





SEGURANÇA DA INFORMAÇÃO

TÓPICOS ESPECIAIS EM ENGENHARIA
PRINCIPAIS CONCEITOS DE SEG. INFO.



AGENDA

- ✕ Principais Conceitos de Segurança da Informação
- ✕ Medidas de Prevenção
- ✕ Gestão de Riscos

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Confidencialidade

Integridade

Disponibilidade

Autenticidade

Irretratabilidade

Pessoas

Processos

Tecnologia



CONFIDENCIALIDADE

É uma característica da informação que diz respeito ao **direito de acesso**.

Garantir que a informação esteja **acessível** apenas para pessoas/organizações que tenham **permissão de acesso**, prevenindo, assim, **revelação não autorizada**.



MEDIDAS DE CONFIABILIDADE

- ✗ Necessidade de conhecer
- ✗ Política da Mesa Limpa
- ✗ Gerenciamento de Acesso Lógico
 - Configurações
- ✗ Separação de Funções
- ✗ Ambientes Dev / Hml / Prd
- ✗ Preenchimento de Tráfego

INTEGRIDADE

É uma característica da informação que diz respeito à sua **exatidão**.

Garantir que a informação seja alterada somente por pessoas **autorizadas** e em situações que efetivamente demandem a **alteração** legítima.





MEDIDAS DE INTEGRIDADE

- ✗ Mudanças não Autorizadas
 - Validação na atribuição de preço
- ✗ Termos consistentens
 - Freguês / Cliente
- ✗ Ações gravadas – Logs
- ✗ Segregar funções
 - > 1 pessoa



DISPONIBILIDADE

Garantir que a informação esteja **disponível**, sempre que necessário, aos usuários e/ou sistemas associados que tenham direito de acesso a ela.

Características:

- Oportunidade
- Continuidade
- Robustez



MEDIDAS DE DISPONIBILIDADE

- ✗ Gestão de dados voltada a minimizar risco de perder informações
- ✗ Armazenamento Rede/Nuvem
- ✗ Procedimentos de Backup
- ✗ Requisitos Legais
 - Tempo de Armazenamento Backup



AUTENTICIDADE

Diz respeito à **certeza da origem** da informação.

Garantir que a informação **provem** da fonte anunciada e que não foi alvo de **mutação** ao longo de sua transmissão

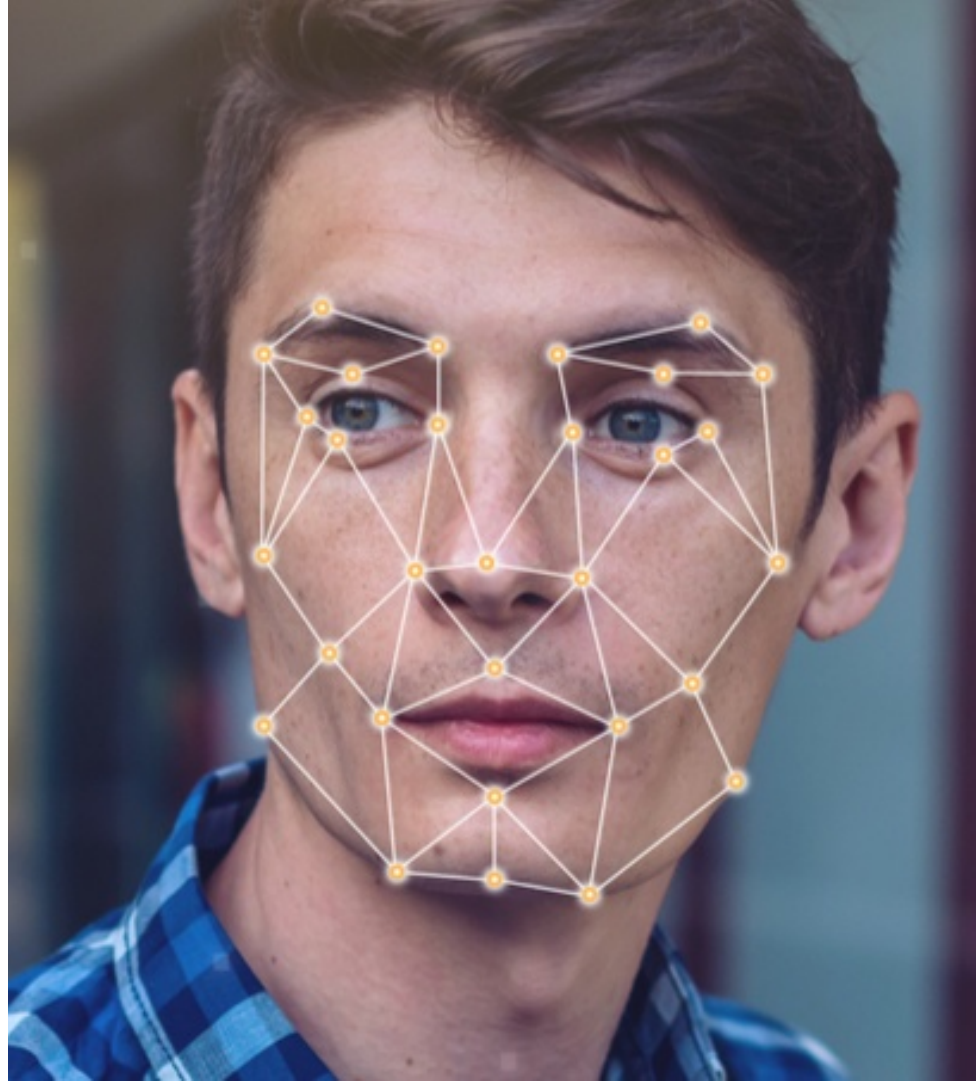
**SO YOU'RE SAYING I
MUST OPEN AN ATTACHMENT**

FOR MY CASH REFUND ?

IRRETRATABILIDADE

Diz respeito à garantia de que o autor de determinada ação **não possa negar** tal ação.

Garantir meios que identifique inequivocamente o autor de uma ação.







COMO PODEMOS GARANTIR A SEGURANÇA DA INFORMAÇÃO?

(OU NO MÍNIMO MITIGAR OS RISCOS)

CRIPTOGRAFIA

Arte de escrever mensagens em forma cifrada

Conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consiga decifrá-la

- [x] Confidencialidade
- [x] Integridade
- [] Disponibilidade
- [x] Autenticidade
- [x] Irretratabilidade

TIPOS DE CHAVES

Simétricas

A mesma chave é utilizada tanto pelo emissor quanto por quem recebe a informação.

Não é recomendado uso para informações sensíveis

Assimétricas

Uma chave privada e outra pública.

Pública: chave de codificação e enviada a quem for lhe mandar informações.

Privada: chave secreta para a decodificação.

HEXAGRAMA PARKERIANO

Confidencialidade

- Donn B. Parker

Disponibilidade

- Atributos Atômicos

Integridade

Utilidade

Posse / Controle

Autenticidade



EXEMPLOS QUEBRA DE PRINCÍPIOS

Confidencialidade

- Servidor de Banco de Dados

Disponibilidade

- Infectado código malicioso

Integridade

- Ransomware

Utilidade

- Embaralhou arquivos usando criptografia

Posse / Controle

- Pedindo BitCoins como resgate

Autenticidade

EXEMPLOS QUEBRA DE PRINCÍPIOS

Confidencialidade

- Servidor de Banco de Dados

Disponibilidade

- Infectado código malicioso

Integridade

- Ransomware

Utilidade

- Embaralhou arquivos usando criptografia

Posse / Controle

- Pedindo BitCoins como resgate

Autenticidade

EXEMPLOS QUEBRA DE PRINCÍPIOS

Confidencialidade

- Colaborador desprovido de honestidade

Disponibilidade

- Cópia não autorizada de um BD

Integridade

- Enviou dados para HD externo

Utilidade

- Deletou arquivos do servidor

Posse / Controle

Autenticidade

EXEMPLOS QUEBRA DE PRINCÍPIOS

Confidencialidade

- Servidor de Banco de Dados

Disponibilidade

- Infectado código malicioso

Integridade

- Ransomware

Utilidade

- Embaralhou arquivos usando criptografia

Posse / Controle

- Pedindo BitCoins como resgate

Autenticidade



Foco

O que
importa?

O que é
perigoso?

O que é
real?

RISCOS

Probabilidade de um agente ameaçador tirar vantagem de uma vulnerabilidade e o correspondente impacto no negócio



EXEMPLOS DE RISCOS

- ✕ Incêndio
- ✕ Funcionário que não trabalha mais no RH
- ✕ Alguém se passando por funcionário
- ✕ Falha de Energia
- ✕ Hacker consegue obter acesso à rede

AMEAÇA

Potencial causa de um incidente não desejado

Agente ameaçador tira vantagem de uma vulnerabilidade



EXEMPLOS DE AMEAÇAS

- ✕ Invasor acessando rede por porta no firewall
- ✕ Processo acessando dados não-autorizados
- ✕ Tornado
- ✕ Funcionário cometendo erro (não)intencional expondo dados sensíveis
 - ou afetando integridade

EXPOSIÇÃO

Fato de estar exposto às perdas provenientes de um agente ameaçador

Vulnerabilidade expõe organização a possíveis ameaças



EXEMPLOS DE EXPOSIÇÃO

- ✗ Gestão de Senhas Fracas
- ✗ Cabeamento não inspecionado
- ✗ Medidas de proteção de incêndio insuficientes

CONTRAMEDIDA / SALVAGUARDA

Prática para mitigar risco em potencial



EXEMPLOS DE CONTRAMEDIDAS

- ✕ Gestão de Senhas Fortes
- ✕ Mecanismos de Controle de Acesso a SO
- ✕ Senhas de BIOS (basic input/output system)
- ✕ Treinamento de Consientização de Segurança



OBRIGADO!

Não esqueça de enviar sua
maior dúvida pelo link que está
no github.

ezarpelao@unaerp.br

<https://github.com/elizarp/unaerp>

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- ✕ Presentation template by [SlidesCarnival](#)
- ✕ Photographs by [Unsplash](#)