UNI
METRO
CAMP
wyden

Introdução à Segurança da Informação - ARA0064

Prof. José Luiz Alonso Silva, MsC
E-mail: jose.lsilva@unimetrocamp.edu.br

5.1 Preservação da Confidencialidade, Integridade e Disponibilidade (CID)

UNI
METRO
CAMP
wyden

Temas da Aula

- CID
  - Confiabilidade
  - Integridade
  - Disponibilidade
- Gestão de Risco

UNI METRO CAMP wyden

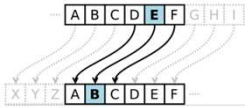
Informações

- Pesquisa Institucional - ISA
  - SAI → Menu → Avaliação Institucional
  - Até 27/05/24
- Simulado 2
  - simulado.wyden.com.br
  - Até 06/06/24
- Lista de Desejos e Aceite no Contrato
  - renova.wyden.com.br
  - Até 08/06/24

UNI METRO CAMP wyden

Melhores Momentos

Dados criptografados só podem ser lidos ou processados depois de serem descriptografados

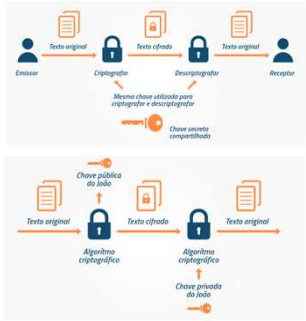


Criptografia de Dados

Identidade eletrônica de uma pessoa ou empresa
Carteira de Identificação Virtual

Possibilita assinar documentos à distância com o mesmo valor jurídico da assinatura física

Certificação Digital



Chaves Simétrica e Assimétrica

UNI METRO CAMP wyden

Atividade Aula 10
Criptografia

- Utilizar um aplicativo ou página web que criptografe uma frase utilizando chave
- **Objetivo**: Consolidar conhecimento do uso de chave criptográfica

- 16 Respostas no Forms

UNI METRO CAMP wyden

Objetivo da Aula

- Definir vulnerabilidades, ameaças, ataques e termos relacionados à preservação da confidencialidade, integridade e disponibilidade (CID)

Imagem: Autor utilizando Wordart

UNI METRO CAMP wyden

Temas de Aprendizagem

1. PRINCÍPIOS DA SEGURANÇA E O CICLO DE VIDA DA INFORMAÇÃO 1.1 SEGURANÇA DA INFORMAÇÃO 1.2 SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO
2. AMEAÇAS E VULNERABILIDADES À SEGURANÇA DE INFORMAÇÃO 2.1 TIPOS DE AMEAÇAS E VULNERABILIDADES 2.2 ATAQUES CIBERNÉTICOS
3. NORMAS DE SEGURANÇA DA INFORMAÇÃO 3.1 FINALIDADES E BENEFÍCIOS DAS NORMAS 3.2 APLICAÇÃO DAS NORMAS
4. BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO 4.1 SENHAS, TREINAMENTO E PROTEÇÃO 4.2 CONTROLE DE ACESSO, VÍRUS E BACKUPS 4.3 CRIPTOGRAFIA DE DADOS E CERTIFICADO DIGITAL
5. GESTÃO DE RISCO 5.1 PRESERVAÇÃO DA CONFIDENCIALIDADE, INTEGRIDADE E DISPONILIDADE (CID) 5.2 ETAPAS DA GESTÃO DE RISCOS
6. GESTÃO DE CONTINUIDADE DO NEGÓCIO (ATIVIDADE PRÁTICA SUPERVISIONADA) 6.1 PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN) 6.2 ETAPAS DO PCN 6.3 PGCN E BIBLIOTECA ITIL

UNI METRO CAMP wyden

Contexto do CID

- Relembrando ...

Vulnerabilidades

Fraquezas ou falhas em sistemas, redes, aplicativos ou processos

Podem ser exploradas para comprometer a segurança das informações

Ameaças

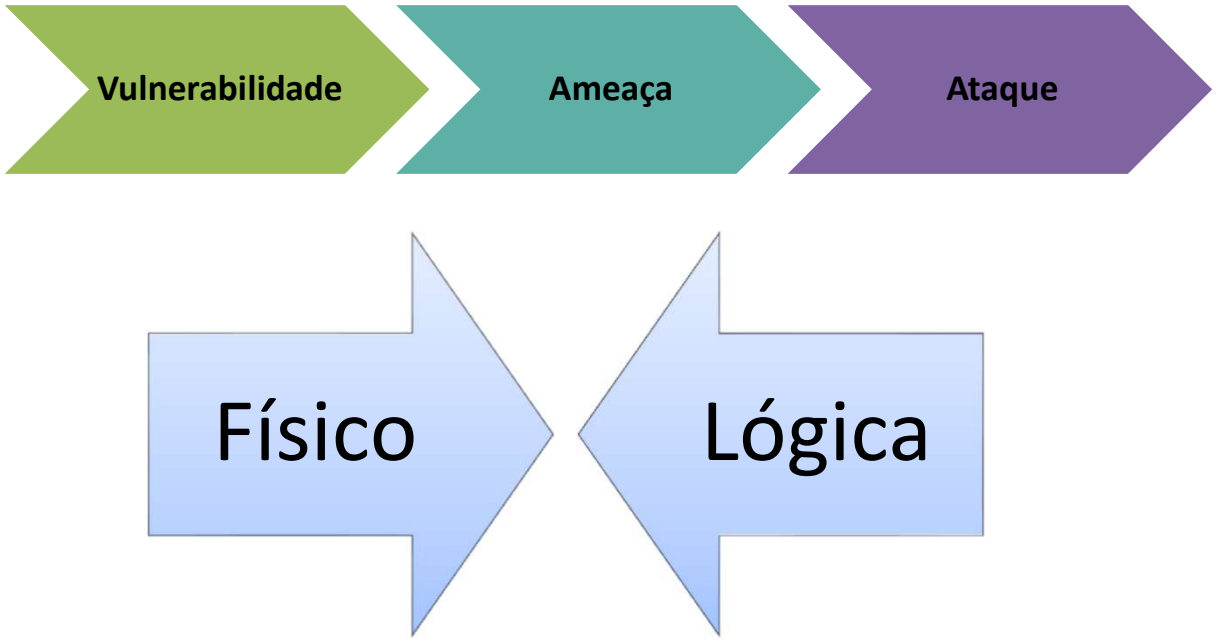
Eventos, pessoas ou entidades que têm a capacidade de explorar vulnerabilidades e causar danos aos sistemas e dados

Ataques

São ações realizadas por ameaças com o objetivo de explorar vulnerabilidades e comprometer a segurança das informações

Imagem: Banco de imagens do MS Power Point

Contexto do CID

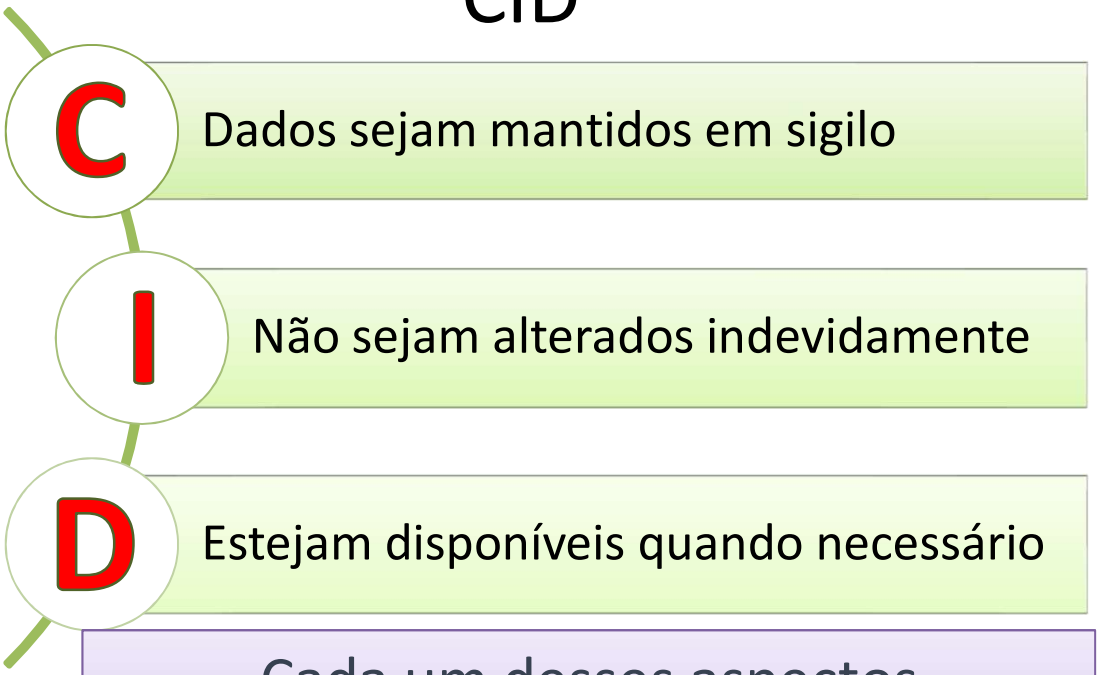


Contexto do CID

Na era da informação, a segurança dos dados é uma preocupação crucial para empresas e indivíduos

A preservação da Confidencialidade, Integridade e Disponibilidade das informações

CID

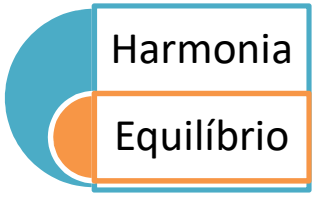


Cada um desses aspectos desempenha um papel importante na proteção dos dados

UNI METRO CAMP wyden

CID

Ações devem ser desenvolvidas simultaneamente	São vitais para o estabelecimento da cultura da proteção de dados



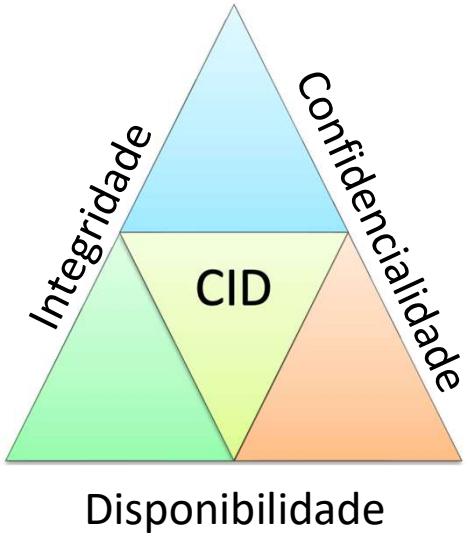
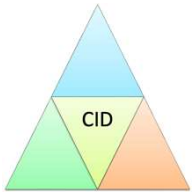


Imagem: autor

Confidencialidade



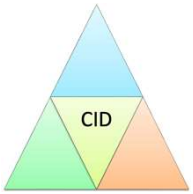
Proteção de informações sensíveis contra acesso não autorizado

Garantir que apenas pessoas autorizadas possam acessar determinados dados ou recurso

Garantir a premissa e a proteção dos dados contra o acessos indevidos

UNI METRO CAMP wyden

Confidencialidade



UNI METRO CAMP wyden

Confidencialidade

- Vazamento de informações
  - Senhas, mensagens, arquivos
- Para evitar que o intruso entenda o conteúdo das mensagens, é necessário cifrar os dados

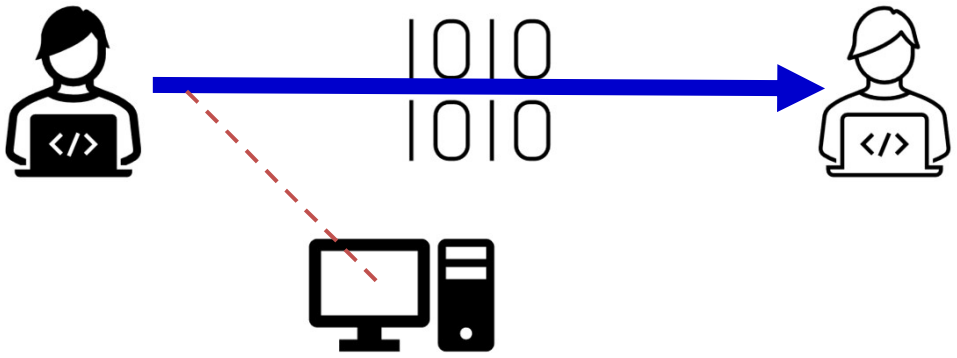
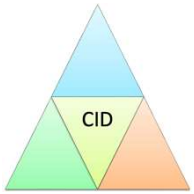


Imagem: autor

UNI METRO CAMP wyden

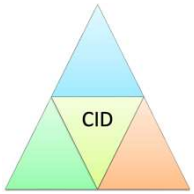
Confidencialidade



- Adotar medidas de controle de acesso

Imagem: autor

Integridade

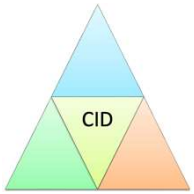


Garantir que os dados não sejam alterados de forma não autorizada

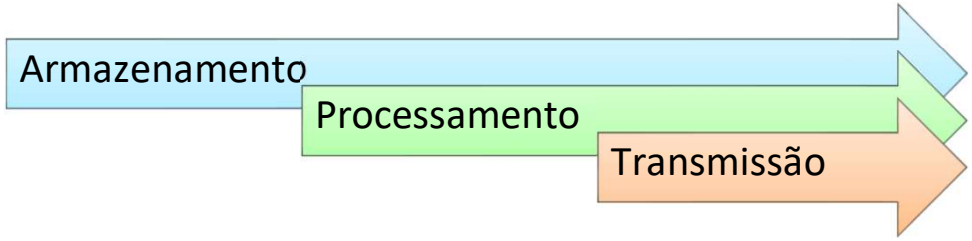
Envolve proteger os dados contra modificações acidentais ou intencionais

Imagem: autor

Integridade



Durante o processo

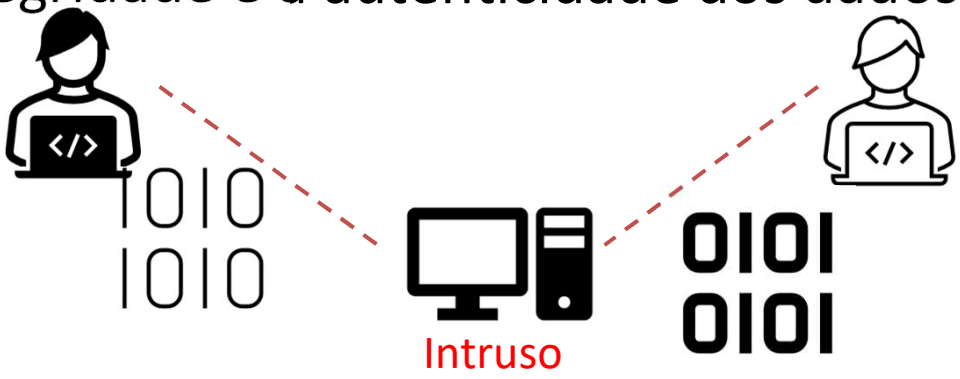


Confiança e consistência dos dados

Imagem: autor

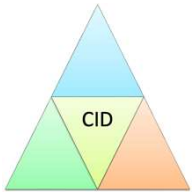
Integridade

- Informações Corrompidas/falsas
  - Alterar destino de um pagamento bancário, arquivos alterados
- Evitar ataques, é a busca para garantir a integridade e a autenticidade dos dados

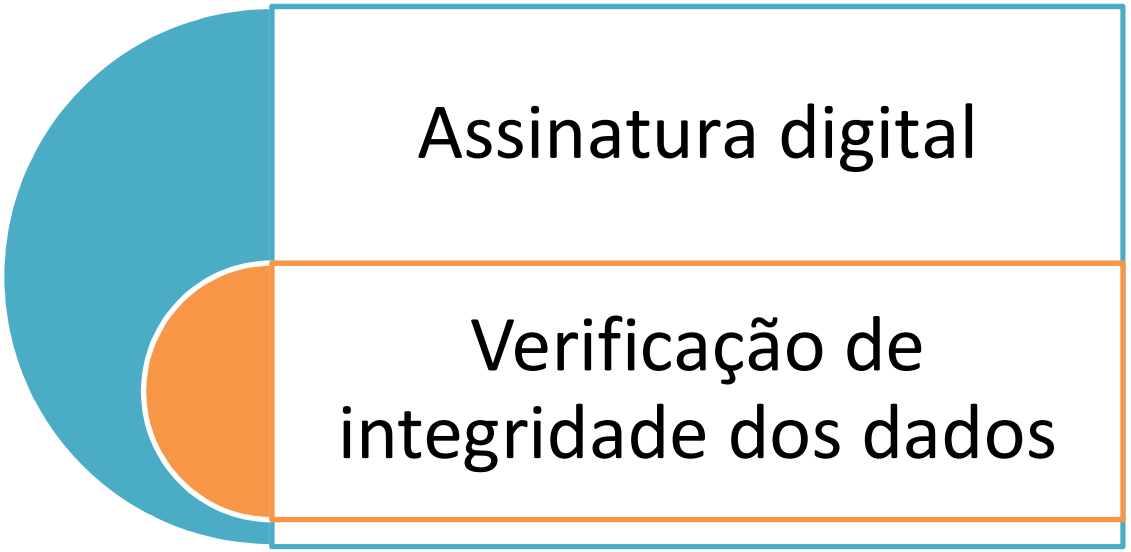


UNI METRO CAMP wyden

Integridade

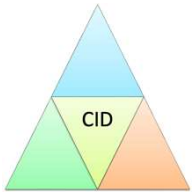


- Adotar técnicas para assegurar que a informação não tenha sido adulterada



UNI METRO CAMP wyden

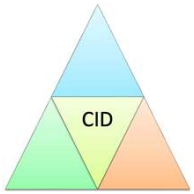
Disponibilidade



Manter os dados disponíveis para serem utilizados quando necessário, com o desempenho adequado

UNI METRO CAMP wyden

Disponibilidade

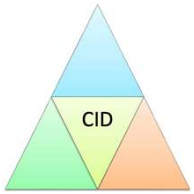


Garantia de que as informações estejam disponíveis para os usuários autorizados quando necessário

Implementação de medidas para evitar interrupções ou indisponibilidade prolongada de sistemas e serviços

UNI METRO CAMP wyden

Disponibilidade



- Adotar ações para mitigar ataques que possam afetar a disponibilidade dos recursos

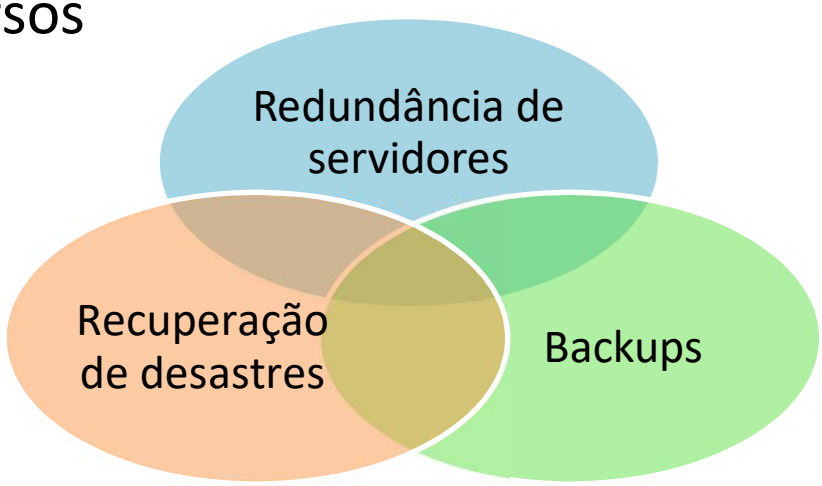
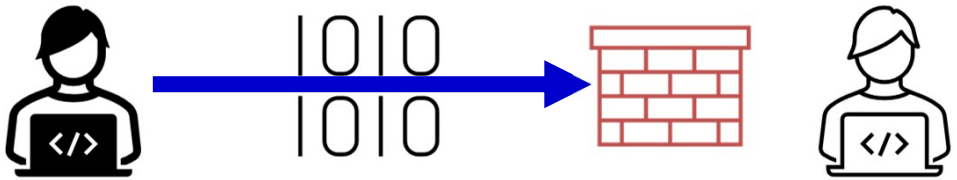


Imagem: autor

UNI METRO CAMP wyden

Disponibilidade

- Dados nunca chegam ao destino
  - Site fora do ar, arquivos apagados e/ou corrompidos, falhas na rede
- É necessária a segurança física dos recursos de processamento e de comunicação de dados



UNI METRO CAMP wyden

Situação Problema

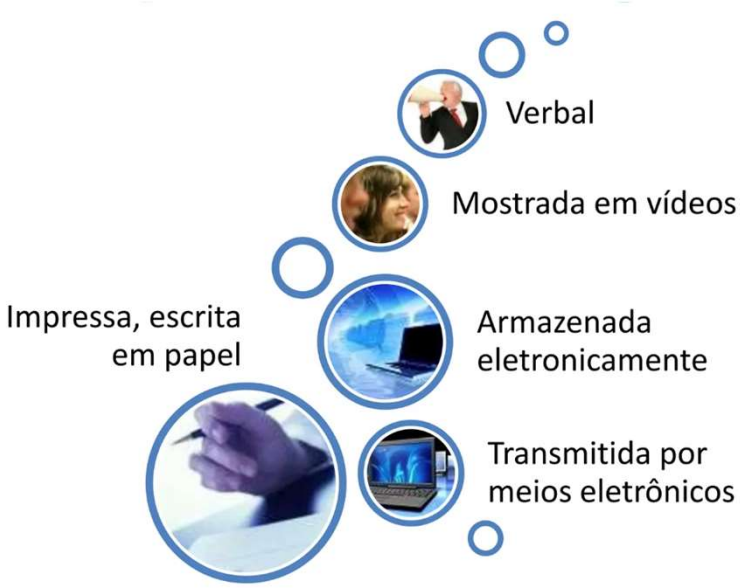
- Todas as falhas de segurança da informação estão dentro do escopo de confidencialidade, integridade e disponibilidade?

Sim, todos as falhas estão relacionadas com Segurança da Informação

Imagem: autor desconhecido

Natureza Multiforme da Informação

- Devem ser protegidas



UNI METRO CAMP wyden

Ativo da Informação
Algo que atribui valor

UNI METRO CAMP wyden

Onde encontro Informação

UNI METRO CAMP wyden

Dimensões de Risco

- O Cubo de McCumber e as Três Dimensões do Risco

As informações estão em diversos locais e a segurança depende de múltiplos fatores

Imagem: https://www.ibm.com/downloads/cas/O0WM1WMQ

UNI METRO CAMP wyden

ISO/IEC 27002:2022
- Controles

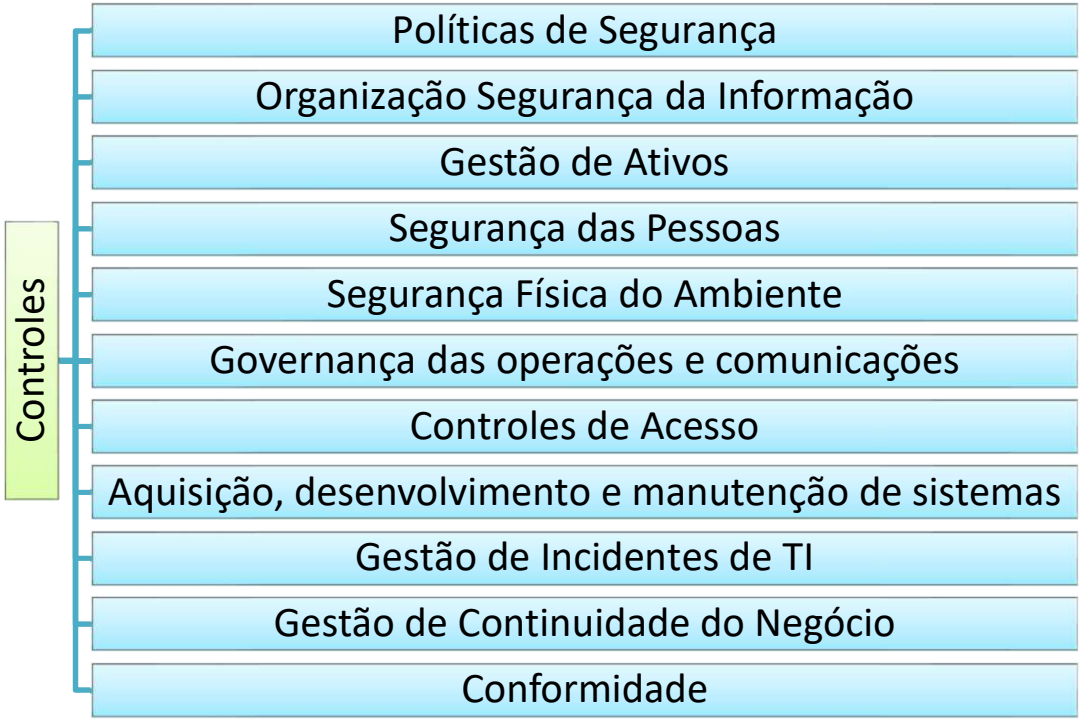
A informação é um ativo muito valioso para uma organização

A informação pode ser impressa, escrita em papel, armazenada em via eletrônica, ou até mesmo conversada

A informação deve ser protegida adequadamente

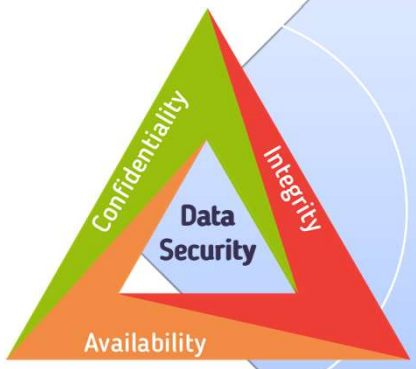
UNI METRO CAMP wyden

ISO/IEC 27002:2022 - Controles



UNI METRO CAMP wyden

Roteiro Baseado na ISO/IEC 27002:2022



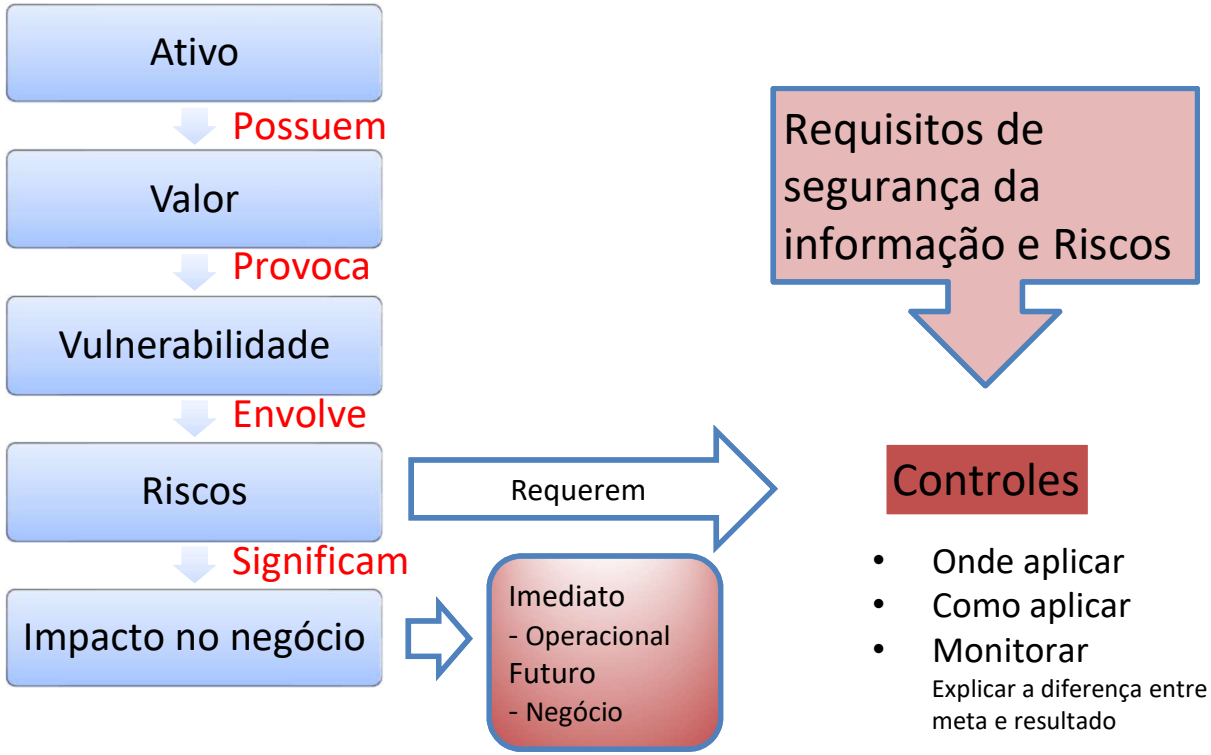
Classificação CID

- Nomear e identificar a informação a ser classificada
- Identificar os controles associados a informação
- Identificar os proprietários e responsáveis pela informação
- Criar um critério que atendam a necessidade da organização
- Aplicar a classificação da informação
- Formalizar a classificação adotada na organização

Ver Questionário de apoio para classificação

UNI METRO CAMP wyden

ISO 27002- Controles



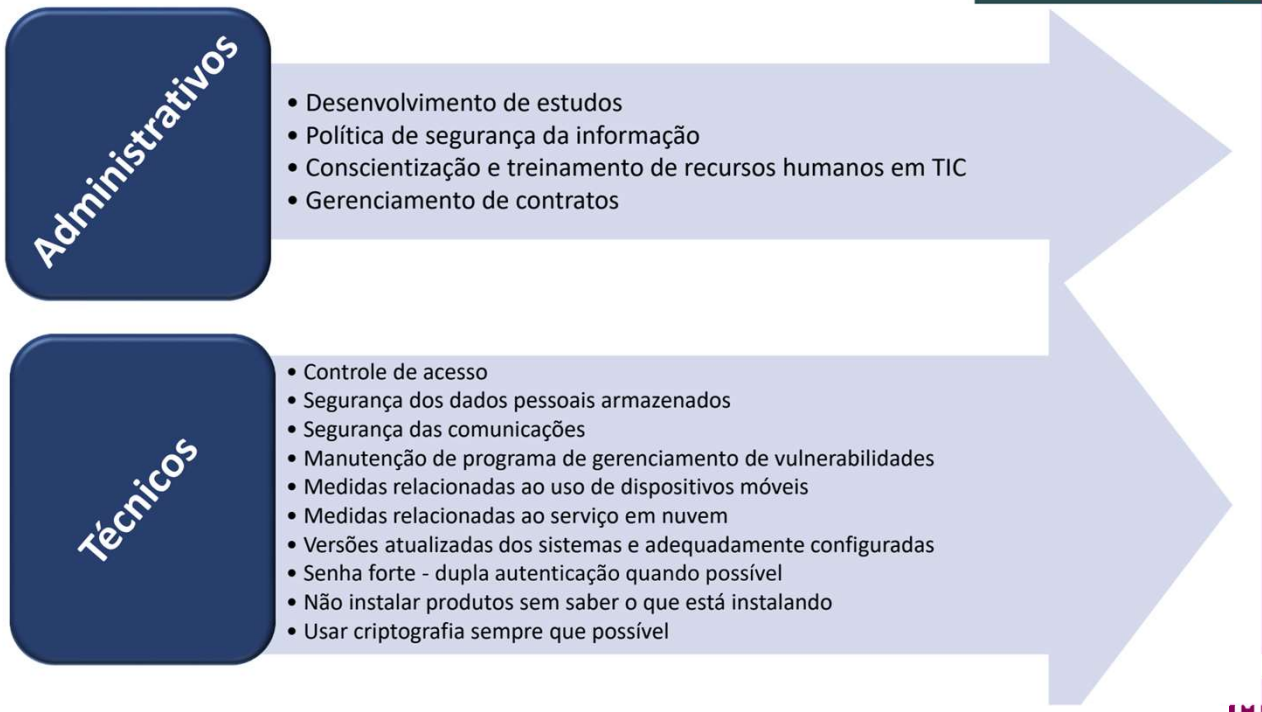
UNI METRO CAMP wyden

Ativos de Informação - ISO-27002

- Proprietário
- Localização
- Formato
- Classificação
  - Secreto
  - Confidencial
  - Público
- CID

Categoria (Natureza)/Tipo do Ativo	Ativos de Informação
Informação	Banco de dados e arquivos magnéticos
	Documentação de sistemas e manual do usuário
	Material de treinamento
	Procedimetnos operacionais de recuperação
	Planos de continuidade
Documentos em papel	Contratos
	Documentação da empresa
	Relatórios confidenciais
Software	Aplicativos
	Sistemas operacionais
	Ferramentas de desenvolvimento
	Utilitários do sistema
Físico	Servidores, desktops e notebooks
	Impressoras e copiadoras
	Equipamentos de comunicação (fax, roteadores)
	Mídias magnéticas
	Gerador, no-break e ar-condicionado
	Móveis, prédios e salas
Pessoa	Empregados, estagiários, terceiros e fornecedores
Serviço ou atividade	Computação (aplicação de patches, backup)
	Comunicação (ligação telefônicas, videoconferências)
	Utilitários gerais
Intangiveis	imagem da empresa
	Reputação
	Credibilidade
	Vantagem estratégica

Tipos de Controles



ISO/IEC 27002:2022 - Controles

- Rotulagem das Informações
  - Controle: Um conjunto adequado de procedimentos para rotulagem das informações deve ser desenvolvido e implementado, de acordo com o esquema de classificação das informações adotado pela organização.
  - Propósito: Facilitar as comunicações a respeito da classificação das informações e automação do suporte de processamento e gerenciamento das informações.
- Transferência das Informações
  - Controle: Regras, procedimentos e acordos de transferência das informações devem ocorrer em todos os tipos de instalações de transferência na organização, entre ela e partes interessadas.
  - Propósito: Manter a segurança das informações transferidas na organização e em qualquer parte interessada externa.
- Controle de Acesso
  - Controle: Regras para o controle físico e lógico de acesso às informações e outros ativos associados devem ser estabelecidos e implementados, conforme os requisitos de negócio e Segurança da Informação.
  - Propósito: Garantir acesso autorizado e prever acesso não autorizado às informações e aos outros ativos associados.

ISO/IEC 27002:2022 - Controles

- Gerenciamento de Identidade
  - Controle: O ciclo de vida completo das identidades deve ser gerenciado.
  - Propósito: Permitir a única identificação de indivíduos e sistemas no acesso a informações da organização e outros ativos associados, bem como habilitar a definição adequada de direitos de acesso.
- Informações de Autenticação
  - Controle: Alocação das informações de autenticação deve admitir controle por um processo de gerenciamento, incluindo aconselhamento aos colaboradores a respeito do manuseio adequado de informações de autenticação.
  - Propósito: Garantir adequada autenticação na entidade e prevenir falhas no processo.
- Direitos de Acesso
  - Controle: Direitos de acesso a informações e outros ativos associados devem ser provisionados, revisados, modificados e removidos, de acordo com políticas de tópicos específicos da organização e regras para controle de acesso.
  - Propósito: Garantir que o acesso a informações e outros ativos associados estejam definidos e autorizados de acordo com os requisitos de negócio.

Questionamento de Apoio ao Roteiro

Quanto ao Valor da informação

- Qual é o grau de exclusividade?
- Qual é o nível de confiabilidade da fonte?
- Qual é a quantidade de informações acessórias que a acompanham?
- Qual é o grau de interesse de terceiros?
- Qual é a quantidade de terceiros interessados?
- Qual é a importância da informação para a organização?

Questionamento de Apoio ao Roteiro

Quanto a Confidencialidade da informação

- A informação é pública?
- Sua divulgação causa algum dano ou prejuízo?
- A divulgação causa constrangimento ou inconveniência operacional?
- Sua divulgação tem impacto significativo nas operações ou objetivos táticos?
- Sua divulgação causa alguma sansão ou punição?
- Qual é a validade?

Questionamento de Apoio ao Roteiro

Quanto a Integridade da informação

- Quais são os dados que compõem a informação?
- A fonte da informação é identificada e confirmada?
- Em que mídia é disponibilizada a informação?
- Em que mídia é armazenada a informação?
- Como é feito o transporte?
- Como são identificados os emissores e receptores?
- Como é verificado se o destinatário recebeu?
- Como é verificado se a informação entregue foi exatamente a mesma emitida?
- Como é realizado o descarte?
- O é verificado que o descarte foi realizado conforme determinado?

Questionamento de Apoio ao Roteiro

Quanto a Disponibilidade da informação

- Quem ou a que processo pode ter acesso?
- Qual é o prazo máximo para a entrega?
- Qual é o meio para solicitar?
- Qual é o meio para entrega?
- O prazo de disponibilidade está sujeito a regulamentação externa?
- Quais são os riscos de físicos de vazamento?
- Quais são os riscos lógicos de vazamento?
- Quais são os riscos humanos de vazamento?

Exemplos

Vazamento de dados

- As informações confidenciais são expostas sem autorização, resultando em perda de confidencialidade

Ataque de ransomware

- Malware que criptografa os dados e exige um resgate para recuperá-los, afetando tanto a integridade quanto a disponibilidade dos dados

Ataque de engenharia social

- Agente mal-intencionado manipula os usuários para obter informações confidenciais, comprometendo a confidencialidade

Ataque de negação de serviço distribuído (DDoS)

- Inundação massiva de tráfego em um serviço ou sistema para sobrecarregá-lo e torná-lo inacessível, impactando a disponibilidade

Duvidas, considerações ...

Imagem Ícones MS-Power Point

UNI METRO CAMP wyden

Referências

- BAARS, Hans. Fundamentos de **Segurança da Informação: com base na ISO 27001 e na ISO 27002.** Rio de Janeiro ? RJ ? Editora Brasport, 2018. Capitulo 3. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044
- GALVÃO, Michele da Costa, Agnaldo Aragon. **Fundamentos em Segurança da Informação.** Rio de Janeiro ? RJ: Editora Pearson, 2015. Capitulo 3. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525>

UNI METRO CAMP wyden

Referências

- SCHNEIDER, Carlos Alberto. **Governança da Segurança da Informação**. Brasília, 2015, Capítulo 4 – Classificação dos Ativos da Informação, do Livro: p. 37-45.

UNI METRO CAMP wyden

Referências

- **Confidencialidade Integridade e Disponibilidade (CID).** Disponível em: <https://www.certifiquei.com.br/confidencialidade-integridade-disponibilidade/>. Acesso em 19/05/2024
- **Soluções de segurança e proteção de dados.** Disponível em: <https://www.ibm.com/br-pt/data-security?>. Acesso em 19/05/2024

UNI METRO CAMP wyden

Atividade aula 11

- Quais são os principais desafios enfrentados na preservação da CID de informações em um ambiente cada vez mais conectado e digitalizado?
- Qual o principal ponto abordado na aula sobre CID e ISO 27002
- Cite um exemplo de controle para gestão adequada de CID
- Com base na resposta anterior, defina um indicador
- Explique como o indicador pode ser coletado
- Elabore uma formula para cálculo do indicador

- Mínimo de 3 e máximo de 6 integrantes
- Responder no Forms: https://forms.office.com/r/04nALQV8iv

UNI METRO CAMP wyden

Para Próxima Aula
Assista aos vídeos

- Segurança da Informação Confidencialidade, Integridade e Disponibilidade: https://www.youtube.com/watch?v=3vhz3IFjl7M
- INFORMÁTICA Princípios da SEGURANÇA DA INFORMAÇÃO | REVISÃO rápida com Mapa Mental Explicado: https://www.youtube.com/watch?v=T3CkJMZCrL8
- Não repúdio Segurança da Informação Dicionário de Informática: https://www.youtube.com/watch?v=Nzb_qGPj


UNI
METRO
CAMP
wyden