Motivação e Definições

- Papéis e responsabilidades na proteção da informação

Segurança da Informação

Competências:

- Implementar práticas e condutas de segurança da informação no ambiente de TI.

Indicadores:

1. Realiza diagnóstico da segurança da informação a partir de políticas do sistema;
2. Especifica requisitos de segurança da informação do sistema de acordo com as necessidades do sistema; e
3. Implementa as principais práticas e condutas de segurança, garantindo que o sistema computacional desenvolvido esteja de acordo com as normas vigentes no mercado.

Bases Tecnológicas, científicas e instrumentais (conteúdos):

- Papéis e responsabilidades na proteção da informação;

Situação de Aprendizagem:

- Desenvolvimento de vocabulário específico da área e desenvolvimento de provas de conceito relacionado ao vocabulário recém adquirido.

TWITTER

Twitter data breach: Hacker posted list of hacked data of 400 million users-- Check whether your data is leaked or not

Email, username, follower count, creation date, and, in some situations, the users' phone numbers are all included in the sample data.

Written By Zee Media Bureau | Last Updated: Dec 25, 2022, 03:52 PM IST | Source: Bureau

- The sample data includes the data of many more well-known users.
- Hackers posted the list of hacked data on the dark web.
- In late November, the previous breach was discovered.

Trending Photos

DEAVI

Departamento de Avaliação Institucional

HOME AVALIAÇÃO INSTITUCIONAL ENADE

Threat Intelligence | 2 MIN READ | QUICK HITS

Killnet Gloats About DDoS Attacks Downing Starlink, White House

Elon Musk-owned Starlink, WhiteHouse.gov, and the Prince of Wales were targeted by Killnet in apparent retaliation for its support of Ukraine.

Becky Bracken
Editor, Dark Reading

November 29, 2022

Editors' Choice

The Cybersecurity Industry Doesn't Have a Stress Problem — It Has a Leadership Problem
Tyler Farrar, CISO, Exabeam

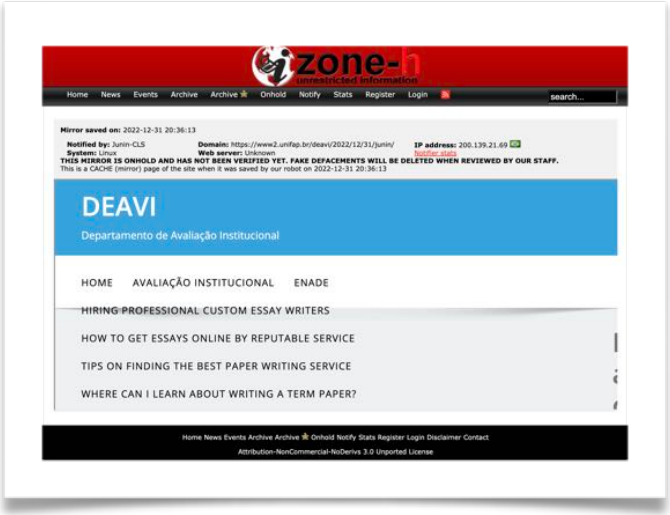
Microsoft Squashes Zero-Day, Actively Exploited Bugs in Dec. Update
Jai Vijayan, Contributing Writer, Dark Reading

Uber Breached, Again, After Attackers Compromise Third-Party Cloud
Elizabeth Montalbano, Contributor, Dark Reading

For Cyberattackers, Popular EDR Tools Can Turn into Destructive Data Wipers
Jai Vijayan, Contributing Writer, Dark Reading


QUESTIONS?
COMMENTS?
CONCERNS?

Segurança da Informação



Confidencialidade

Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados

Integridade

Propriedade de salvaguarda da exatidão e completeza de ativos

Disponibilidade

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada

ISO/IEC 13335-1:2004

Segurança da Informação

Preservação da **confidencialidade**, **integridade** e **disponibilidade** da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Confidencialidade

Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados

Integridade

Propriedade de salvaguarda da exatidão e completeza de ativos

Disponibilidade

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada

ABNT NBR ISO/IEC 17799:2005

Ameaças à confidencialidade

- Exemplos de problemas são:

  - Acesso não autorizado;
  - Vulnerabilidades do ***login/password*** (p.ex. partilha de ***passwords***);
  - Intercepção não autorizada da informação em trânsito (p.ex. ***sniffing***); e
  - Gestão não controlada da informação.

Ameaças à integridade

- Exemplos de problemas são:

  - Erros no software;
  - Mau funcionamento de equipamento;
  - Erros operacionais (e.g. na introdução de dados); e
  - Vírus que corrompem a informação.

Ameaças à disponibilidade

» Exemplos de problemas são:

- Falhas nos equipamentos ou serviços de rede (p.ex. ao nível do hardware/software, falhas de energia, erros/bugs);
- Erros no manuseio do sistema;
- Causas naturais (incêndios e/ou inundações);
- Recursos insuficientes para o correto funcionamento do software; e
- Quando ocorrem ataques propositados para impedir o funcionamento normal do sistema (p.ex. DoS-Denial of Service attacks, SPAM, etc).


QUESTIONS?
COMMENTS?
CONCERNS?

Segurança da Informação

Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como **autenticidade**, **responsabilidade**, **não repúdio** e **confiabilidade**, podem também estar envolvidas.

Autenticidade

Propriedade de assegurar as veracidades do emissor e do receptor de informações trocadas.

Não repúdio

Ou Irretratabilidade, é a garantia de que o autor de uma informação não poderá negar falsamente a autoria de tal informação.

Confiabilidade

Garantir que um sistema vai se comportar segundo o esperado e projetado.

ABNT NBR ISO/IEC 17799:2005


QUESTIONS?
COMMENTS?
CONCERNS?

Segurança da Informação

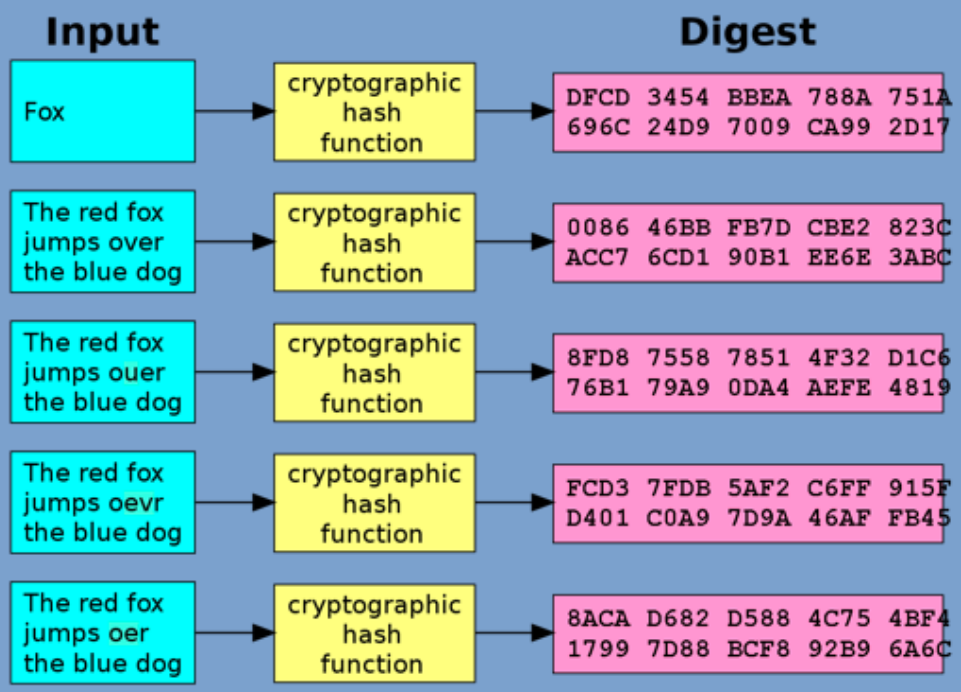
- Confidencialidade
- Integridade
- Disponibilidade
- Não repúdio
- Autenticidade
- Confiabilidade

Ferramentas: criptografia e senha.

Segurança da Informação

- Confidencialidade
- Integridade
- Disponibilidade
- Não repúdio
- Autenticidade
- Confiabilidade

Ferramentas como os algoritmos de hash permitem confirmar se a informação foi alterada.

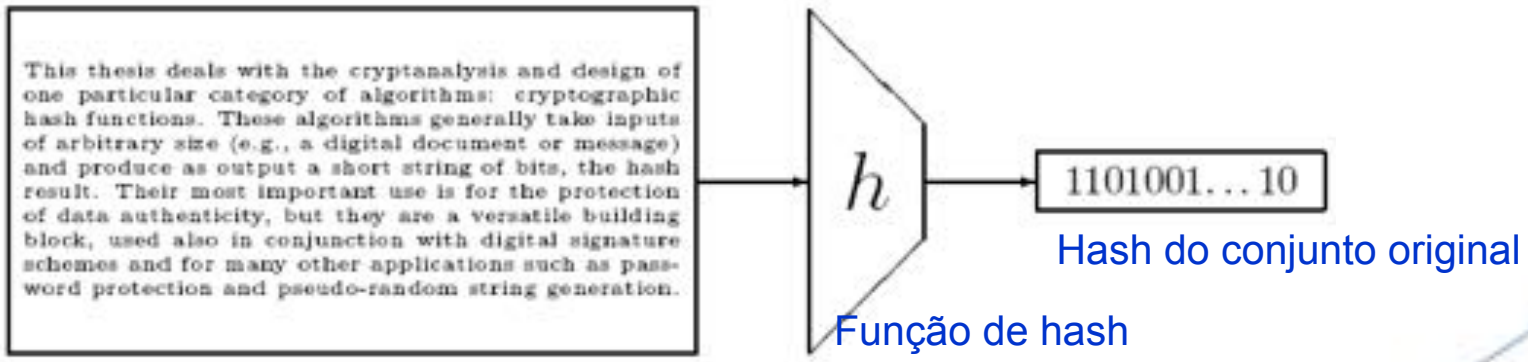


Hash
Introdução

» Também chamada de função de espalhamento, são funções que convertem uma sequência de bits em um conjunto de strings de tamanho fixo;

» Embora matematicamente seja possível encontrar o mesmo hash para conjuntos distintos de bits, isso é difícil na prática. Isto é chamado de colisão.

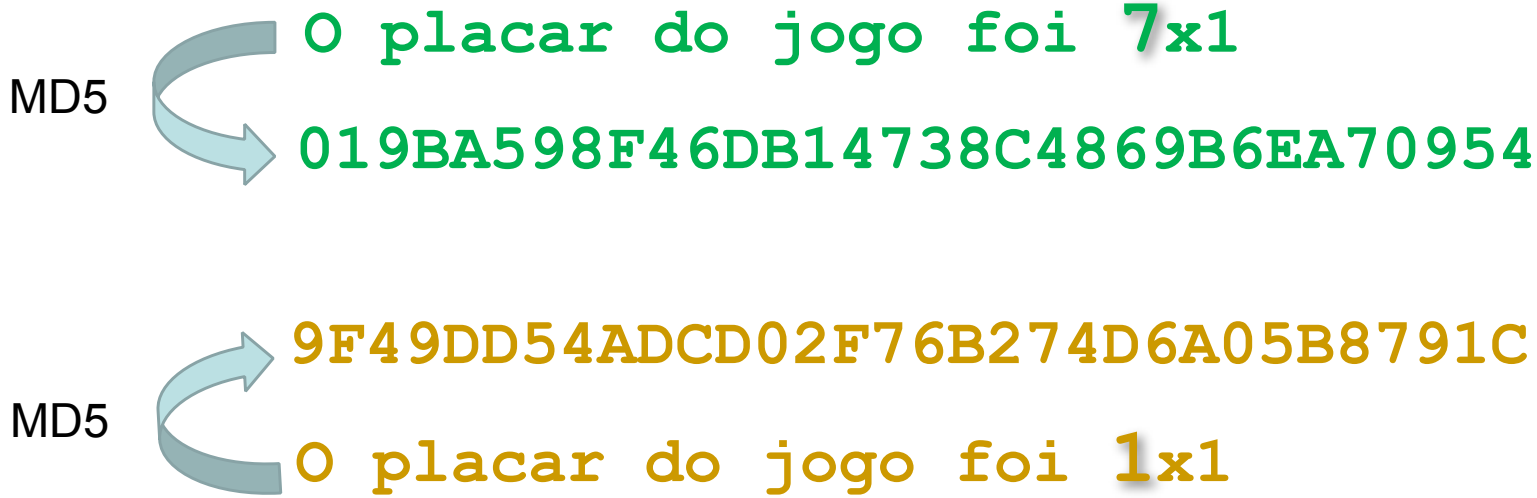
» Uma boa função *hash é aquela que: (i) é simples de ser computada e (ii) minimiza o número de colisões, isto é, para cada chave de entrada, qualquer uma das saídas possíveis é igualmente provável de ocorrer.*



Hash

Algoritmo de cálculo de identificador único da informação.

A modificação de um bit da informação de entrada altera totalmente o resultado.



Hash

ALGORITMO	TAMANHO BITS
MD5	128
SHA-1	160
SHA-224	224
SHA-256	256
SHA-384	284
SHA-512	512

Hash

Exemplo de funções hash:

Entrada: **Segurança da Informação**

MD5 (128 bits): **2597568A2A61B57FAFD4ACED25985EAA**

SHA-1 (160 bits): **A85E94C5F1FDF90520C80F9F90FCFCE4A317D141**

SHA-256: **EC1A757E3C679B372BADFD01A7453AB4A6C80AB40**
D424D0135765DCBB50E8252

Hash
MD5: Message Digest

- Desenvolvidos pela RSA em 1991
- MD5 proposto em 1991 por Rivest (MD4)
- Difícil de se provar o nível de segurança
- MD5 roda 30% mais lento que MD4
- MD4 e MD5 geram valor ***hash*** de 128 bits
- Vulnerabilidade:
  - Como o MD5 faz apenas uma passagem sobre os dados, se dois prefixos com o mesmo hash forem construídos, um sufixo comum pode ser adicionado a ambos para tornar uma colisão mais provável. Deste modo é possível que duas strings diferentes produzam o mesmo hash.
- Exemplo
  - MD5("The quick brown fox jumps over the lazy dog") 9e107d9d372bb6826bd81d3542a419d6
  - MD5("The quick brown fox jumps over the lazy ***c***og") = 1055d3e698d289f2af8663725127bd4b

Hash
SHA

- Surgiu em 1993, considerado sucessor do MD5
- Grande variedade de aplicações: TSL, SSL, PGP, SSH, IPSec, etc.
- Também possui vulnerabilidade

Hash
Comparação entre MD5 e SHA

- Pertencem a mesma família de Funções Hash: MDx-class;
- MD5 é mais vulnerável a ataques de força-bruta devido a sua menor saída: 128 bits contra 160 bits do SHA;
- O MD5 é mais rápido que o SHA, pois este último possui mais etapas em seu algoritmo (80 contra 64 do MD5) e um buffer maior (160 bits contra 128 bits do MD5);
- Já foram encontradas colisões para a função de compressão do MD5, enquanto que o SHA permanece inabalável.

Hash

Pode acontecer de duas informações possuirem o mesmo valor de hash?

SIM!

Hash

Por conta disso usamos mais de um algoritmo ao mesmo tempo, para minimizar a probabilidade de obtermos uma colisão.

Entrada: **Segurança da Informação**

MD5 (128 bits): **2597568A2A61B57FAFD4ACED25985EAA**

SHA-1 (160 bits): **A85E94C5F1FDF90520C80F9F90FCFCE4A317D141**

SHA-256: **EC1A757E3C679B372BADFD01A7453AB4A6C80AB40 D424D0135765DCBB50E8252**

Hash

Estas duas imagens possuem o mesmo valor de ***hash***

Hash

Ataque de inversão: encontrar uma inversão.

Probabilidade: $1/2^n$.

Quantidade de operações: 2^n

Ataque de aniversário:

Num grupo de k pessoas, qual o valor mínimo de k para que a probabilidade de que pelos menos duas façam aniversário no mesmo dia seja maior do que 50%?

$1 – 365x364x...x(365 –k +1)/365k > ½ \Rightarrow k = 23$

- Considerando k entradas e $m = 2^n$ possíveis saídas, qual o valor de k para que a probabilidade de colisão seja maior do que 50%?

$1 – m!/[(m-k)!mk] \approx 1 – e[-k(k-1)]/n > ½ \Rightarrow k \approx m^{1/2} = 2^{n/2}$

Hash
Aplicações

- **Assinatura Digital:** para assegurar que o documento não foi alterado; para verificar a autenticidade de um documento; Distribuição do software;
- **Digital timestamping:** assegurar a data e hora da criação do documento;
- **Proteção de senhas:** armazena-se o hash da senha;
- **Autenticação da mensagem:** assegurar que a mesma não foi alterada.

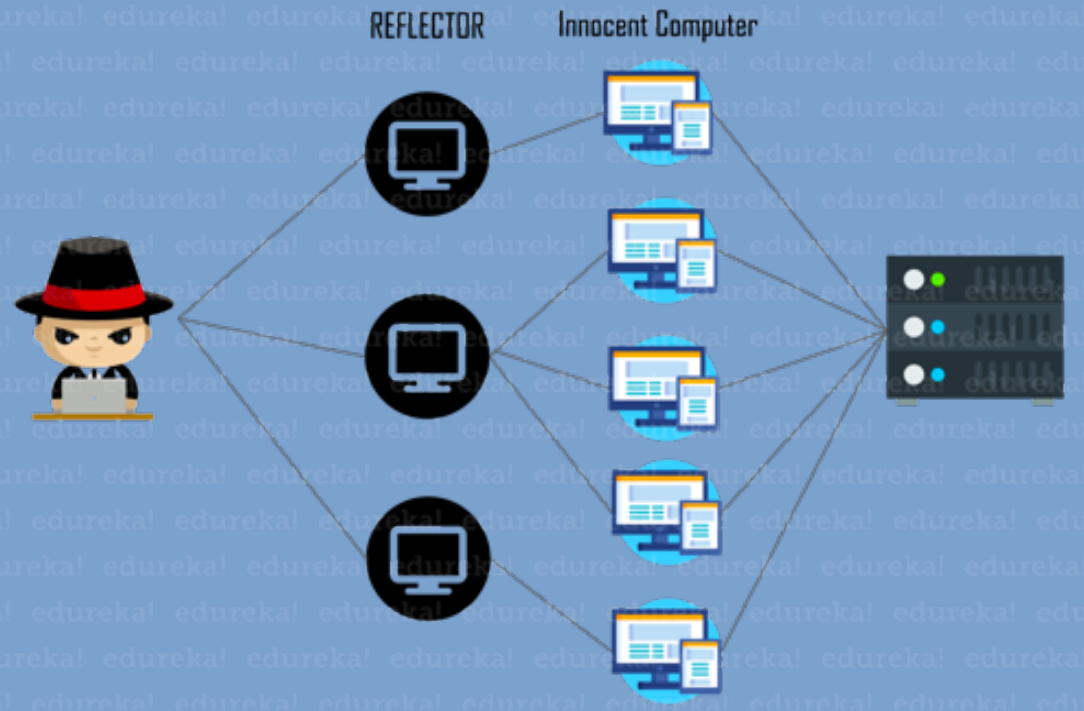

QUESTIONS?
COMMENTS?
CONCERNS?

Segurança da Informação

- Confidencialidade
- Integridade
- Disponibilidade
- Não repúdio
- Autenticidade
- Confiabilidade

Disponibilidade

É assegurada através do uso de recursos como geradores de energia, computadores de "reserva".

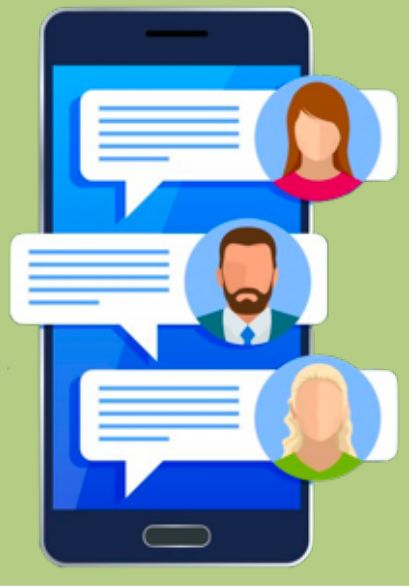


Segurança da Informação

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Confiabilidade

Não Repúdio ou Irretratabilidade

Autenticidade e Integridade juntas garantem o Não-Repúdio; Condição necessária à validade jurídica das informações digitais. Recursos como o uso de criptografia são usados para esse fim.



Segurança da Informação

- Confidencialidade
- Integridade
- Disponibilidade
- Não repúdio
- Confiabilidade

Autenticidade

Recursos como senhas, biometria, assinatura digital e certificação digital são usados para esse fim.

Segurança da Informação

- Confidencialidade
- Integridade
- Disponibilidade
- Não repúdio
- Autenticidade

Confiabilidade

Garantir que um sistema vai se comportar segundo o esperado e projetado.


QUESTIONS?
COMMENTS?
CONCERNS?

Segurança da Informação

Ativo é qualquer *coisa* que tenha valor para a organização.

Ativo

Segurança da Informação

Exemplos de ativos:

- **Ativos de informação:** base de dados e arquivos, contratos e acordos, etc;
- **Ativos de software:** aplicativos, sistemas, etc;
- **Ativos físicos:** equipamentos computacionais, de comunicação, etc;
- **Serviços:** Eletricidade, refrigeração, etc;
- Pessoas e suas qualificações, habilidades e experiências; e
- Intangíveis, tais como a reputação e a imagem da organização.

Ativo

Segurança da Informação

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Segurança Informação

Ameaças

Vulnerabilidades

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

Segurança Informação

Ameaças

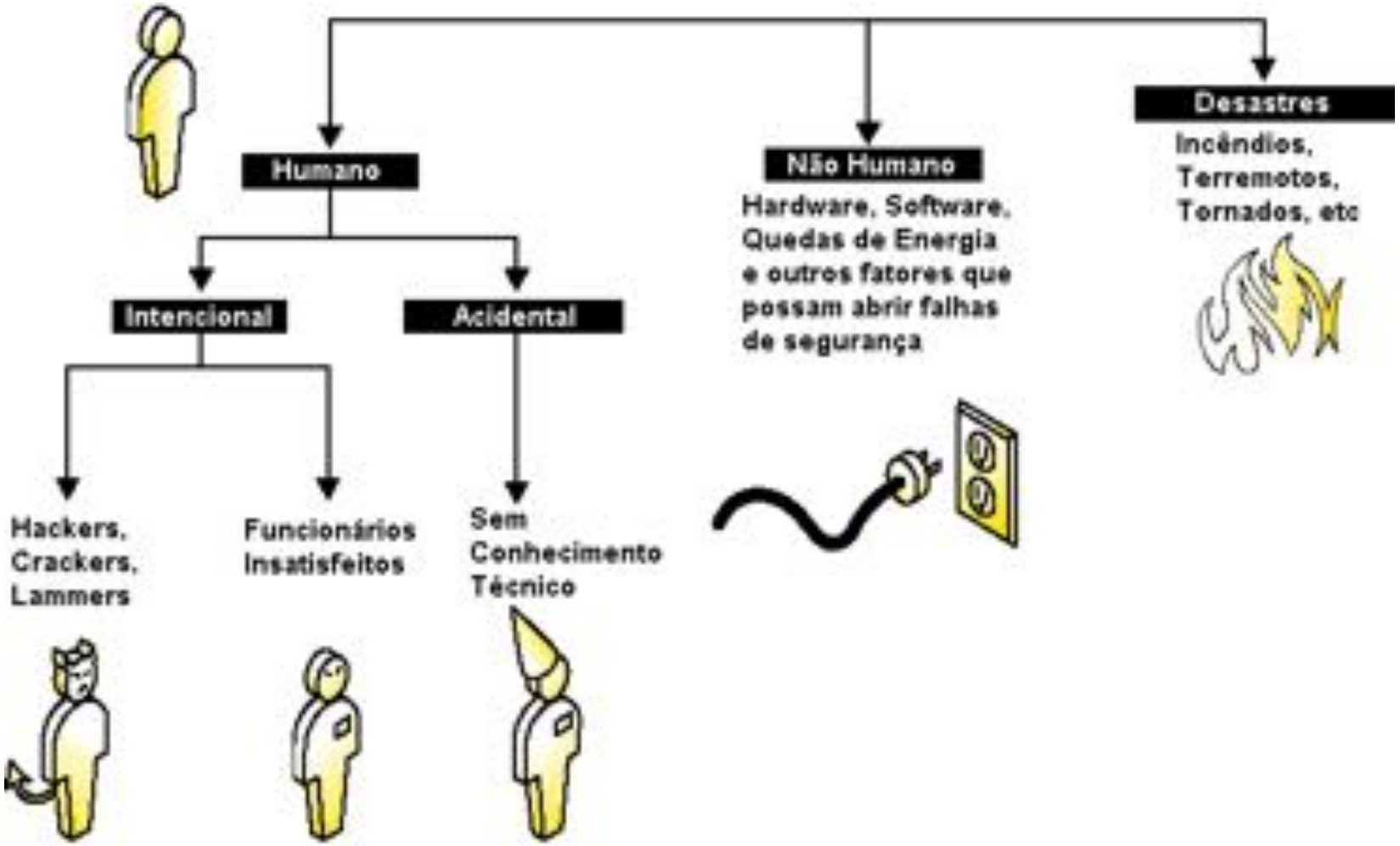
Vulnerabilidades

Ameaças Físicas: Falhas dos Equipamentos e Instalações; e

Ameaças Lógicas: Vulnerabilidades em softwares, como bugs.


Ameaças

Ameaças


Humano
Não Humano
Desastres
Incêndios, Terremotos, Tornados, etc
Hardware, Software, Quedas de Energia e outros fatores que possam abrir falhas de segurança
Intencional
Acidental
Hackers, Crackers, Lammers
Funcionários Insatisfeitos
Sem Conhecimento Técnico


QUESTIONS?
COMMENTS?
CONCERNS?

Segurança Informação

Ameaças

Vulnerabilidades

Medidas de Proteção (Controles)

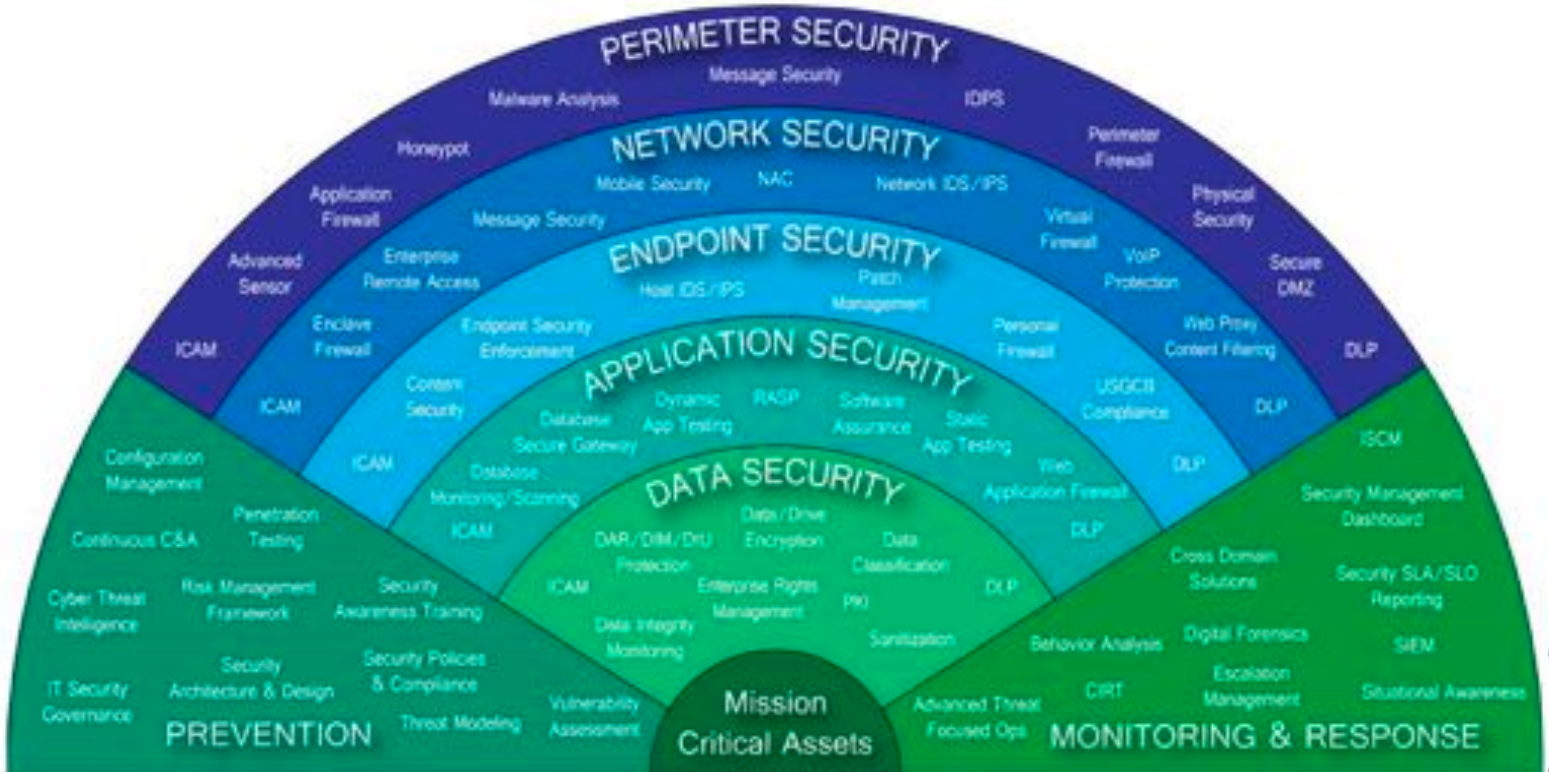
Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

Classificação das proteções

- Lógica
  - Permissões em sistemas de arquivos
  - Firewalls
  - Perfis de usuários em aplicações
- Física
  - Portas
  - Fechaduras
  - Guardas
- Administrativa
  - Políticas
  - Normas
  - Procedimentos

Tipos de proteções

» Uma implementação eficaz de segurança se baseia na utilização de diferentes tipos de proteções
  – As proteções complementam-se, sobrepondo-se e fornecendo redundância caso alguma delas falhe.



Tipos de proteções

- Preventiva
  - Impedir ou dificultar uma violação de segurança em potencial com a implantação de uma contramedida
    - Evita que incidentes ocorram
- Desencorajadora
  - Reduzir a ameaça, desencorajando a ação pelo medo ou pela dúvida
    - Desencoraja a prática de ações
- Limitadora
  - Reduzir o risco reduzindo o valor das perdas potenciais ou reduzindo a probabilidade de ocorrer a perda
    - Diminui os danos causados

Tipos de proteções

- Monitoradora
  - Monitora o estado e o funcionamento
- Detectora
  - Determinar que uma violação de segurança é iminente, está em andamento, ou que ocorreu recentemente, e assim tornar possível tomar alguma ação para reduzir a perda em potencial
    - Detecta a ocorrência de incidentes
- Reativa
  - Reage a determinados incidentes

Tipos de proteções

- Corretiva
  - Alterar a arquitetura de segurança utilizada com o objetivo de eliminar ou reduzir o risco de recorrência de uma violação de segurança ou ameaça(s), tais como, eliminando a(s) vulnerabilidade(s).
    - Repara falhas existentes
- Recuperadora
  - Restaurar a um estado normal de operação do sistema, compensando uma violação de segurança, possivelmente através da eliminação ou reparação de seus efeitos.
    - Plano de contingência
    - Repara danos causados por incidentes


QUESTIONS?
COMMENTS?
CONCERNS?

ormação

Incidente: somente se aplica para os eventos que têm uma probabilidade significativa de causar um problema com a segurança da informação;

Vulnerabilidades

Medidas de Proteção (Controles)

Incidente

Segurança Informação

Ameaças

Vulnerabilidades

Incidente

Medidas de Proteção
(Controles)

IMPACTO À ORGANIZAÇÃO

Impacto à Organização

Possíveis efeitos de um ataque ou invasão

Exemplos:

- Indisponibilidade do serviço;
- Uso não autorizado ou mau uso dos sistemas;
- Perda ou alteração de dados;
- Perda financeira;
- Perda de confiança;
- Alteração de site (web site defacement);
- Dano a imagem da empresa; e
- Perda de mercado.


QUESTIONS?
COMMENTS?
CONCERNS?

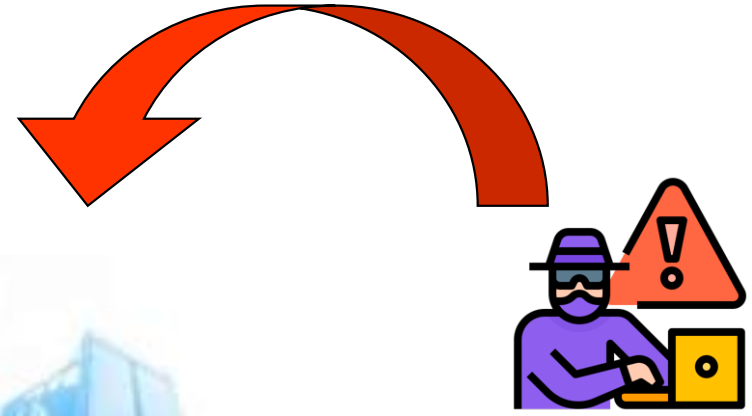
Risco: combinação da probabilidade de um evento e de suas consequências;

ormação

Risco?

Vulnerabilidades

Medidas de Proteção (Controles)



Incidente

IMPACTO À ORGANIZAÇÃO

Risco

Potencial de uma ameaça (evento) se concretizar, através de uma vulnerabilidade, e causar impactos

O tratamento (processo de seleção e implementação de medidas (controles) para modificar um risco) do risco engloba:

Aceitação: quando o custo de implementação é maior que o impacto que pode causar;

Redução: tomar ações para diminuir o custo;

Transferência: mover o risco para um terceiro, criando compensações, quase sempre menores, sobre as perdas; e

Ignorar: contar apenas com a sorte.

Risco

O tratamento do risco faz parte de um processo (metodologia) que ainda envolve:

Análise de Risco: Análise das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência;

Risco

O tratamento do risco faz parte de um processo (metodologia) que ainda envolve:

Avaliação do Risco: processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco;

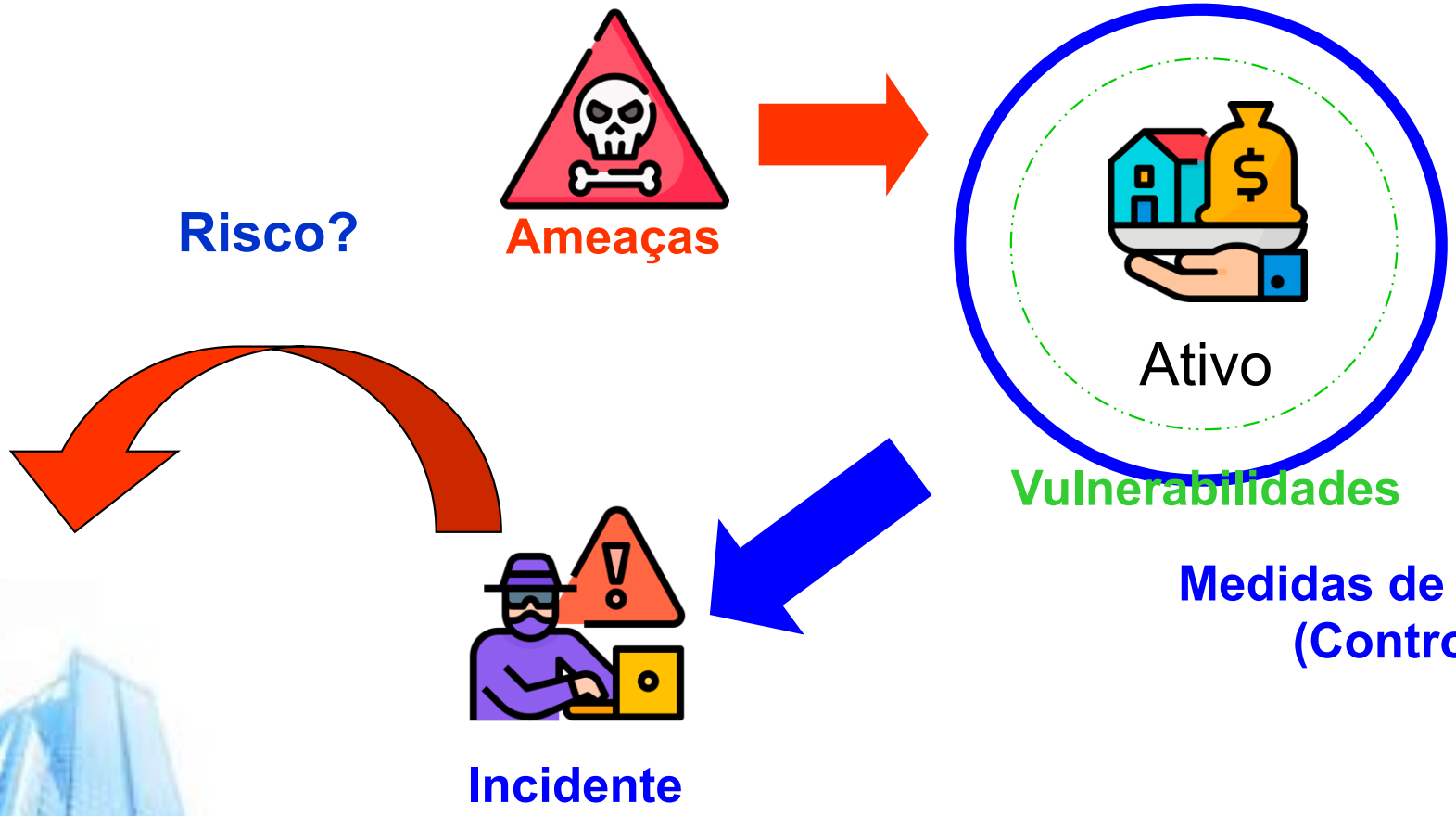
Risco

O tratamento do risco faz parte de um processo (metodologia) que ainda envolve:

Gerenciamento de Risco: Processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável;


QUESTIONS?
COMMENTS?
CONCERNS?

Segurança da Informação



IMPACTO À ORGANIZAÇÃO

Ataque

- Duas classes: passivos e ativos
- Passivos:
  - Interceptação
    - Descoberta de conteúdo
    - Análise de tráfego
- Ativos:
  - Interrupção
  - Modificação
  - Fabricação
  - Repetição

Ataque

Por quê existem as invasões aos sistemas?

- Orgulho;
- Exibicionismo/fama;
- Busca de novos desafios;
- Curiosidade;
- Protesto;
- Roubo de informações;
- Financeiro;
- Uso de recursos adicionais;
- Vantagem competitiva; e
- Vingança.

Tipos de Ataques

Negação de serviços

Definição: Exaurir um recurso ou exploração de um determinado formato/metodologia/algoritmo

- Syn Flood – inundar a fila de SYN para negar novas conexões;
- Buffer overflow – colocar mais informações do que cabe no buffer;
- Distributed DoS (DDoS) – ataque em massa de negação de serviços;
- Ping of Death – envio de pacote com mais de 65507 bytes; e
- Smurf – envio de pacote ICMP em broadcast a partir de uma máquina, sendo inundada com as respostas recebidas.

Tipos de Ataques

Simulação

- Definição: forjar algum dado e/ou se fazer passar para algum recurso válido.

- IP Spoofing – uso do IP de uma máquina para acessar outra;
- DNS Spoofing – assumir o DNS de outro sistema - Investigação; e
- Port scanning – varredura de portas para tentar se conectar e invadir.

Tipos de Ataques

Investigação

- Definição: coleta de dados para a formulação de um ataque.

- Port scanning – varredura de portas para tentar se conectar e invadir; e
- Scam- Acesso a um grande número de pessoas, via email, com link para sites clonados que pedem informações pessoais;
- Packet Sniffing – escuta e inspeciona cada pacote da rede e
- IP/Session Hijacking – interceptação da seção pelo invasor.

Tipos de Ataques

Quebras de Senha

- Definição: coleta de dados para a formulação de um ataque.

- Dicionário: uso de conjunto de palavras conhecidas para a geração de senhas; e
- Força bruta – tentativa e erro.

Tipos de Ataques

Outros

- Alteração de site (web defacement);
- Engenharia social;
- Ataque físico às instalações da empresa;
- Botnet - rede zumbi cooptada para a realização de um ataque malicioso;
- Uso de cavalos de tróia e códigos maliciosos;
- Trashing – revirar lixo em busca de informações;
- War dialing – liga para vários números de telefone para identificar os que tem modem instalado; e
- Ransomware - sequestro de dados através da encriptação dos sistemas de armazenamento.


QUESTIONS?
COMMENTS?
CONCERNS?

Exercícios

1. Pesquise na internet casos de quebras da CID que tenham ocorrido nos últimos 6 meses.

2. Implemente uma aplicação que calcule o hash de frases fornecidas pelo usuário. Algoritmos: MD5 e SHA1.

3. Implemente uma aplicação que confirme que as imagens abaixo realmente geram uma colisão quando o algoritmo utilizado é o MD5. Calculo o hashi SHA256 de cada uma delas e demonstre que são diferentes.

4. Para cada tipo de proteção, forneça um exemplo que podemos observar na Faculdade SENAC/RJ.

Reflexão

Contribuição do tópico para a minha formação?

1. Entendimento dos termos;

   a. confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade, confiabilidade, vulnerabilidade, ativo, proteção, ameaça, incidente, risco e ataque.

2. Identificação dos requisitos de software que devem ser atendidos;

   a. hash e senha.

3. Implementação de medidas de controle que podem compor aplicações que serão desenvolvidas.


QUESTIONS?
COMMENTS?
CONCERNS?