Segurança Informática

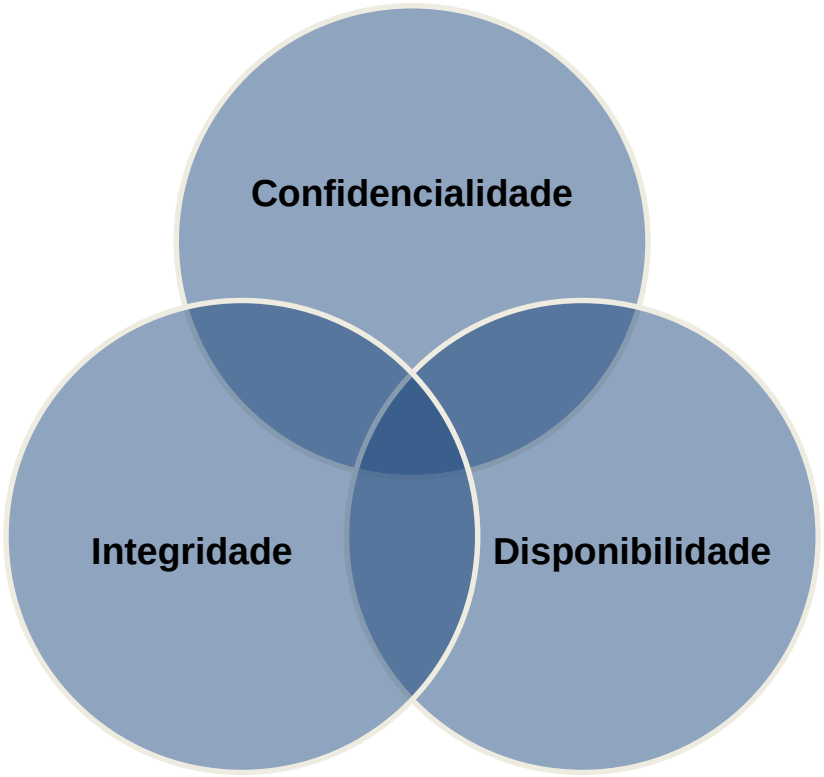
Perguntas Exemplo

Perguntas Exemplo

- Diga o que entende por integridade da informação?

Componentes base

- Confidencialidade
  - Garantia de que a **Informação** não é divulgada de forma inadequada a entidades ou processos não autorizados.
- Integridade
  - Garantia da prevenção contra a modificação e/ou destruição não autorizada da **Informação**.
- Disponibilidade
  - Garantia da acessibilidade da **Informação** onde e quando necessária e sem demora indevida.



Perguntas Exemplo

- Explique 4 tipos diferentes de controlos de segurança e dê um exemplo para cada um deles.

Controlos de segurança

- Dissuasão
  - Dissuadir os atacantes
- Prevenção
  - Evitar falhas de segurança
- Detecção
  - Detectar falhas de segurança
- Correcção
  - Tolerar/corrigir falhas de segurança
- Recuperação
  - Recuperar depois de falhas de segurança
- Compensação
  - Mecanismos de segurança alternativos

Perguntas Exemplo

- Enumere e explique 4 Princípios da protecção da informação Saltzer e Schroeder.

Princípios protecção da informação

- 8 Princípios Saltzer and Schroeder:
  - Privilégio Mínimo
    - Dar apenas privilégios necessários de acordo a tarefa/função
  - Predefinições Seguras (Fail-Safe)
    - Falhar de modo seguro
    - Negar acesso por omissão
  - Economia de Mecanismo
    - Simplicidade
    - Mais fácil de entender e testar (menos possibilidades de bugs)
  - Mediação Completa
    - Verificação contínua da autorização de aceder ao recurso
    - Evitar caching de credenciais e possibilidade de circundar o mecanismo

Princípios protecção da informação

- 8 Princípios Saltzer and Schroeder:
  - Desenho Aberto (público)
    - Não depender de segredos de implementação
    - Possibilidade de teste prévio por vários experts
  - Separação de Privilégios
    - Autorização com várias condições
    - Separação por vários elementos
  - Mínimo Mecanismo Comum
    - Limitar dependências de informação
  - Aceitação Psicológica
    - Não dificultar a vida dos utilizadores

Perguntas Exemplo

- Descreva e compare criptografia simétrica de bloco com criptografia simétrica de fita (stream).

Cifras stream e bloco

- Cifras stream (contínuas/sequenciais/de fita)
  - Converte 1 caractere em texto claro para 1 caractere de texto cifrado
  - Rápido, fraca propagação de erros, baixa difusão, susceptível a inserção e eliminações maliciosas, vocacionadas para hardware
- Cifras de bloco
  - Um grupo de caracteres em claro são cifrados para 1 bloco
  - Alta difusão, imunidade a inserções, lento, propagação de erros, vocacionadas para software

- Difusão: Uma mudança de um símbolo no texto em claro muda completamente o texto cifrado.

- Confusão: Não deve ser possível prever o que acontece ao texto cifrado mudando um símbolo no texto em claro.

Perguntas Exemplo

- Descreva e compare criptografia simétrica com criptografia assimétrica.

Comparação

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse; secrecy and integrity of datasingle characters to blocks of data, messages, files	Key exchange, authentication
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow; typically, 10,000 times slower than secret key

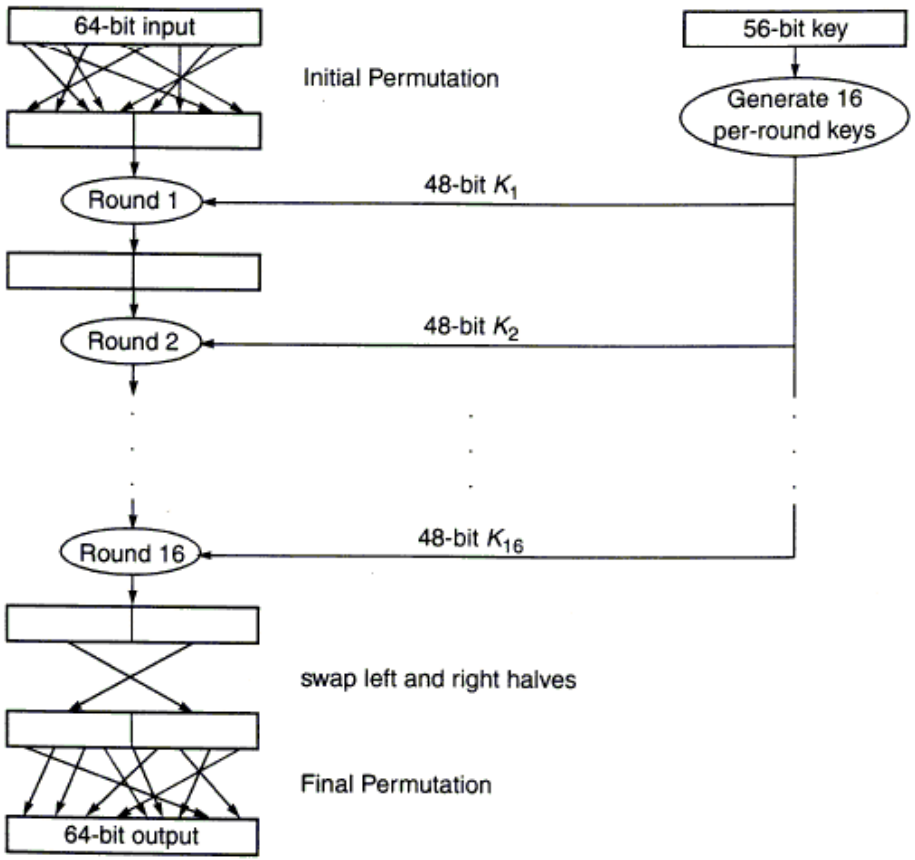
Fonte: Pfleeger

Perguntas Exemplo

- Compare o algoritmo DES com o algorithmo AES.

Algoritmos cifra simétrica

- DES - Data Encryption Standard
- Desenvolvido pela IBM em 1972 e em 1976 US Standard
- Primeiro standard criptográfico
- Supostamente enfraquecido de início, com chaves para exportação fora dos EUA com 40 bits
- Transposição + Substituição
- Chave = 56 bits + 8 bits de paridade
- Cifra de blocos de 64bits



Fonte: Universidade Colorado

Algoritmos cifra simétrica

- AES- Advanced Encryption Standard 1999
- NIST lançou um concurso para um novo algorithmo de cifra em Outubro de 2000
  - Requisitos de avaliação: segurança, aleatoriedade do output, licenciamento gratuito, base matemática, requisitos computacionais e de memória, simplicidade, performance em software e hardware e flexibilidade
  - Algoritmos são atacados publicamente
- Vencedor foi o Rijndael
  - Chaves de 128, 192, 256 bits
  - Blocos de 128, 192, 256 bits

Algoritmos cifra simétrica

	DES	AES
Date	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length)	128, 192, 256 (and possibly more) bits
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accepted open public comment
Source	IBM, enhanced by NSA	Independent Dutch cryptographers

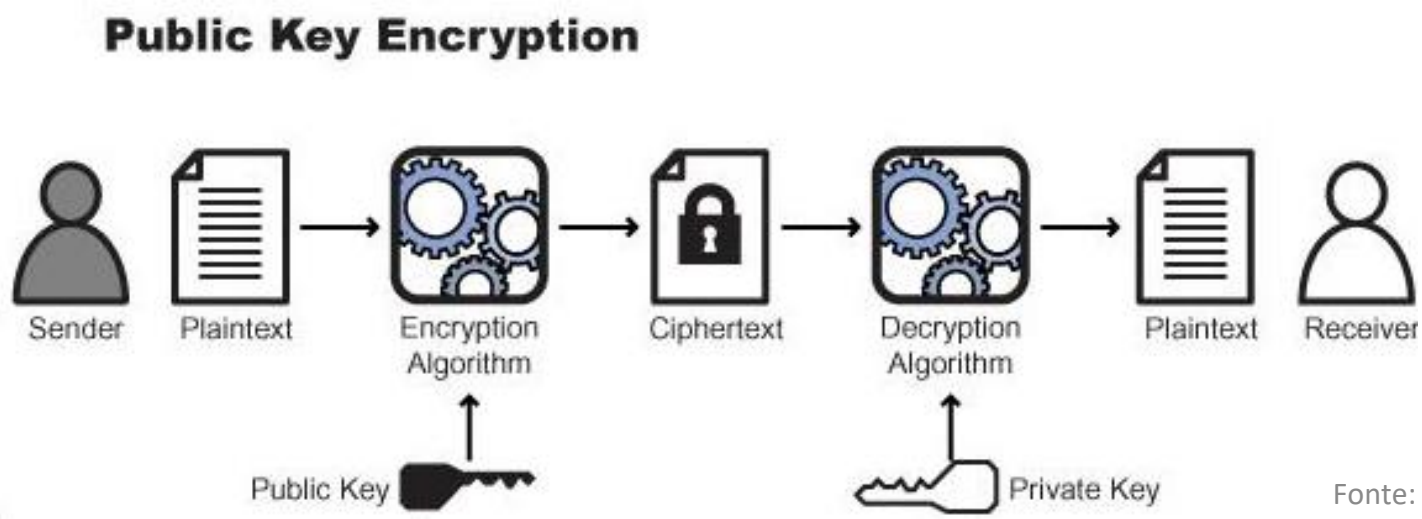
Fonte: Pfleeger

Perguntas Exemplo

- Explique o processo de envio de uma mensagem usando criptografia assimétrica com o objectivo de garantir a confidencialidade da informação.

Cifra Assimétrica

- Par de Chaves (2 chaves relacionadas)
  - 1 Privada e intransmissível
  - 1 Pública conhecida pelos intervenientes na comunicação
- Uma chave cifra e outra decifra
- Impossível de obter uma chave a partir da outra



Fonte: Infosectoday

Perguntas Exemplo

- Explique o que se entende por MD5?

Checksums Criptográficos

- Algoritmos que produzem uma síntese da mensagem
- Padding: adição de bits para dar o tamanho de bloco correcto
- Unidireccional (one-way): Com o checksum não é possível derivar a mensagem
- Resistência a colisões: 2 Mensagens diferentes não podem dar um checksum igual
- 2 Tipos:
  - Hash
  - MAC: Message Authentication Code

Funções de Hash

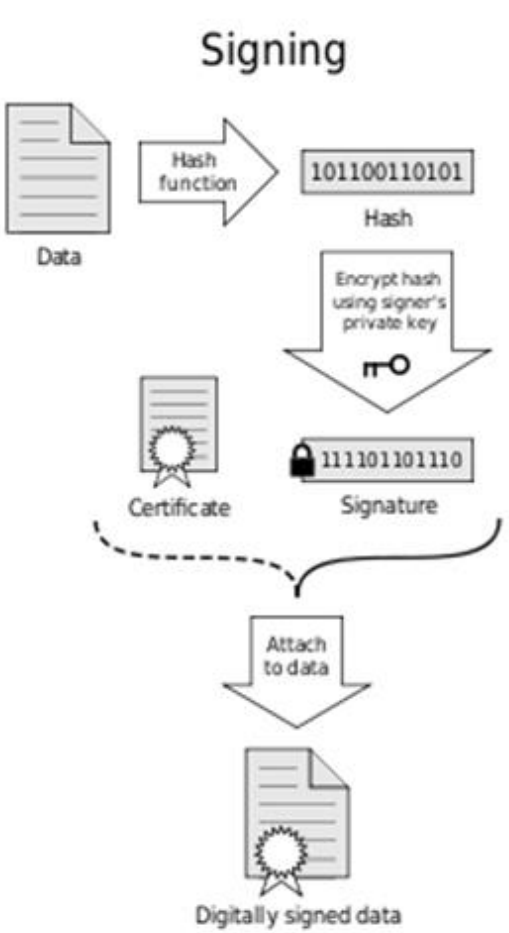
- MD5 (Rivest 1991)
  - 128 bits, blocos de 512 bits
  - Ataque optimizado com colisões (2^39), testado com sucesso para forjar certificados e documentos
  - Não recomendado para uso actual
- SHA-1 (NSA 1993)
  - 160 bits, blocos 512 bits
- SHA-2
  - 224, 256, (blocos 512)
  - 384, 512 bits, (blocos 1024 bits)
- SHA-3
  - Concurso: escolhido algoritmo Keccak
  - 224, 256, 384, 512 bits

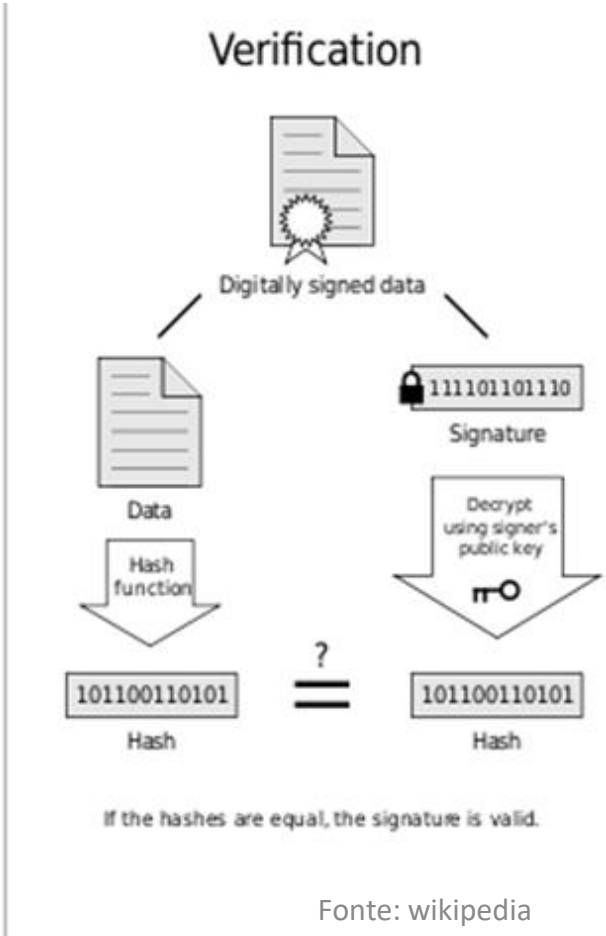
Perguntas Exemplo

- Explique o processo de assinatura digital de uma mensagem e o processo de verificação da assinatura.

Assinatura digital

- Associa uma mensagem a uma entidade univocamente
- Prova o conteúdo da mensagem e autentica o emissor (integridade)
- Insere data/hora de assinatura (não reutilização)
- Deve ser possível provar a origem dessa assinatura perante terceiros (não repudiação)
- Tem de existir uma relação de confiança com a entidade certificadora que assinou a chave pública do assinante





Fonte: wikipedia

Perguntas Exemplo

- O que entende por sistemas AAA?

Conceitos base

- Sistemas/protocolos AAA:
  - Autenticação: provar a identidade
  - Autorização: lista de permissões ou regras de controlo de acesso associadas à identidade autenticada
  - "Accounting": rastreabilidade/auditabilidade do uso de recursos
- Controlo de acesso: Protecção de recursos contra acesso não autorizado

Perguntas Exemplo

- Explique 3 factores de autenticação, de 1 exemplo para cada 1 deles.

Factores de autenticação

- 3 factores base de autenticação:
  - Algo que se sabe: password, PIN
  - Algo que se tem: smartcard
  - Algo que se é: biometria
- Alguma literatura considera também estes factores:
  - Algo que se faz: padrões de teclas, padrões de escrita
  - Algo que indica onde se está (origem): GPS
- Quando tem pelo menos 2 dos factores chama-se autenticação forte ou multi factor

Perguntas Exemplo

- Na sua opinião que política de controlo de acesso se encontra mais frequentemente nas organizações? Justifique a resposta.

Políticas controlo acessos

- Controlo de acesso discricionário (DAC):
  - Utilizadores são donos de recursos e controlam o acesso aos mesmos (atribuem privilégios, transferem a posse do recurso)
  - É uma política de controlo de acessos flexível
  - Problemas:
    - Utilizadores não têm noções de segurança nem grandes bases de tecnologia, logo leva a negligencia, erros e abuso
    - Malware pode enganar o utilizador para receber privilégios adicionais

Políticas controlo acessos

- Controlo de acesso mandatório (MAC):
  - Conceito de rótulos (labels) de segurança estáticos para os objectos e autorizações formais de acesso aos mesmos (política global)
  - Não existe transferência de permissões de acesso
  - Sistema de controlo de acessos rígido (need to know)
  - Usado em sistemas militares:
    - Bell-LaPadula (confidencialidade)
    - Biba (integridade)

Políticas controlo acessos

- Controlo de acesso baseado em funções (RBAC):
  - Controlo de acesso usado actualmente nas empresas (escalável)
  - Permite responsabilidade e permissões sobrepostas
  - Abstracção: Forma grupos de objectos e sujeitos com atributos iguais
  - Hierarquia: A hierarquia organizacional determina os direitos
  - Facilidade de gestão: alterações podem ser aplicadas a grupos e existe a possibilidade de herança das camadas inferiores

Perguntas Exemplo

- Descreva 1 ataque que se pode realizar para descobrir uma password.

Ataques passwords

- Força bruta: Tentar todas a combinações
- Dicionário: Testar um conjunto de palavras predefinidas
- Rainbow tables:
  - Pré computação de tabelas indexadas para memória para força bruta optimizada de hashes
  - Uso de “salt” como prevenção deste ataque concatenando um valor pré-estabelecido com a password antes do processo de hashing

    Exemplo: hash(userid|password)

Perguntas Exemplo

- Se o objectivo for filtrar conteúdo web (HTTP) que tipo de firewall utilizaria? Justifique.

Tipos de firewall

- Proxy:
  - Circuit gateway (socks)
    - Serve para vários protocolos , actua na camada de sessão
  - Application gateway (smtp relay, web proxy)
    - Específico para cada protocolo
  - Cliente faz o pedido ao proxy definindo o serviço e destino a aceder e o proxy faz o pedido e devolve o resultado ao cliente depois de analisado
  - Tem conhecimento dos modos de funcionamento dos protocolos e analisa todo o pacote, por essa razão tem a capacidade de analisar conteúdos
  - Maior complexidade, pode não suportar protocolos mais recentes, pode fazer caching de conteúdo estático, pode fornecer autenticação adicional

Perguntas Exemplo

- Compare host IDS com network IDS.

Host IDS

- Pode ser individual ou pode ter agentes instalados nas várias máquinas a monitorizar com gestão centralizada
  - Pode afectar a performance dos hosts e da rede
- Analisa a informação dos logs, configurações, ficheiros, memória e outra que o agente ache relevante
  - Exemplo: chamadas ao sistema privilegiadas
  - Pode ter conhecimento aplicacional específico
- Possibilita a análise de tráfego cifrado porque reside no host onde ele é decifrado
- Consegue perceber se a intrusão teve sucesso, mas o atacante pode desligar o hids

Network IDS

- Tem acesso a tráfego de rede com vários destinos com captura passiva (port mirroring/tap, firewall)
- Analisa conteúdo desse tráfego
  - Se o tráfego for cifrado não consegue analisar
- Deve obter os pacotes iguais aos que chegam ao destino (ter a mesma visão que os hosts a proteger)
- Tem dificuldade em detectar se houve realmente uma intrusão (só vê o ataque)
- O bloqueio do nids não deve ter impacto na rede (fail-open)

Perguntas Exemplo

- Explique o que entende por Honeypot.

Honeypots

- Sistema isco monitorizado com o objectivo único de ser atacado
- Tecnologia de segurança proactiva, mecanismo de engano
- Não existe tráfego legitimo para eles por isso limita falsos positivos
- Avalia ameaças reais para percepcionar o nível de risco
- Conhecimento detalhado do modus operandi do atacante
- Honeytoken: Item monitorizado colocado em localizações sensíveis
- Usos: IDS, Malware, Worms, Botnets, Spam, Phishing, Wireless, Web

Taxonomia Honeypots			
Objectivo	Investigação	Produção	
Interacção	Baixa	Média	Alta
Instalação	Física	Virtual	
Comportamento	Estático	Dinâmico	

Perguntas Exemplo

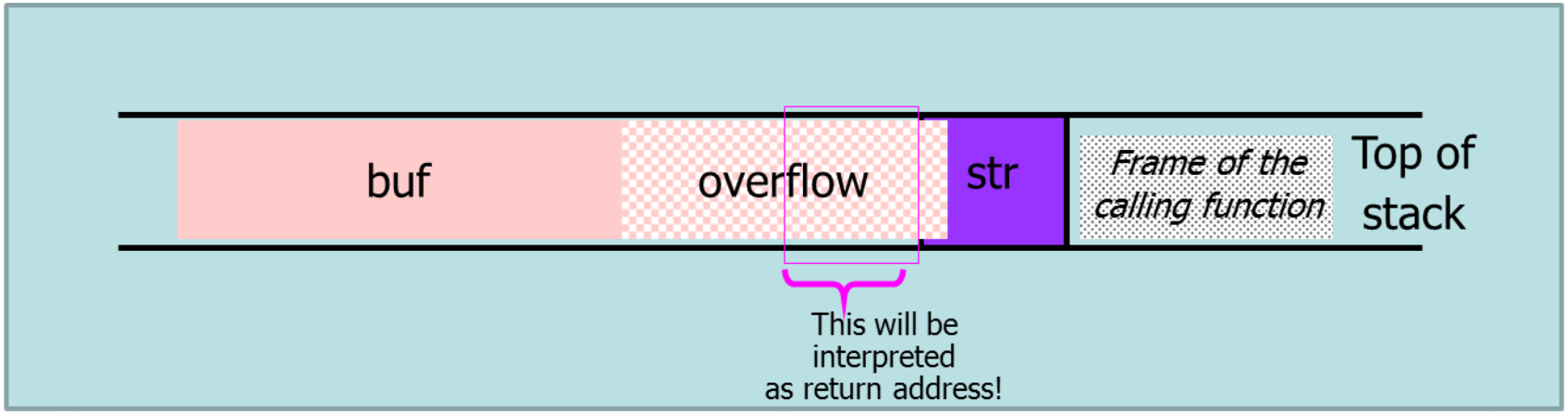
- Descreva a vulnerabilidade presente no seguinte código.

```
void func(char *str) {
        char buf[126];
        strcpy(buf,str);
   }
```

Buffer overflow

- Stack overflow: Se forem passados mais de 126 caracteres o endereço de retorno é sobreposto

```
void func(char *str) {
        char buf[126];
        strcpy(buf,str);
    }
```



Perguntas Exemplo

- Descreva a vulnerabilidade presente no seguinte código.

```
int main(int argc, char *argv[]) {
        FILE *fd;
        if (access("/some_file", W_OK) == 0) {
                printf("access granted.\n");
                fd = fopen("/some_file", "wb+");
                /* write to the file */
                fclose(fd);
        }  else {
                err(1, "ERROR");
        }
        return 0;
}
```

Race conditions

- Time of check, time of use (TOCTOU):

```
int main(int argc, char *argv[]) {
        FILE *fd;
        if (access("/some_file", W_OK) == 0) {
                printf("access granted.\n");
                fd = fopen("/some_file", "wb+");
                /* write to the file */
                fclose(fd);
        }  else {
                err(1, "ERROR");
        }
        return 0;
}
```

- Problema: o atacante faz o seguinte entre a verificação e o acesso:

```
rm /some_file
ln /myfile /some_file
```

Perguntas Exemplo

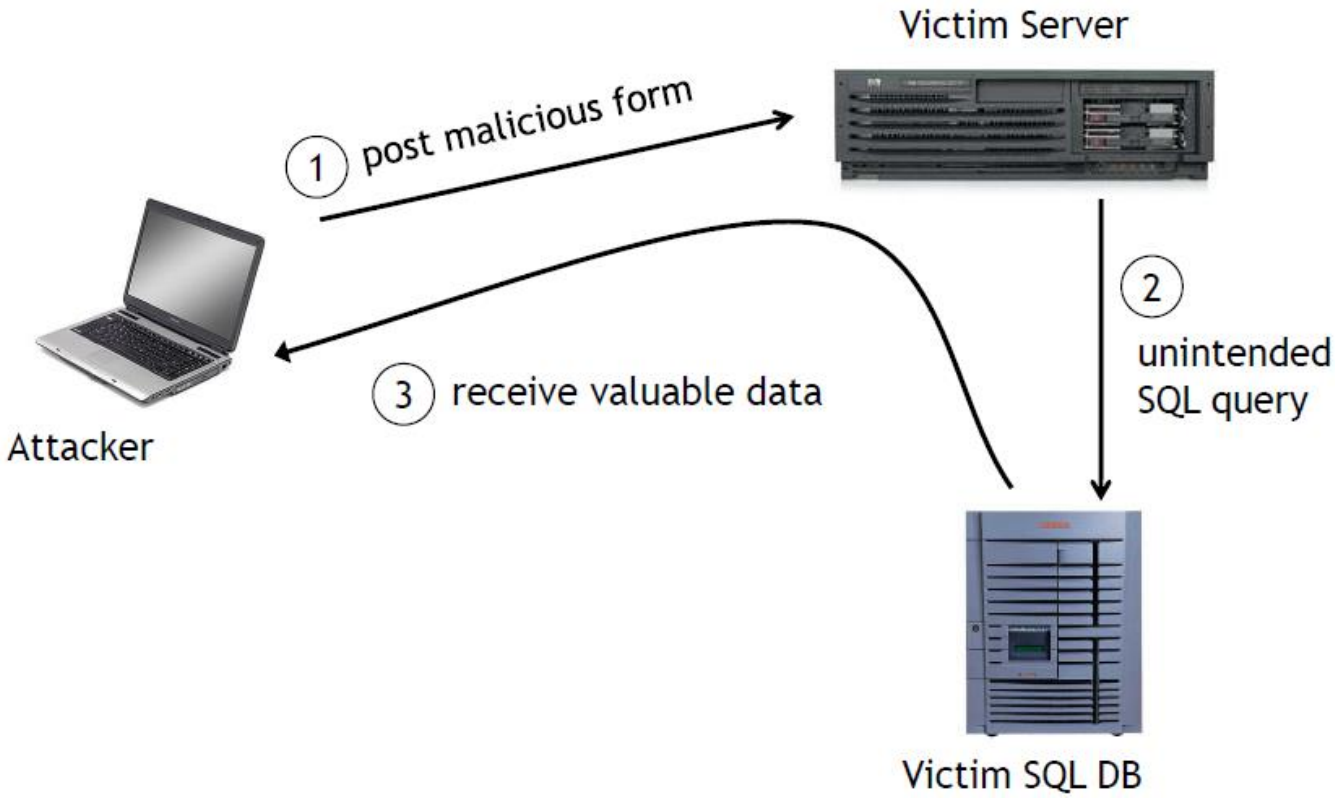
- Descreva o funcionamento de um ataque SQL injection.

SQL Injection

- SQL Injection: possibilidade de envio não autorizado de código SQL para ser interpretado pela DB do site destino e ser devolvido

  ou inferido

  o resultado

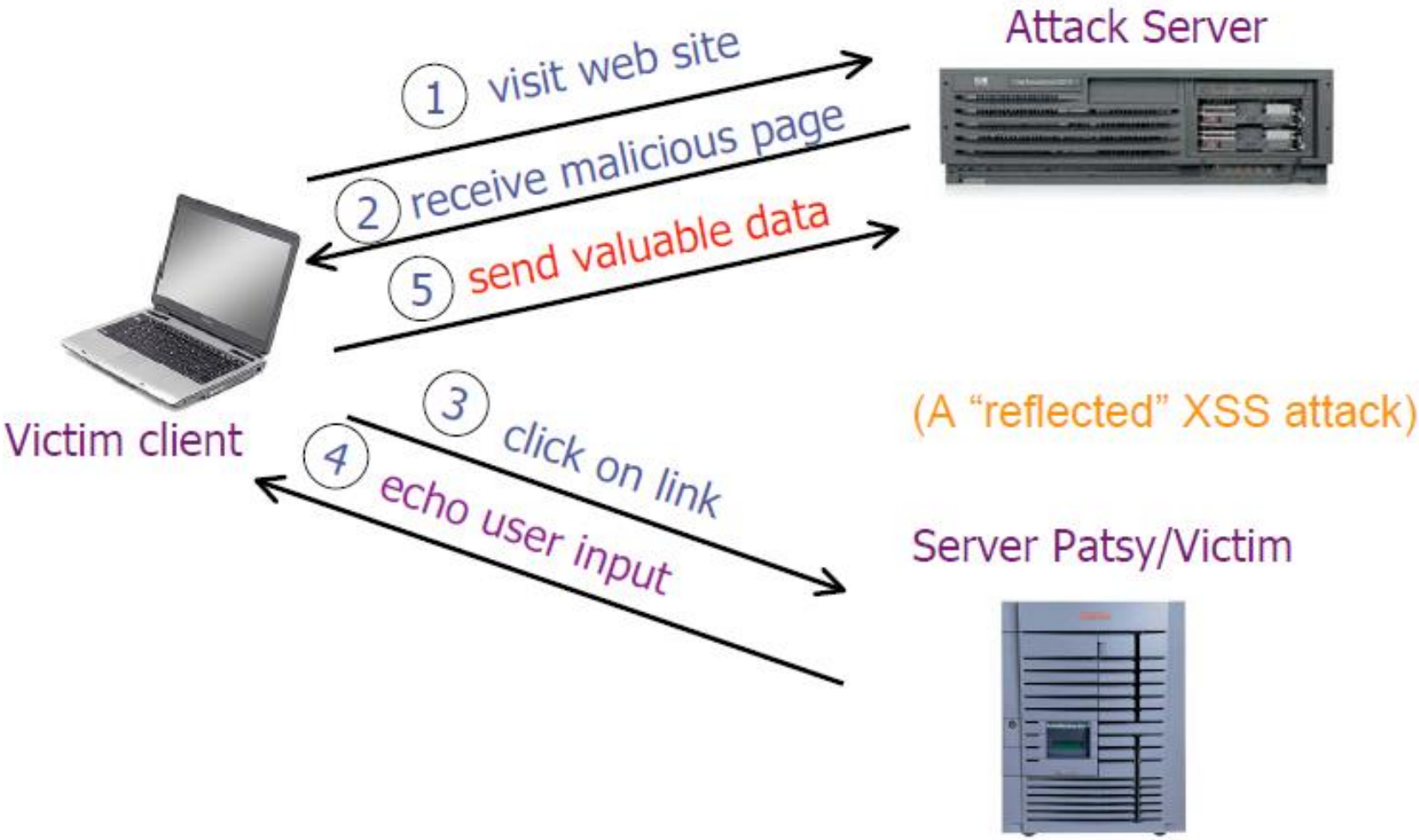


Perguntas Exemplo

- Compare o funcionamento de um ataque XSS reflectido (reflected) com um ataque XSS persistente (stored).

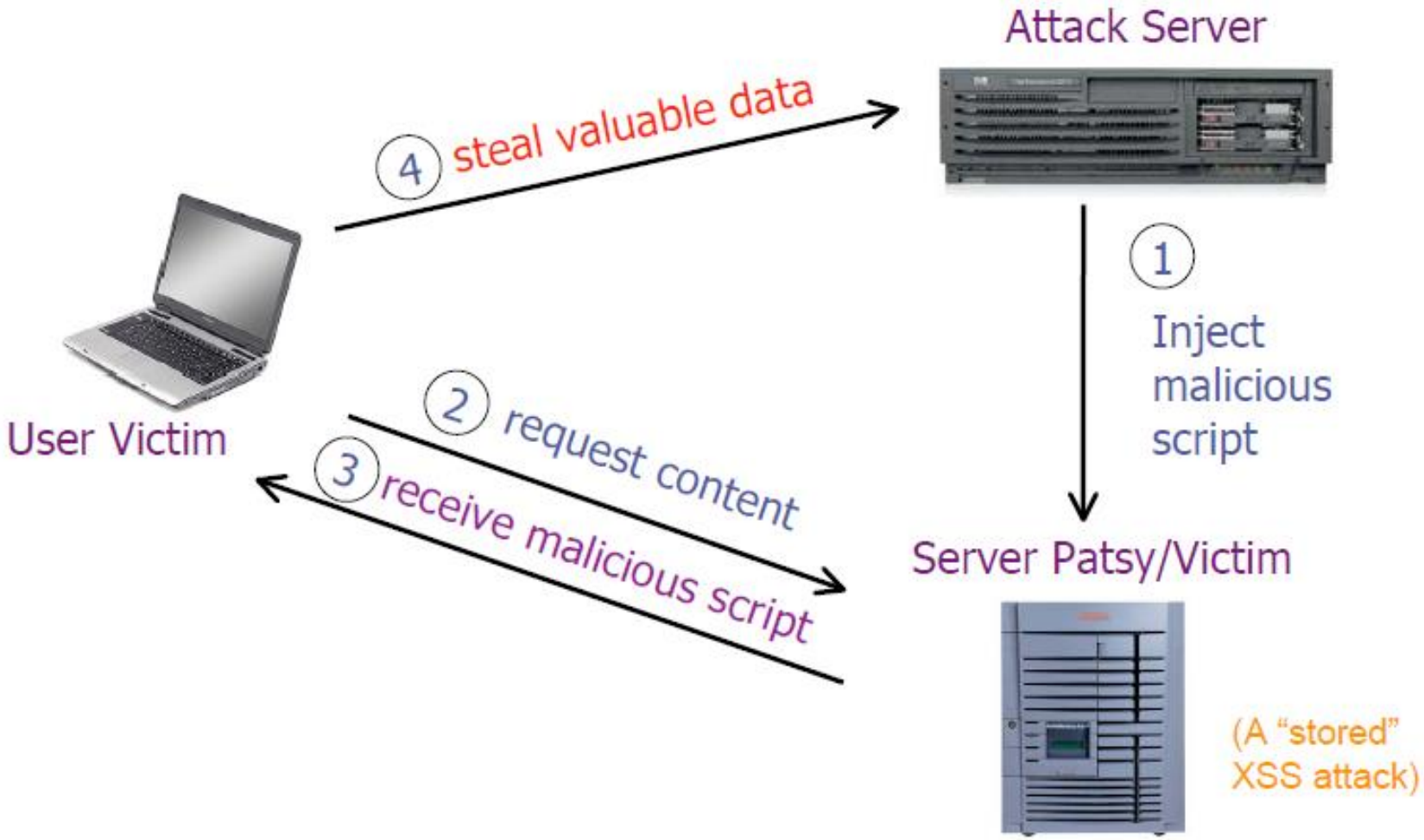
XSS

- Reflected XSS:



XSS

- Stored XSS:



Perguntas Exemplo

- Descreva uma forma de protecção contra ataques CSRF.

CSRF

- Protecção CSRF:
  - Tokens de validação
    - Elaborar um token de validação random que contenha também o sessionID
  - Validação de referer
    - Pode ser alterado apagado facilmente
  - Header HTTP costumizado
    - Adicionar origin ao header (XMLHttpRequest, XDomainRequest)
  - CAPCHA
  - Forçar reautenticação para operações críticas

Perguntas Exemplo

- Qual é o principal objectivo de uma gestão de risco?

Princípios de gestão de risco

- Objectivo da gestão de risco: Controlar e mitigar (minimizar) o risco até um nível aceitável pela gestão de topo
  - O risco só pode ser eliminado se houver a extinção da actividade que gera o risco
  - Os bens da organização devem ter um valor associado de acordo com o impacto da sua perda no negócio
    - Estes valores devem ser obtidos através de uma análise de impacto no negócio (BIA: Business Impact Analysis).
  - A análise de risco é efectuada para fornecer informação à gestão de topo que possibilite a decisão de como actuar perante o risco
    - Contém uma análise custo benefício que permite prioritizar as acções de mitigação.

Perguntas Exemplo

- Enumere e descreva os métodos de tratamento de risco.

Princípios de gestão de risco

- Tratamento de riscos:
  - Reduzir/mitigar: Implementação de medidas de segurança para mitigar o risco.
  - Aceitar: Aceitação do nível de risco pela gestão de topo tendo a organização fundos para cobrir a perda.
  - Transferir: Contratar um seguro para cobrir a perda ou outsourcing do serviço.
  - Eliminar: Descontinuar a actividade de negócio que é alvo do risco.

Perguntas Exemplo

- Compare a análise de risco qualitativa com a quantitativa.

Análise de risco qualitativa

- Análise subjectiva e não quantificada
  - Risco determinado por escalas
  - Baseada na elaboração de cenários discutidos entre vários especialistas

Threat = Hacker Accessing Confidential Information	Severity of Threat	Probability of Threat Taking Place	Potential Loss to the Company	Effective-ness of Firewall	Effectiveness of Intrusion Detection System
IT manager	4	2	4	4	3
Database administrator	4	4	4	3	4
Application programmer	2	3	3	4	2
System operator	3	4	3	4	2
Operational manager	5	4	4	4	4
Results	3.6	3.4	3.6	3.8	3

Fonte:CISSP All-in One

Análise de risco quantitativa

- Análise que atribui valores monetários aos riscos
- Asset Value (AV): valor do bem para o negócio
- Exposure Factor (EF): Percentagem de exposição a uma ameaça
- Single Loss Expectancy (SLE): valor de perda numa única concretização de ameaça
  - SLE= AV X EF
- Annualized Rate of Ocurrence (ARO): Número de vezes que a ameaça acontece por ano (histórico)
- Annualized Loss Expectancy (ALE): valor de perda por ano
  - ALE= SLE X ARO

Análise de risco quantitativa

- Uma medida de segurança para mitigar a perda por ano (ALE) nunca pode ter um custo similar por ano

Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annual Loss Expectancy (ALE)
Facility	Fire	$230,000	.1	$23,000
Trade secret	Stolen	$40,000	.01	$400
File server	Failed	$11,500	.1	$1150
Data	Virus	$6500	1.0	$6500
Customer credit card info	Stolen	$300,000	3.0	$900,000

Fonte:CISSP All-in One

Qualitativa VS quantitativa

Characteristic	Qualitative	Quantitative
Employs complex functions	No	Yes
Uses cost/benefit analysis	No	Yes
Results in specific values	No	Yes
Requires guesswork	Yes	No
Supports automation	No	Yes
Involves a high volume of information	No	Yes
Is objective	No	Yes
Uses opinions	Yes	No
Requires significant time and effort	No	Yes
Offers useful and meaningful results	Yes	Yes

Fonte:Cissp Study Guide

Perguntas Exemplo

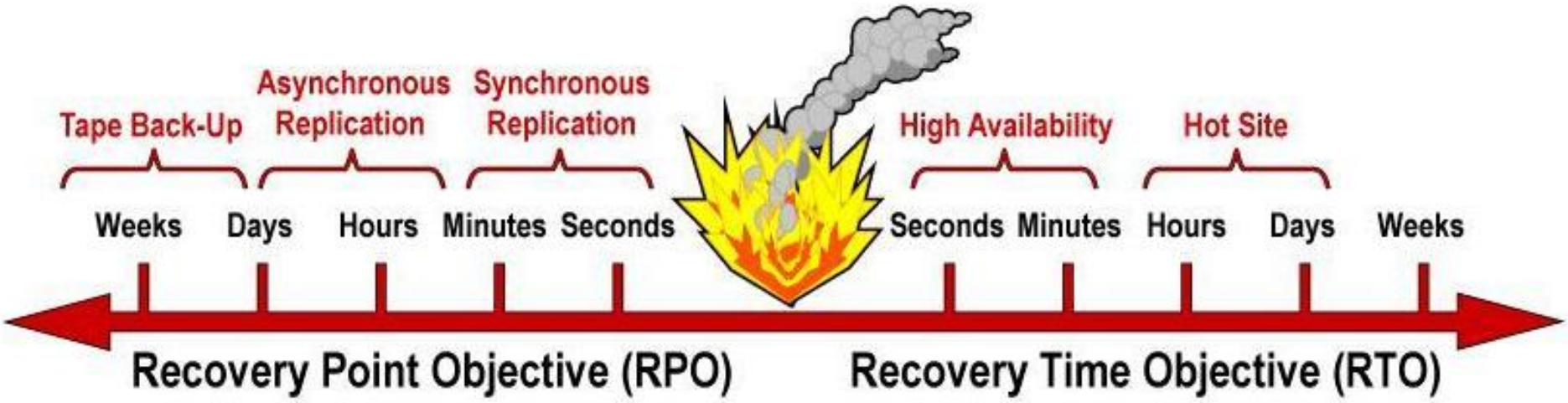
- Descreva o que entende por RTO e RPO.

Análise de impacto no negócio

- **Maximum Tolerable Downtime (MTD).** Tempo máximo que o dono do processo tolera que o processo esteja em baixo.
  - Visão do negócio
  - Também chamado Maximum Tolerable Period of Disruption (MTPD)
- **Recovery Time Objective (RTO).** Tempo máximo de recuperação de um serviço antes que exista impacto nos processos /negócio

Análise de impacto no negócio

- **Recovery Point Objective (RPO)**. Ponto no tempo até qual os dados devem ser recuperados para o serviço funcionar.



Perguntas Exemplo

- Comente a seguinte expressão: ”A empresa onde trabalho é certificada ISO 27002”

ISO 27001

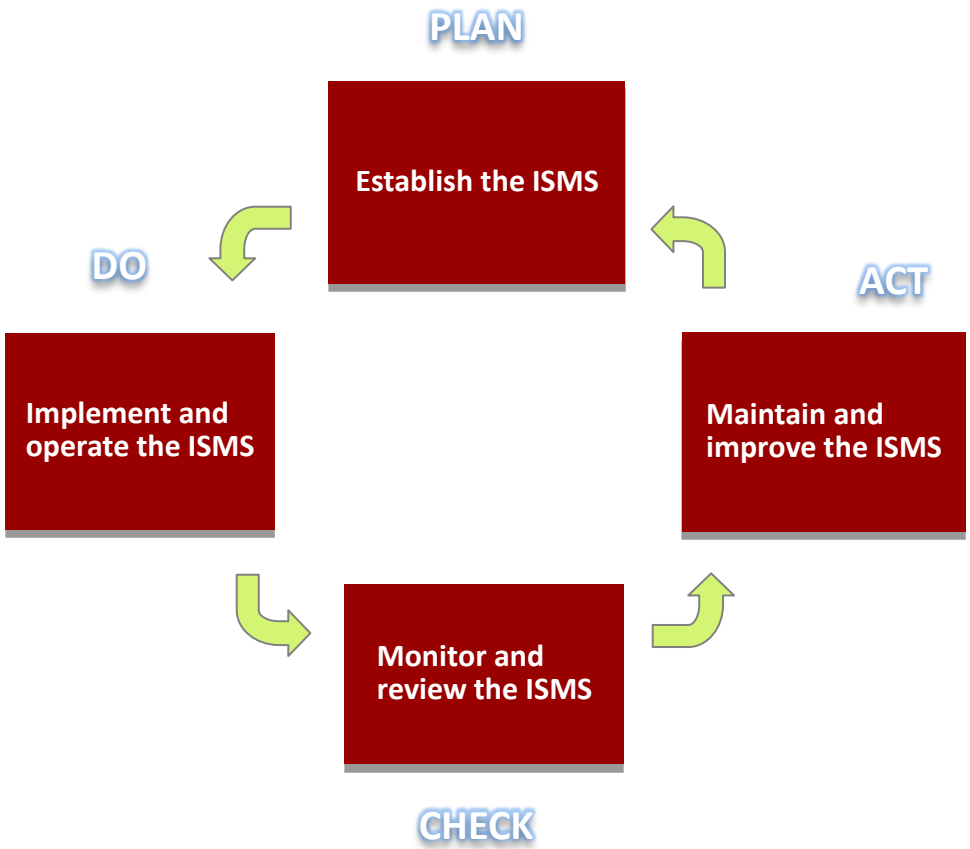
- ISO 27001
  - Norma que estabelece os requisitos para um Sistema de Gestão de Segurança de Informação (SGSI)
  - Existe a possibilidade de certificação do SGSI
- ISO 27002
  - Código de melhores práticas para Segurança da Informação
  - Lista de objectivos de controlo e recomendações de implementação

Perguntas Exemplo

- O que significa o ciclo PDCA no âmbito da ISO 27001?

ISO 27001

- É baseado no ciclo de Deming de melhoria contínua
- Não é apenas um sistema técnico de gestão de segurança de informação mas sim uma metodologia
- O conjunto dos controlos seleccionado como aplicáveis à organização tem o nome de ***SOA – Statement of Applicability***



Perguntas Exemplo

- Descreva o que entende por PCI-DSS.

PCI-DSS

- Payment card industry data security standard
  - Criado pela American Express, Discover Financial Services, JCB, MasterCard Worldwide e Visa International
  - Assegurar protecção de dados e medidas de segurança consistentes e unificadas para transacções de cartões de crédito
  - Aplica-se a todas as instituições que guardam dados de transacções comerciais online