a orientações e controles mais detalhados que suportam as cinco funções do gerenciamento de risco.
  - **Camada de Implementação →** que proveem um mecanismo para ver e entender as características da abordagem para o gerenciamento de riscos da organização, para priorizar e alcançar os objetivos de segurança da informação. As camadas vão de **parcial (Tier 1)** a **adaptativo (Tier 4**), refletindo as respostas informais e reativas iniciais até a agilidade e a resposta formal baseada na visão de riscos
  - **Perfis →** são os alinhamentos de padrões, guias e práticas em um cenário de implementação. Os perfis podem identificar as oportunidades de melhoria da postura de segurança, comparando um perfil atual (“as is”) com um perfil alvo (“to be”).

- Esse framework trabalha com os elementos importantes para as atividades destes 3 níveis, que inclui os **objetivos, as priorizações, orçamentos, métricas e comunicação**
- Possui **5 funções →** Identificar, proteger, detectar, responder e recuperar (Têm uma visão estratégica do ciclo de vida dos riscos de segurança)
- As funções possuem **23 categorias** que abrangem resultados cibernéticos, físicos, pessoais e comerciais
- E são em **108 subcategorias** que são orientações para criar/melhorar um programa de segurança cibernética.

**CIS CONTROLS, DO CENTER FOR INTERNET SECURITY (CIS)**

- Ele trabalha para minimizar os ataques mais comuns contra sistemas e rede
- Tem o **objetivo de melhorar o estado de segurança da empresa**, ele faz um controle em camadas.
- Possui as seguintes características: **O ofensivo direciona a defesa / Priorização / Medidas e métricas / Diagnóstico e mitigação contínua / Automação**
- Consiste em 153 proteções divididas em 18 controles de segurança, com 3 grupos de implementações bem definidos, sendo eles classificados de acordo com o tamanho da empresa

  - **IG1 - Controles higiênicos, que protegem contra ataques comuns** → Empresas familiares com 10 funcionários
  - **IG2 - Controles para empresas com equipes de segurança** → Organização regional
  - **IG3** - **Controles contra adversários sofisticados** → Grande corporação com milhares de funcionários

- **PRINCIPAIS NORMAS E PADRÕES**

  - **Segurança da informação** → ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013
  - **Riscos** → ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011
  - **Continuidade de negócios** → ABNT NBR ISO/IEC 27031:2015 e ABNT NBR ISO 22301:2013
  - **Governança de TI** → COBIT
  - **Serviços de TI** → ITIL

- **FAMÍLIA ISO 27.000 – ISO 27.001**

  - **É a única que pode ser certificada** e quem faz as certificações é um auditor líder
  - Fornece um roteiro passo a passo para garantir que a empresa tenha medidas de segurança adequadas que protejam informações importantes das ameaças internas e externas.
  - Os sistemas de gestão **NÃO** são tecnológicos ou necessariamente automatizados.
  - É no seu sentido mais amplo, com o SGSI incluindo estratégias, planos, políticas, medidas, controles e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar, manter e melhorar a segurança da informação.

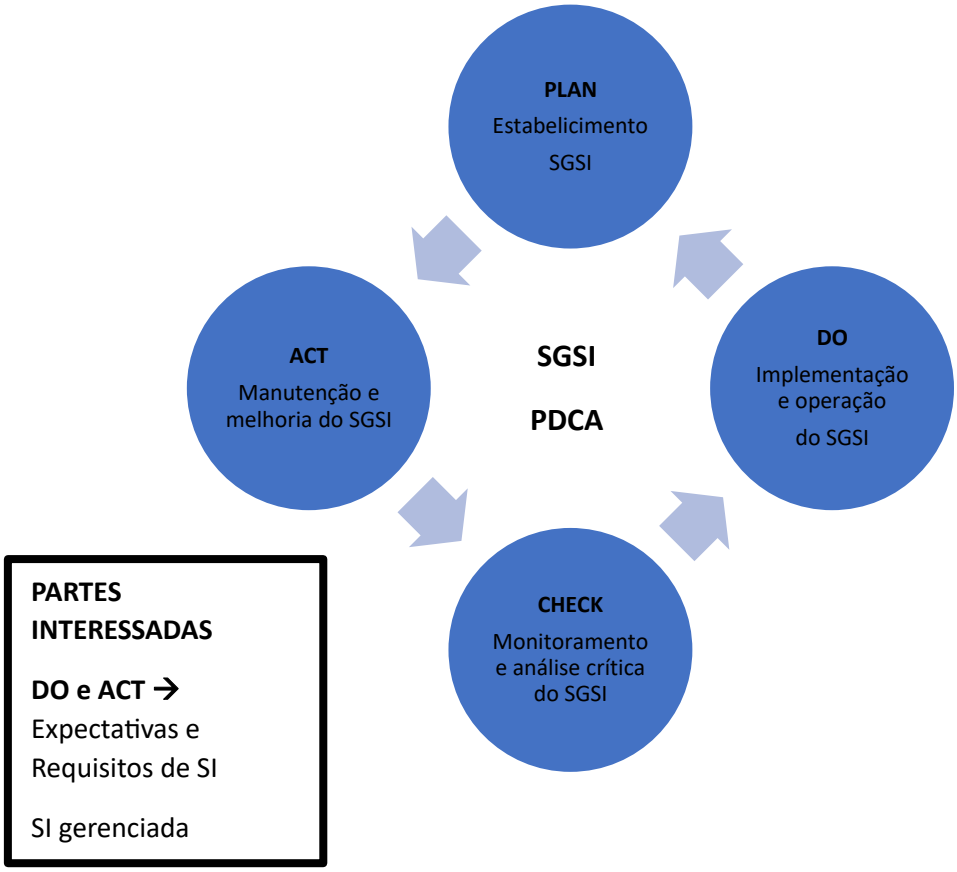
- **FAMÍLIA ISO 27.000 – ISO 27.002**

    - **Focada em definir os controles de segurança de informação**, de uma forma geral ela trabalha com análise de risco, aplicabilidade dos controles de segurança.
    - **Recomenda-se o bloqueio total de acesso as informações.**
    - Objetivos de controles de segurança da informação

↓↓↓↓


- **<u>SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)</u>**

    - SGSI -> Elemento chave para a **cultura da Segurança da Informação** -> Fazer **TODAS** pessoas entenderem que a S.I é de extrema importância.
    - A norma ABNT NBR ISO/IEC 27001 é quem estabelece os requisitos de um SGSI
    - **É um conjunto de políticas, procedimentos, diretrizes e práticas criado para preservar informações da empresa**. Preserva o CID da informação através da aplicação de uma gestão de riscos e fornece confiança de que esses riscos estão sendo bem gerenciados.
    - Especificar e implementar o SGSI de acordo com as características da sua organização
    - Algumas de suas características:
        - ✓ Abordagem baseada em riscos
        - ✓ Envolvimento da Alta Direção -> Liderança apoiar e promover a cultura
        - ✓ Política de Segurança da Informação
        - ✓ Controles de Segurança da Informação
        - ✓ Monitoramento e Revisão
        - ✓ Melhoria contínua
    - Como evoluem com o tempo é necessário estabelecer, implementar, manter e melhorar continuamente um SGSI
    - Uma das principais características do SGSI → **Processo de melhoria contínua ou PDCA (Plan, Do, Check, Act)**




- **<u>Requisitos do SGSI</u>**

- ✓ Contexto da organização
- ✓ Liderança
- ✓ Planejamento
- ✓ Apoio
- ✓ Operação
- ✓ Avaliação de desempenho
- ✓ Melhoria

- **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD**

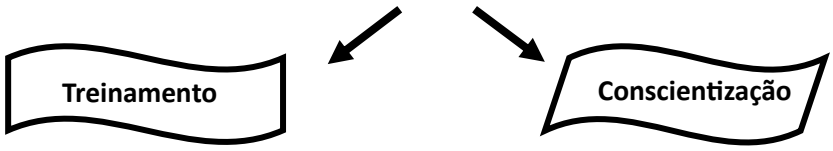
  - Os dados podem ser coletados desde que **mediante finalidade e base legal**
  - A empresa que trata dos dados pessoas é a responsável pelos dados coletados e os deve proteger. Para mantê-los deve implementar controles de segurança da informação para evita incidentes que podem levar ao vazamento de dados pessoais
  - **Lei N. 12.965 - Marco Civil da Internet** → Lei que regula o uso da internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa e para a atuação do Estado.
  - **Lei N. 12.737 – Lei Carolina Dieckmann** → Altera o código penal, tornando crime a invasão de aparelhos eletrônicos para obtenção de dados particulares, interrupção de serviço telemático ou de informática de utilidade pública.

- **POLITICA DE SEGURANÇA DA INFORMAÇÃO**

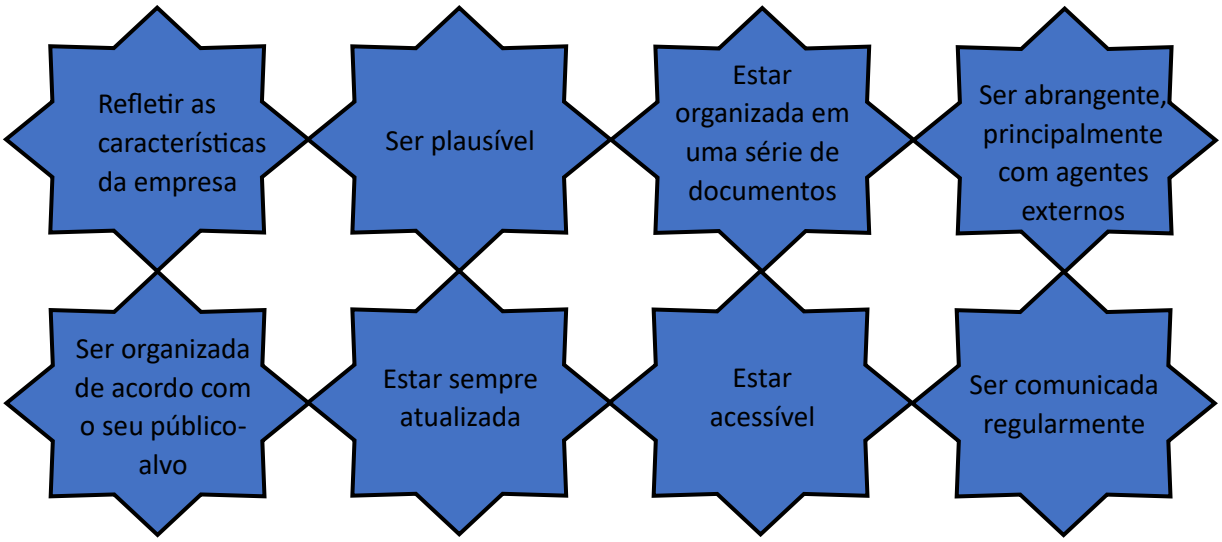
  - As políticas de segurança constituem um dos principais controles de segurança da informação
  - Guiam as ações de todos da organização, incluindo os terceiros, prestadores de serviços, parceiros e fornecedores com a definição de elementos como regras, orientações, diretrizes, responsabilidades e sanções.
  - Ela deve tratar de todos os aspectos cotidianos da organização, incluindo processos, as pessoas e as tecnologias

- **CULTURA DE SEGURANÇA**

  - Toda empresa possui sua própria cultura de segurança e é baseada em hábitos, crenças e conhecimentos, para que essa cultura seja fortalecida
  - O fortalecimento da cultura de segurança deve ter a participação da alta direção, para todos verem o quão importante ela é



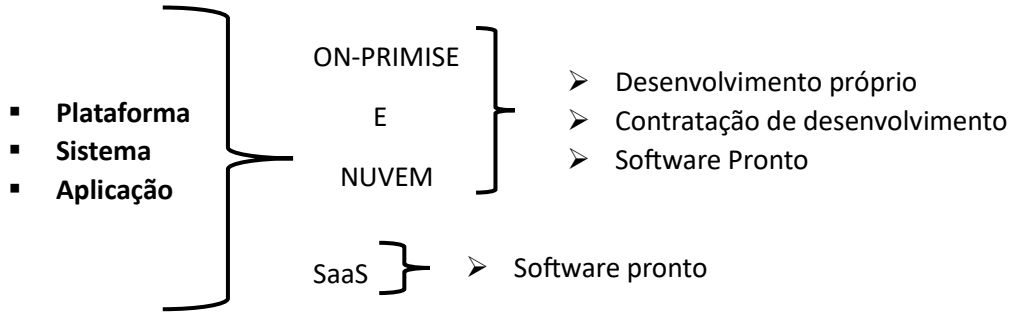

- **POLITICA DE SEGURANÇA E PRICAVIDADE deve:**



- **Termo de Contrato ou Confidencialidade** → um acordo legal entre as partes para estabelecer a obrigação de manter informações confidencias em sigilo, seu objetivo é proteger informações sensíveis de serem divulgadas a terceiros.

- **<u>Segurança da Informação na aquisição e desenvolvimento de sistemas</u>**

  - Há diversas alternativas e refletem diretamente em como a segurança e privacidade devem ser tratadas por sua empresa, principlamente quanto as responsabilidades.




  - **<u>Análise de segurança em diferentes níveis</u>**

    - **SAST – Análise estática** → Teste aplicado no **código-fonte**, remove vulnerabilidades/erros do código antes do software entrar em produção
    - Não requer um sistema em execução para realização avaliações
    - Implementado desde as primeira linhas de código e segue por todas as etapas
    - Teste de white box (caixa branca) – verificar a estrutura interna do software

    - **DAST – Análise dinâmica** → Teste aplicado com o **código em execução**, deve ser realizado antes do software entrar em produção.
    - pode ser usado para complementar a análise estática
    - Teste de black box (caixa preta) – verificar a estrutura externa (funcionalidades) do software

    - **IAST – Análise interativa** → Teste de forma interativa, combinando os testes estáticos e dinâmicos SAST e DAST

  - **<u>Modelos de contratação em nuvem</u>**

    - **IaaS – Infraestrutura como Serviço** → oferece uma infraestrutura de TI automatizada e escalonável – armazenamento, hospedagem, redes – de seus próprios servidores globais, cobrando apenas pelo o que o usuário consome. Desta forma, em vez de adquirir licenças de software ou servidores próprios, as empresas podem simplesmente alocar recursos de forma flexível a partir das suas necessidades.

- **PaaS – Plataforma como Serviço** → Fornecem todos os conceitos básicos da IaaS, assim como as ferramentas e recursos necessários para desenvolver e gerenciar aplicativos com segurança sem precisar se preocupar com a infraestrutura. Os servidores que hospedam sites são exemplos de PaaS.
- **SaaS – Software como Serviço** → É o local onde um software é hospedado por terceiros e pode ser acessado pela web, geralmente bastando um login. Por esse modelo, a empresa contrata um plano de assinatura e utiliza os programas necessários para os negócios. Neste sentido, o SaaS é muito mais interessante para o uso de aplicativos específicos, como os de gestão de relacionamento com o cliente (CRM).

- **<u>CICLO DE VIDA DE DESENVOLVIMENTO SEGURO</u>**

  - **TREINAMENTO**
    - Treinamento de segurança
  - **REQUISITOS**
    - Estabelecimento de requisitos de segurança
    - Criação de pontos de qualidade e bug bars
    - Avaliação dee riscos de segurança e privacidade
  - **CONCEPÇÃO (DESIGN)**
    - Estabelecimento de requisitos de design
    - Análise de superfície de ataques
    - Modelagem de ameaças
  - **IMPLEMENTAÇÃO**
    - Uso de ferramentas aprovadas
    - Desaprova funções inseguras
    - Análise estática
  - **VERIFICAÇÃO**
    - Análise dinâmica
    - Testes de Fuzz
    - Revisão de superfície de ataques
  - **LANÇAMENTO**
    - Plano de resposta a incidentes
    - Revisão final de segurança
    - Formalização do lançamento
  - **RESPOSTA**
    - Execução do plano de resposta a incidentes

- Umas das práticas definidas pelo modelos SDL da Microsoft é a modelagem de ameaças.

- **ARMAZENAMENTO DE DADOS**

    - Dados e informações estão em fluxo constante e existem diferentes estados: **a transmissão, o processamento, o armazenamento** e estão em meio **físico, digital** e na **cabeça das pessoas**.
    - Ambos precisam de segurança em todo este fluxo.

- **ESTADOS DOS DADOS EM MEIOS DIGITAIS: DIU, DAR, DIM**

    - **DADOS TRANSMITIDOS (DIM) →** Em redes sem fio ou em qualquer tipo de conexão, incluindo a internet. Podem ser comprometidos durante a transmissão, o que pode comprometer a CID. Ataque a rede.
    - **DADOS EM PROCESSAMENTO (DIU) →** Realizam as transforamções dos dados necessários para s operações e possibilitam as interações entre usuário e o serviço. Menos oportunidades de ataques. Ataques mais elaborados.
    - **DADOS ARMAZENADOS (DAR) →** Possuem uma grande exposição aos agentes de ameaça, e recebem grande parte da atenção de segurança. Os atacantes precisam passar por algumas barreiras antes de chegar aos dados armazenados, é um ataque a banco de dados.

- **FORMAS DE PROTEÇÃO: MASCARAMENTO, ANONIIZAÇÃO E PSEUDONIMIZAÇÃO**

    - **MASCARAMENTO →** Controle que protege os dados, limitando a exposição. Os dado nãosão expostos em toda a sua toatlidade, com apenas trechos que sejam suficientes para as operações. No contexto PCI DSS, o mascaramento é um método para ocultar um segmento de dados ao ser exibido ou impresso. **Ex.** Numero do cartão de crédito 1234 12XX XXXX XXX34
    - **TRUNCAMENTO →** Método que remove permanentemente um segmento dos dados no armazanamento, as substituições são feitas de forma mais geral, **sem indicar o nuúmero de algarismos substituídos**.
    - **ANONIMIZAÇÃO →** É a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de assiciação, direta ou indireta, a um indivíduo.
    - **PSEUDONIMIZAÇÃO →** É o tratamento por meio do qual um dado perda a possiblidade de associação, direta ou indireta, a um iindivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em abiente controlado e seguro.

- **SEGURANÇA DE DADOS NA NUVEM**

    - **Provedores de nuvem →** Provisionamento, a migração e o desprovisionamento de dados considerando o término do contrato. Os dados não podem ser acessados indevidamente pelo provedor de nuvem

- **SEGURANÇA NA INTERNET**

  - Segurança e privacidade envolvem o que deve ser protegido e os componentes ou ativos de um ambiente que podem ser explorados em ataques
  - Conhecer bem as formas e estados dos dados e informações / CID
    - **Formas**: Física, Digital, nas Pessoas
    - **Estados**: Transmitidos, Armazenados, em Processamento
    - **CID:** Confidencialidade, Intergridade e Disponibilidade
  - **Transações WEB →** Quando você solicita algum serviço seus dados passam por diversos caminhos, onde agentes de ameaça estão à espreita em busca de chances para roubar os dados pessoas, das transações web e identidades digitais. Além de explorar vulnerabilidades utlizam de golpes a fim de ter acessos a informações valiosas.
  - **Os agentes de ameaça buscam oportunidades em 3 ambientes →** Ambiente do usuário; ambiente de internet que inclui o provedor de internet; no ambiente dos provedores de serviços, sistemas e plataformas.
  - Para a segurança de transações web é preciso evitar se expor, para não dar informações a ataques tantos físicos, como virtuais.
  - Transações podem envolver diferentes tipos de dados ou informações: **dados pessoais, dados financeiros ou dados confidenciais,** que podem sofrer modificações, vazamentos afetando respectivamente a Integridade, confidencialidade e disponibilidade.
  - **Ameaças no banco →** furto de identidade, captura de senha, captura da senha de transação, modificação da transação e a interrupção do acesso, afetam a autenticação ao serviço.
  - **Conexões Web podem ser protegidas com →** O uso de protocolos de segurança como HTTPS/TLS/SSL, que cria um túnel seguro por onde trafegam as informações.
  - Garantem a **confidencialidade** (**dados cifrados com chave simétrica**), a **integridade** dos dados (uso de Message Authentication Code, **MAC**), a **autencidade das partes (com o uso da criptografia de chave pública**)
  - Em provedor de serviços como bancos o ambiente pode ser atacado em qualquer um dos componentes, incluindo as **aplicações, os servidores de aplicação, os sistemas operacionais, as máquinas virtuais, os bancos de dados.**
  - O banco é um dos órgãos que mais investe em Segurança da Informação
  - **Principais golpes na internet**
    - Furto de Identidade
    - Fraude na antecipação de recursos
    - Phishing ou scan
    - Pharming
    - Golpes de comércio eletrônico
    - Boato ou hoax
  - **Privacidade na Web →** Rastreamento do que as pessoas fazem na Web, como os cookies e a divulgação espontânea de informações pessoais em rede sociais, que podem resultar em crimes que passam a barreira digital e podem afetar diretamente as pessoas com fraudes e crimes diversos.
  - Com a LGPD, todos devem preservar a privacidade e a proteção de dados pessoais.

- **<u>PROTEÇÃO PARA DISPOSITIVOS MÓVEIS</u>**

    - Principais vetores de ataques
    - Representam grandes desafios para as empresas, pois além dos dados corporativos, há os dados pessoais que requerem atenção, consequentemente implica no aumento da complexidade de proteção e aumento de riscos.
- **Objetivos de segurança no uso de dispositvos móveis no mundo corporativo**
    - Separar o que é Pessoal e Profissional no dispositivo
    - Antimalware
    - Remoção de apps vulneráveis
    - Autenticação de duplo fator
    - Uso de criptografia no tráfego
    - Conexão apenas com dispositivos confeáveis
- **Capacidades de segurança necessárias**
    - Proteção contra o acesso indevido aos dados do dispositovo móvel
    - Configurações de privacidade
    - Proteção contra tentativas de phishing
    - Proteção dos dados armazenados no dispositivo
    - Gerenciamento centralizado para aplicar políticas e configurações aos disp.
    - Avalliação da segurança das aplicações
- **Engenharia Social de dispositivos móveis**
    - **Phishing** -→ Páginas falsas em que a vítima recebe um link e acaba inserindo suas credenciais, seus dados mais sensiveis, e também a instalação de códigos maliciosos por apps falsos.
    - **LeifAccess ou Shopper**→ Malware distribuído via mídia social, plataforma de jogos ou chat de jogos, ele envia mensagens falasa de alertas para o usuário ativar os serviços de acessibilidade do dispositivo para criar contas, baixar apps
- **Segurança em dispositivos móveis para empresas**
    - Saber escolher a arquitetura a ser usada no dispositivo, se ele será somente para uso corporativo, ou se ele terá permissão para uso pessoal também.
    - **Modelo COPE** →Aparelho é de propriedade dda emoresa e provê uma flexibilidadae de uso ao permitir que tanto a empresa quanto o usuário possam instalar apps no dispositivo.
    - **Modelo BYOD ou CYOD** → O dono do dispositivo móvel é o próprio usuário.
    - **Recomendações de segurança e privacidade para empresas adotarem no uso dos dispositivos** → Conduzir uma análise de riscos em dispositivos móveis e para as informações acessadas por eles; Adotar tecnologia de segurança móvel como EMM, plataformas de defesa contra ameaças móveis ou serviço de veto a aplicações móveis, com o uso de técnica estáticas, dinâmicas e comportamentais, para analiasr o risco de segurança ou de privacidade; Prover a segurança em cada dispositivo e adotar um solução de gerenciamento de mobilidade corporativa (EMM/MDM); Ciclo de vida.´

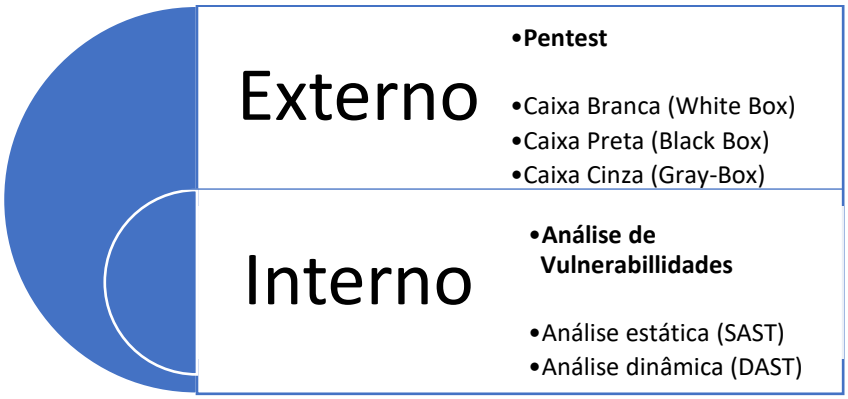
- **ANÁLISE DE VULNERABILIDADE E PENTEST**

  - Podem existir vulnerbilidades em plataforma Web e móvel, na gestão de vulnerabilidades **a identificação de vulnerabilidades é importantissima e é o <u>ínicio</u> de tudo**, uma vez descobertas devemos trata-las com **os controles de segurança**.


> **CONTROLES:** Físico/Tecnologico/Processo é aplicado em **ATIVOS** que possuem **VULNERABILIDADES** que são eliminadas pelo **CONTROLE.**

- **TESTES DE SEGURANÇA**

  - São importates para a **gestão de segurança da informação** PORQUE identificam as vulnerabilidades que precisam serem tratadas, há vários tipos de testes como análises e avaliações de riscos, análises de vulnerabilidades que focam tradicionalmente em aspectos tecnológicos.
  - Testes de Segurança como análise de vulnerabilidades e pentests são so principais serviços ofertados por empresas especializadas em segurança.
  - **OWASP – Open Web Application Securyti Project**→ entidade sem fins lucrativos e com reconhecimento internacional, que atua com foco na colaboração para o fortalecimento da segurança de aplicativos web.
  - Para ela teste de segurança é o processo de comparar o estado de um sitemas ou aplicação de acordo com um conjunto de critérios, podem ser feitos no final do desenvolvimento ou fazer parte do ciclo de desenvolvimento desde o início, com a implementação de requisitos e testes de seguranças automatizados.
  - <u>Os testes de segurança envolvem variáveis como</u> : **Origem dos testes (Interno ou Externo)**, as **informações prévias disponíveis para os testes,** o **uso de ferramentas automatizadas** e a **qualificação dos profissionais.**




- Os testes internos fazem parto do ciclo de vida de desenvolvimento de software, com atividades de segurança sendo realizadas nas fases de **definição, especificação, desenvolvimento, implantação e manutenção das plataformas Web e móvel.**
- **SAST** → Envolve a análise dos componentes do sistema sem a sua execução, pela análise manual ou automatizada do CóDIGO-FONTE.
- **Análise manual** → exige proficiência na linguagem e no framwork usado pela aplicação e possibilita a indentificação de **vulnerabilidades na lógica de negócios, violações de padrões e falhas na especificação,** especificamente quando o código é tecnicamente seguro, mas com falhas na lógica.
- **Análise automatizada** → É feita com ferramentas que checam o código-fonte por conformidade com um conjunto pré-definido de regras ou melhores práticas da indústria. A revisão manual do código pode ser feita com uma de métodos mais básicos de busca de palvras-chave no código-fonte, também podem ser utilizados os ambientes de desenvolvimento, IDEs.
- **DAST**→ Envolve a análise do sistema durante a sua execução, em tempo real, de forma manual ou automatizada. Não provê informações que a SAT provê. É conduzida na camada da plataforma e nos APIs do backend, que são locais em que as requisições e respostas das aplicações podem ser analisadas. É mais cara.

- **PENTEST**

- Teste de penetração/pentest/testes de intrusão/ethical hacking → Realizados a partir do ambiente externo. Seu objetivo é determinar **"se"** e **"como"** um agente de ameaçã pode obter um acesso **não autorizado** a ativos.
- Identificar meios de explorar vulnerabillidades para driblas os controles de segurança dos componentes do sistema.
- Há 3 tipos de pentests, que depende das informações do ambiente obtidas antes dos testes de segurança:
    - **Teste de Caixa-Preta (black-box)** → Conhecimento zero. Sem qualquer informação sobre o ambiente que está sendo testado. O profissional faz o teste como se fosse um atacante real.
    - **Teste de Caixa-Cinza (gray-box)** → Conhecimento parcial. É fornecida alguma informação como uma credencial de acesso, enquanto outras

informações têm que ser descobertas. Teste mais comum devido aos custos, tempo e escopo.

- **Teste de Caixa-Branca (white-box)** ➔ Conhecimento total. Temos todo o conhecimento sobre o ambiente, incluindo o código-fonte, documentação e diagramas. Teste mais rápido.

- **METODOLOGIA OWASP**

  - Foca em **aplicações Web**, e visa a construção de aplicações mais confiáveis e seguras.
  - Testar o software deve estar em todo o ciclo de vida de desenvolvimento de software e que a melhor maneira de prevenir **bugs** de segurança em aplicações em produçao é o **SDLC** incluir a segurança em cada uma de suas fases.
  - Framework da metodologia da OWASP
    - **Antes do desesnvolvimento** ➔ Definição do SDLC. Revisão de Políticas e Padrões. Desenvolvimento de métricas
    - **Definição e Especificação** ➔ Revisão dos requisitos de segurança e da especificação e arquitetura. Criação e revisão dos modelos UML e ameaça.
    - **Desenvolvimento** ➔ Execução simulada do código. Revisão do código.
    - **Implementação** ➔ Pentest da aplicação. Teste do gerenciamento de configuração
    - **Manutenção** ➔ Revisão do gerenciamento operacional. Checagem periódica. Verificação das mudanças.

- **METODOLOGIA PTES**

  - A PTES (Penetration Testing Execution Standard) é uma metodologia de segurança ofensiva que fornece um padrão para realizar testes de segurança em qualquer ambiente. É uma abordagem abrangente que visa garantir que todos os aspectos do sistema sejam testados.
  - É composta por **sete seções**, que definem as aticidades a serem realizadas, desde as interações iniciais até orelatório.
    - **Interações Inciais** → iniciar as atividades
    - **Obtenção de Informações** → obter informações para a análise
    - **Modelagem de ameaças**
    - **Análises de vulnerabilidades**
    - **Exploração** → para passar pelos controles de segurança existentes
    - **Pós-exploração** → para manter o acesso e controle do alvo
    - **Relatório final**

- **METODOLOGIA OSSTMM**

    - A metodologia OSSTMM (Open Source Security Testing Methodology Manual) é uma das mais conhecidas e utilizadas na realização de testes de segurança. Ela é baseada em cinco áreas de testes: informação, pessoal, processo, tecnologia e física. A metodologia enfatiza a necessidade de testes em várias camadas e abordagens diferentes para garantir a segurança geral de um sistema.
    - Tipos de testes de segurança
        - Blind
        - Double Blind
        - Gray Box
        - Double Gray Box
        - Tardem
        - Reversal

- **AUDITORIA DE SISTEMAS**

    - **Auditoria** → Auditoria é uma inspeção e verificação formal para checar se um padrão ou conjunto de guias está sendo seguido, se os registros estão corretos e se os objetivos de eficiência e eficácia estão sendo alcançados.
    - **Objetivos**
        - Validar atividades, processos e sistemas
        - Avaliar a eficiência e aeficácia dos controles
        - Atestar a conformidade adminsitrativa, regulatória e legal
        - Assegurar para a alta gestão e diferetnes atores a estabilidade organizacional
    - A gestão de riscos identifica, analisa, avalia, comunica e trata os riscos em um contexto determinado.
    - Os controles de segurança são definidos e implementados a partir da visão de riscos e de acordo com padrões e requisitos regulatórios e legais
    - **A auditoria valida a eficiência e eficácia dos controles**, com uma análise criteriosa que segue processos e aplica técnicas e ferramentas. **Só pode ser feita por AUDITORES** e seu papel é fundamental e o resultado é uma empresa mais segura e em conformidade com padrões, regulações e leis aplicáveis
    - **Responsabilidades de um Auditor**
        - Documentar a função em um estatuto, indicando propósito, responsabilidade, autoridade e a prestação de contas.
        - Obter aprovação formal do estatuto pela diretoria executiva e/ou comitê de auditoria
        - Ser objetivo nos assuntos de auditoria.
        - Deixar clara as obrigações e responsabilidades para que sejam providas informações apropriadas, relevantes e no tempo correto
    - As técnicas de auditoria podem ir de entrevistas a testes técnicos com o uso de ferramentas para análise de logs e até mesmo de código-fonte

- O **planejamento** da auditoria é essencial para o sucesso, e o escopo e objetivo da auditoria devem estar claros, entendidos e aceitos pelo auditor e pelo auditado.
- Um componente importante do plano de auditoria é o programa de auditoria, também conhecido como programa de trabalho. O programa de auditoria é composto por procedimentos e passos específicos que serão utilizados para testar e verificar a efetividade dos controles


- **FASES DE UM PROCESSO DE AUDITORIA**


- **<u>PLANEJAMENTO</u>**
  - **Objeto** da auditoria pode ser um sistema, uma localidade ou uma unidade de negócio.
  - **Objetivo** da auditoria é determinar se as mudanças no código-fonte de um sistema crítico ocorrem em um ambiente bem definido e controlado.
  - **Escopo** da auditoria é o sistema que é composto por diferentes componentes que precisam passar por uma avaliação completa. É o escopo que direciona o auditor a definir o conjunto de testes relevantes para a auditoria, junto de qualificações técnicas e recursos necessários para avaliar diferentes tecnologias e seus componentes.
  - **Planejamento de pré-auditoria**, a condução de uma avaliação de riscos ajuda na justificativa das atividades e no refinamento do escopo
  - O planejamento da auditoria é finalizado com a **definição dos procedimentos,** que envolvem a identificação da documentação (políticas, padrões e guias), dos requisitos de conformidade regulatória, da lista de indivíduos para as entrevistas e dos métodos e ferramentas para a avaliação

- **<u>TRABALHO EM CAMPO</u>**
  - Obtenção dos dados, testes dos controles, realização das descobertas e validações e a documentação dos resultados.

- **RELATÓRIOS**
  - Entrega da auditoria, com a elaboração, revisão, entrega e acompanhamento dos resultados.
  - Exemplo de auditoria tem os seguintes passos
    - Revisão de documentação.
    - Entrevista com indivíduos-chave.
    - Estabelecimento de critérios de auditoria.
    - Condução de visitas ao data center.
    - Condução de revisão de áreas de alto risco.
    - Documentação dos resultados.
    - Preparação do relatório e revisão pelos atores.
    - Entrega do relatório final.

- **TÉCNICAS DE AUDITORIA DE TI**

  - Métodos para avaliar controles
    - Software de auditoria para analisar o conteúdo de arquivos de dados, como os logs de sistemas e a lista de acesso de usuários.
    - Software especializado para avaliar conteúdo de sistemas operacionais, banco de dados e arquivos de parâmetros de aplicações.
    - Técnicas de desenho de fluxos para documentar processos de negócios e controles automatizados.
    - Logs de auditorias e relatórios para avaliar parâmetros.
    - Revisão de documentação.
    - Perguntas e observação.
    - Simulações passo a passo
    - Execução de controles
  - **Ferramentas de Auditoria** → questionários, scripts, banco de dados relacionais, planilhas eletrônicas, ferramentas de auditoria específicas (Computer-Assisted Audit Tools, CAATs) e metodologias para coleta de transações.
  - O planejamento segue os itens gerais
    - **A segurança do provedor de nuvem** segue os processos essenciais de identificação, proteção, detecção, resposta e recuperação. Esses processos visam maximizar a confidencialidade, integridade e disponibilidade dos dados e informações dos clientes. A segurança é baseada na avaliação dos riscos, que é a probabilidade de um agente de ameaça explorar vulnerabilidades de um ativo, resultando em incidentes de segurança e impactos para a empresa. Os controles de segurança são identificados e implementados com base nessa avaliação de riscos, incluindo os riscos que são aceitos.
    - **Por que a segurança é importante**, **focando nos clientes** → os clientes demandam a segurança porque precisam proteger seus negócios, e o provedor de nuvem operará seus sistemas e dados. Além disso, há a necessidade de conformidade legal e regulatória, exigida para todo o setor.
    - **Demanda dos clientes para a conformidade**→ a conformidade é baseada em regulamentos e leis, como a do setor financeiro, que exige proteção dos ativos tecnológicos, e a do setor de saúde, que exige a segurança e privacidade dos

dados dos pacientes, por exemplo. O conjunto de controles deve ser verificado sob a óptica destas necessidades legais e regulatórias e atestado pelo auditor.

- **Auditoria de segurança, por que fazer →** os controles de segurança implantados podem não ser eficientes e eficazes, o que compromete a segurança do provedor de nuvem e de todos os seus clientes. Além disso, riscos não identificados podem não estar sendo tratados. A auditoria é necessária para validar atividades, processos e sistemas; avaliar a eficiência e eficácia dos controles; atestar a conformidade administrativa, regulatória e legal; e assegurar para a alta gestão e diferentes atores a estabilidade organizacional. estabilidade organizacional.

- **Principais fases do processo de auditoria →**
  - Planejamento→ Envolve principalmente a definição do escopo e das técnicas e ferramentas a serem utilizadas na auditoria
  - Trabalho em campo → Os dados são adquiridos e controles são testados e verificados
  - Relatórios → Os resultados da auditoria são organizados e apresentados
- O provedor de nuvem é seguro com a gestão de riscos e a gestão de segurança da informação, comum processo de melhoria contínua que culmina com a assertividade cada vez maior da visão de riscos e dos controles implantados. Com a auditoria, assim, pode ser confirmada para a alta gestão da empresa que o negócio está funcionando bem e está preparado para enfrentar os potenciais desafios.

- **<u>CONTROLES GERAIS DE AUDITORIA DE SISTEMAS</u>**

- **<u>CONTROLES DE SEGURANÇA E PRIVACIDADE</u>**

  - **Controles físicos** → são aqueles mais palpáveis, visíveis, como o controle de acesso físico a uma área segura. Ex.: Monitoramento de circuito fechado de TV
  - **Controles Tecnológicos** → Ex.: Firewall, VPN
  - **Controles Processuais** → são aqueles que estabelecem pontos de controle a serem executados pelos envolvidos. Ex.: Atualização periódica de sistema operacional
  - Os controles de segurança são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança.
  - Os controles de privacidade são salvaguardas administrativas, técnicas e físicas aplicadas em sistemas e organizações para gerenciar riscos de privacidade e para assegurar conformidade com requisitos de privacidade aplicáveis
  - Os requisitos de segurança e privacidade direcionam a seleção e implementação de controles de segurança e privacidade e são derivados de leis, ordens executivas Controles de Segurança e Privacidade, diretrizes, regulações, políticas, padrões e necessidades de missão para assegurar a confidencialidade, integridade e disponibilidade das informações processadas, armazenadas e transmitidas, e também para gerenciar riscos.
  - O NIST define as cinco funções da segurança: identificação, proteção, detecção, resposta e recuperação

- **CONTROLES ORGANIZACIONAIS E RELÇAO COM SEGURANÇA E CONTINUIDADE DO SERVIÇO**

    - A segurança e privacidade fazem parte do contexto das empresas e estão integradas com outros assuntos, como a governança de TI.
    - A governança de TI visa a transformação digital e a relação com a entrega de valor, a mitigação dos riscos de negócios e a otimização de recursos.
    - A governança tem como principais objetivos →
        - Avaliação de necessidades, condições e opções de todos os atores envolvidos, em busca de determinar objetivos corporativos balanceados.
        - Direcionamento para a priorização e tomada de decisão.
        - Monitoramento do desempenho e conformidade de acordo com os direcionamentos e objetivos definidos.

- **COBIT (CONTROL OBJETIVES FOR INFORMATION AND RELATED TECHNOLOGY)**

    - Framework de **governança de TI** que trata de uma visão organizacional, a qual tem relçao com a segurança e privacidade
    - Define os componentes para construir e sustentar um sistema de governança, composto por processos, estrutura organizacional, políticas, procedimentos, fluxos de informação, cultura, comportamentos, qualificações e infraestrutura.
    - **Há cinco domínios no COBIT**, um para a governança e quatro para o gerenciamento, sendo composto por um total de **40 processos**, que podem ser entendidos como controles organizacionais. Os exemplos citados dos 40 processos organizacionais são referentes aos controles de segurança:
        - Avaliar, direcionar e monitorar
        - Alinhar, planejar e organizar
        - Construir, adquirir e implementar
        - Entregar serviço e suporte
        - Monitorar, verificar e avaliar
    - Alguns processos ou objetivos de controle organizacionais definidos no COBIT, estão voltados diretamente para a segurança. Por exemplo, a condução de auditorias do sistema de gestão da segurança da informação em intervalos definidos é uma das atividades que devem ser feitas

- **ITIL (INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY)**

    - Framework de **melhores práticas que visa auxiliar as empresas a entregar e suportar serviços de TI**, provendo uma estrutura alinhada com a visão, missão, estratégia e objetivos da organização.
    - Há um sistema de valor dos serviços, composto por → Cadeia de valor de serviços. Princípios. Governança. Melhoria contínua. 34 práticas de gerenciamento. Dentre os benefícios do ITIL para as empresas, estão:
        - Padronização do modelo de operação de TI.
        - Cumprimento dos requisitos de clientes e funcionários.

        - Maior agilidade e capacidade para inovação.
        - Entregas em ambientes em constante mudança.
        - Maior controle e governança.
        - Demonstração do valor de TI.
        - Oportunidade para melhorias.
    - As 34 práticas do ITIL envolvem guias que são agrupadas em três categorias
        - Práticas de gerenciamento geral
        - Práticas de gerenciamento de serviço
        - Práticas de gerenciamento técnico.

- **CONTROLES DE ACESSOS possuem 4 categorias**

    - **Requisitos do negócio para controle de acesso**
        - Política de controle de acesso
        - Acesso às redes e aos serviços de rede
    - **Gerenciamento de acesso de usuário**
        - Registro e cancelamento de usuário
        - Provisionamento para acesso de usuário
        - Gerenciamento de direitos de acesso privilegiado
        - Gerenciamento de informação de autenticação secreta de usuário
        - Análise crítica dos direitos de acesso de usuário
        - Retirada ou ajuste de direitos de acesso
    - **Responsabilidade dos usuários**
        - Uso da informação de autenticação secreta
    - **Controle de acesso ao sistema e a aplicação**
        - Restrição de acesso à informação
        - Procedimentos seguros de entrada do sistema (log-on)
        - Sistema de gerenciamento de senha
        - Uso de programas utilitários privilegiados
        - Controle de acesso ao código-fonte de programas

    - **CONTROLE LÓGICO, FÍSICO E PROCESSUAL**

        - Envolvem investimentos em pessoas, processos e tecnologias, principalmente para o desenvolvimento de uma cultura de segurança, e podem ser administrativos, técnicos ou operacionais. Alguns exemplos:
            - Conscientização
            - Políticas. Sistemas de detecção de intrusão
            - Registro de eventos (logging)
            - Varredura de vulnerabilidades
            - Classificação da informação
            - Hardening de arquitetura e de tecnologia
            - Hardening de sistemas.

- **RELATÓRIO DO PLANEJAMENTO COM FOCO NOS CONTROLES**

  - **Tipos de controles considerados e para que servem** → Controles são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança, e também para assegurar conformidade com requisitos aplicáveis.
  - **Podem ser →**
    - **Técnicos, tecnológicos ou lógicos**, como o antivírus ou o backup
    - **Físicos**, como o cadeado para que o desktop utilizado pelo presidente da empresa não seja roubado
    - **Processuais,** administrativos ou operacionais, como a política de segurança ou o processo de revisão de contas de usuários
  - **Como os controles são definidos →** os controles são definidos pelos riscos existentes na empresa, que direciona mas necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos. Além dos riscos, a definição dos controles pode ser feita a partir de requisitos que direcionam a seleção e implementação de controles, e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa.
  - **Normas ou frameworks que podem ser a base para a definição dos controles →** a ABNT NBR ISO/IEC 27002 define um conjunto de objetivos de controle de segurança da informação, e pode ser utilizada para a definição dos controles.
  - **COBIT** → é um framework para governança de TI e possui um conjunto de controles mais amplos que podem ser implantados, incluindo os de segurança e privacidade.
  - **ITIL** → é um conjunto de melhores práticas para o gerenciamento de serviços e estabelece também um conjunto de controles mais amplos que inclui aspectos de segurança
  - **Controles para aquisição, desenvolvimento e manutenção de sistemas:** os controles para este assunto devem incluir os requisitos de segurança de sistemas de informação, para garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. É necessário ainda que controles de segurança sejam definidos em processos de desenvolvimento e de suporte, para garantir que a segurança da informação esteja projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. Os controles de segurança devem ainda abordar os dados para teste, principalmente nos aspectos de privacidade, que devem ser reforçados devido à Lei Geral de Proteção de Dados Pessoais (LGPD).
  - **Controle de acesso** →o controle de acesso deve ser tratado pelos requisitos do negócio para controle de acesso, com a política de controle de acesso e o acesso às redes e aos serviços de rede. O gerenciamento de acesso do usuário deve incluir aspectos como o registro e cancelamento de usuário, provisionamento para acesso de usuário,

gerenciamento da informação de autenticação secreta de usuários e análise crítica dos direitos de acesso de usuário. O controle para as responsabilidades dos usuários deve envolver o uso da informação de autenticação secreta. O controle de acesso ao sistema e à aplicação deve envolver a restrição de acesso à informação, procedimentos seguros de entrada no sistema (log-on), uso de programas utilitários privilegiados e controle de acesso ao código-fonte de programas.

- **Auditoria** → a auditoria visa garantir que os controles sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz. Assim, a auditoria de sistemas é essencial para a efetiva proteção da empresa, ao analisar a eficiência e eficácia dos controles definidos e implementados.

- **TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS**

  - O objetivo e o escopo da auditoria podem estar relacionados com a conformidade com normas, padrões, frameworks, leis e requisitos de negócios.
  - A auditoria avalia e verifica a eficácia e eficiência dos controles implantados, que são necessários de acordo com a avaliação de riscos e das normas, padrões, frameworks, leis e requisitos de negócios relacionados. Alguns exemplos de abordagens para as auditorias:
    - Governança
    - Riscos
    - Gestão
    - Processos de gestão de riscos.

- **OBJETIVOS DE AUDITORIA DE SISTEMAS**

  - Alguns exemplos de objetivos de auditoria para a segurança e privacidade das empresas, que exigem o planejamento de procedimentos, técnicas e ferramentas específicos, são
    - Políticas, padrões e procedimentos de segurança adequados e efetivos.
    - Riscos emergentes identificados, avaliados e tratados de uma forma confiável e adequada.
    - Ataques e brechas são identificados e tratados no tempo e na forma apropriados.

- **PRINCIPAIS TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS**

  - Auditoria de controles de segurança e privacidade exige um conjunto de habilidades que envolvem aspectos especializados, tais como para os pentests, a análise de configurações de servidores ou firewalls, ou revisão de regras de ferramentas de segurança
  - As auditorias são normalmente compostas por um conjunto de metodologias, técnicas e ferramentas
  - Elas devem ser utilizadas para identificar, levantar evidências e para analisar e validar as evidências. Além disso, as metodologias, técnicas e ferramentas devem auxiliar o auditor a organizar e documentar os resultados. Há técnicas para interagir com as pessoas em busca das informações, que se complementam às análises manuais e às análises técnicas.

- **OBJETIVOS DAS TÉCNICAS E FERRAMENTAS**

  - Identificar e levantar evidências
  - Analisar e validar as evidências
  - Organizar os resultados

- **As técnicas e ferramentas envolvem**

  - **Interação com pessoas →**
    - Entrevistas
    - Questionários
    - Pesquisas
    - Perguntas e observação
    - Dinâmicas em grupo.
  - **Análise manual →**
    - Análise e revisão de documentação
    - Análise de políticas, procedimentos e processos.
    - Análise de configurações
    - Desenho de fluxos para documentar processos de negócios e controles automatizados
    - Simulação de mesa
    - Revisões gerenciais
    - Autoavaliação
    - Análise de código
  - **Análise técnica →**
    - Planilhas eletrônicas
    - Scripts
    - Software de auditoria Ferramentas de auditoria específicas
    - Software especializado - S.O, B.D, arquivos

    - Logs de auditorias e relatórios
    - Simulações passo a passo
    - Execução de controles: Metodologias para coleta de transações
    - Pentests ou testes de penetração

- **APLICABILIDADE DAS TÉCNICAS E FERRAMENTAS PARA AUDITORIAS**

    - O universo a ser avaliado em uma auditoria de segurança e privacidade pode ser baseado em três linhas de defesa, que direcionam como as técnicas e ferramentas podem ser aplicadas:
        - Gestão interna
        - Gestão de riscos
        - Auditoria interna
    - A auditoria interna é essencial para a avaliação de desempenho do SGSI e é bastante similar com a auditoria de certificação:
        - Definição de escopo e levantamento de pré-auditoria
        - Planejamento e preparação
        - Trabalho em campo
        - Análise
        - Reporte
- **Relatório das técnicas e ferramentas que serão utilizadas na auditoria**

    - Os controles implantados no data center foram resultados da avaliação de riscos, que direcionaram as necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos.
    - Além dos riscos, a definição dos controles foi feita a partir de requisitos que direcionam a seleção e implementação de controles e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa, como a norma de certificação de data centers TIA-942, o padrão de segurança PCI DSS da indústria de cartões de pagamento e as melhores práticas de gerenciamento de serviços ITIL
    - O primeiro ponto da auditoria é a realização de uma avaliação de riscos, para que todos os riscos do escopo referente ao datacenter tenham sido mapeados.
    - Na avaliação de riscos, devem ser identificados e mapeados ameaças, agentes de ameaças, ativos, suas vulnerabilidades, e calculados a probabilidade e os impactos.
    - Os ativos são →
        - A área segura
        - Os racks com os servidores e os equipamentos de comunicação
        - Os administradores de sistemas
        - As máquinas virtuais
        - Sistemas operacionais disponibilizados para os clientes
        - Sistema de provisionamento de acesso aos clientes

- Após a avaliação dos riscos, o tratamento dos riscos pode se basear nos controles do TIA-942, PCI DSS, ABNT NBR ISO/IEC 27002, NIST Cybersecurity Framework, ITIL e COBIT, entre outros, focando nestes ativos. Os controles das diferentes normas, padrões e frameworks são equivalentes e complementares.
- A verificação dos controles pode ser feita pensando nos controles técnicos, físicos e processuais, que são utilizados pela empresa
- Os principais controles existentes na empresa devem estar cumprindo os objetivos de, pelo menos →
    - Políticas de segurança da informação
    - Organização da segurança da informação
    - Segurança em recursos humanos
    - Gestão de ativos
    - Controle de acesso
    - Criptografia
    - Segurança física e do ambiente
    - Segurança nas operações
    - Segurança nas comunicações
    - Aquisição, desenvolvimento e manutenção de sistemas.
- As técnicas e ferramentas para a auditoria no provedor de nuvem podem incluir, pelo menos →
    - Análise das políticas, processos e procedimentos de segurança e privacidade
    - Entrevistas com todas as áreas da empresa para percepção sobre se a política de segurança é de conhecimento organizacional e se está sendo seguida
    - Visita ao data center para analisar a segurança física
    - Análise de configuração do firewall
    - Análise do fluxo para gestão de identidades
    - Pentest para identificar vulnerabilidades do ambiente
    - Análise de logs do banco de dados
    - Análise dos relatórios do IDS/IPS
    - Análise dos antivírus
    - Teste de phishing