CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA EDUCAÇÃO

Centro Administrativo Governador Virgilio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

LUIZ GONZAGA FONSECA MOTA
ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL

# Segurança em RDC

Prof. Luis Felipe Oliveira

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25


# Aula 02 - Introdução a Segurança: confidencialidade, integridade, disponibilidade e não repúdio

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25



# O que veremos hoje ???

Introdução

Confidencialidade

Integridade

Disponibilidade

Autenticidade

Não-repúdio

Controle de acesso

Gerenciamento de risco

# O que veremos hoje ???

Introdução

Confidencialidade

Integridade

Disponibilidade

Autenticidade

Não-repúdio

Controle de acesso

Gerenciamento de risco

# Introdução

Hoje, vamos abordar um tema que é fundamental tanto para as organizações quanto para os indivíduos: a proteção de informações sensíveis contra ameaças internas e externas.

É importante entender os conceitos básicos e as melhores práticas para garantir a confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio das informações.

# Confidencialidade

É a garantia de que as informações serão acessadas apenas por pessoas autorizadas. É um dos pilares da segurança da informação e sua importância não pode ser subestimada.

A confidencialidade pode ser alcançada através do uso de criptografia, controle de acesso e políticas de segurança bem definidas.

**Ex.: o acesso a dados médicos de um paciente, que deve ser restrito apenas aos profissionais de saúde envolvidos em seu tratamento.**

# Integridade

É a garantia de que a informação não foi alterada ou corrompida de forma intencional ou acidental. Garante que a informação seja confiável e precisa.

Quando a integridade é comprometida, as informações podem se tornar imprecisas, incompletas ou até mesmo falsas, o que pode levar a decisões erradas e consequências graves.

**Ex.: um ataque de malware pode corromper arquivos importantes, um hacker pode alterar dados em um banco de dados ou um funcionário desonesto pode modificar informações sensíveis.**

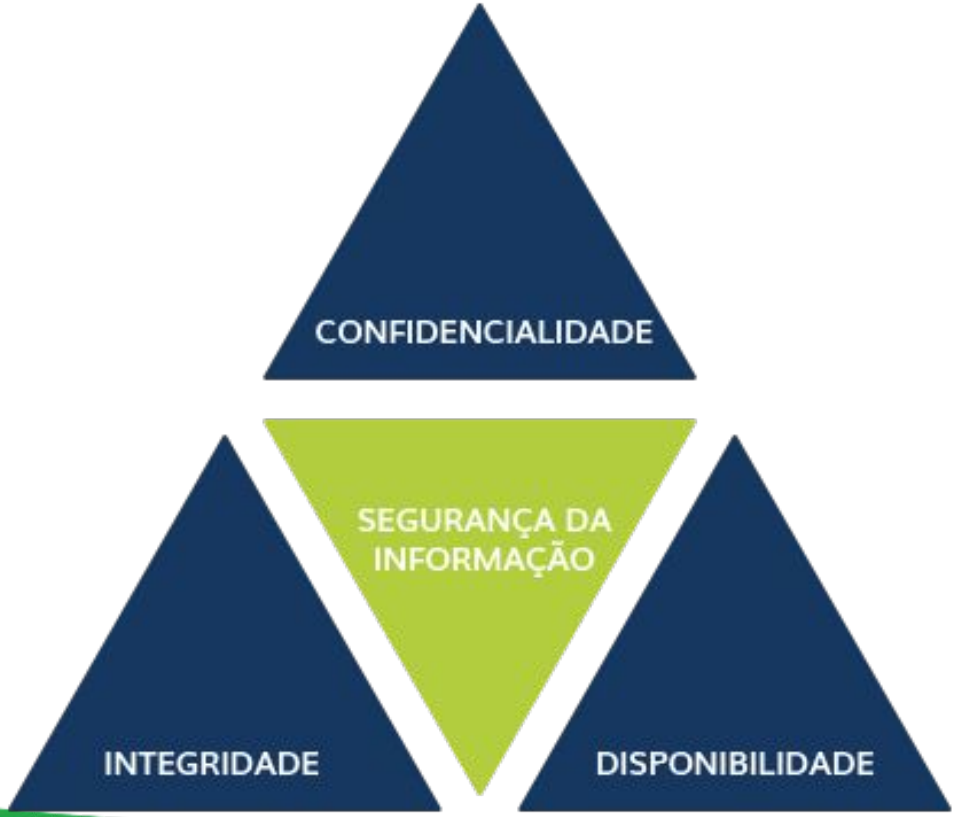
# Disponibilidade

É a capacidade de acessar a informação quando necessário. A disponibilidade é tão importante quanto a confidencialidade e a integridade. Uma organização que não consegue manter sua informação disponível pode perder clientes e até mesmo ir à falência.

**Ex.: um hospital que não consegue acessar os registros médicos dos pacientes. Isso pode levar a erros médicos graves e colocar em risco a vida dos pacientes.**

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25





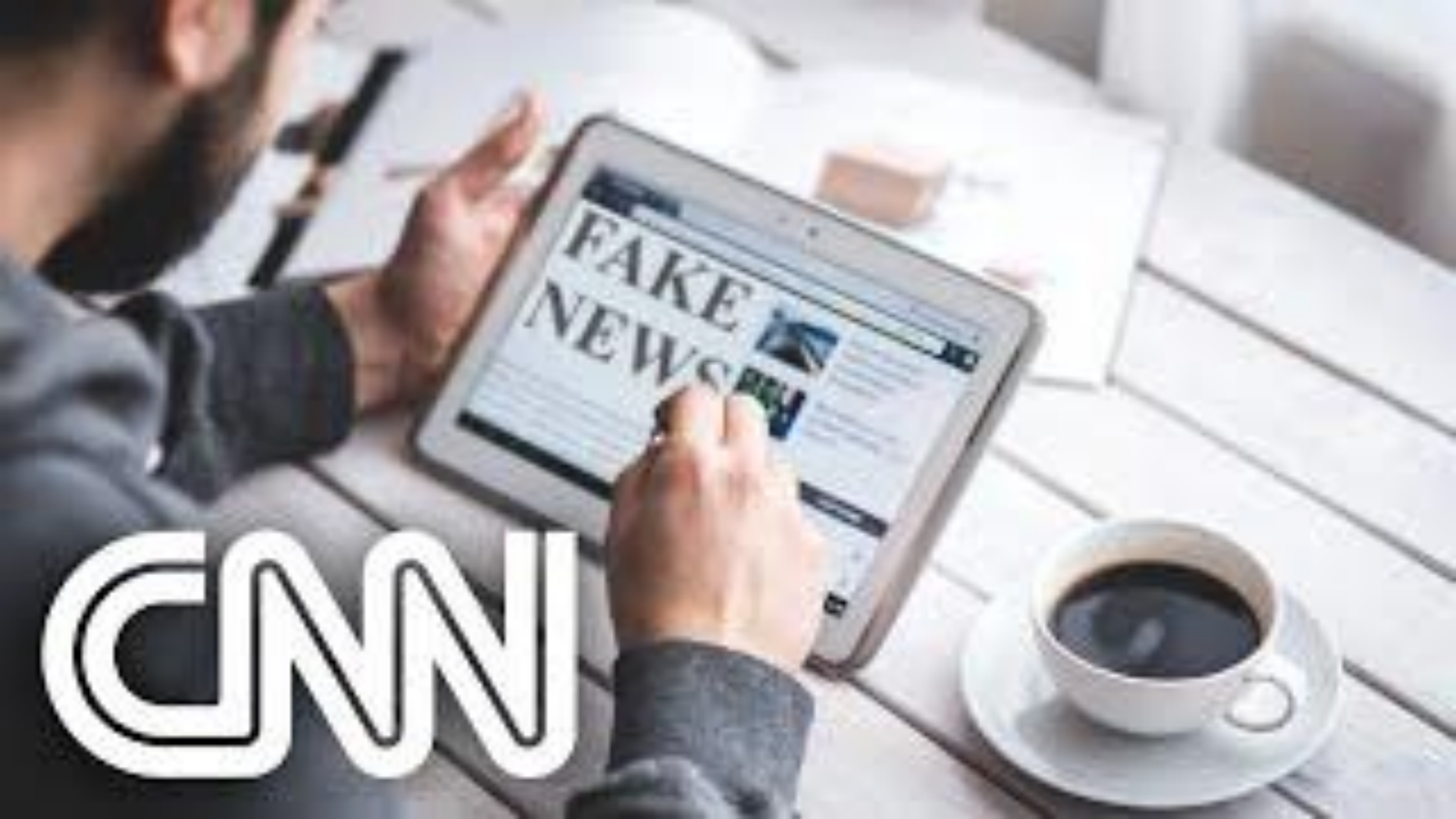
# Autenticidade

É a característica da informação que garante que ela é genuína e originada por uma fonte confiável. A autenticidade é fundamental para a segurança da informação, pois sem ela, não podemos confiar nos dados que recebemos e tomamos decisões com base neles.

**Ex.: um ambiente empresarial, um e-mail falso pode levar a uma transferência de dinheiro para uma conta fraudulenta. Em um contexto mais amplo, informações falsas podem levar a decisões erradas em nível político e social, causando danos irreparáveis.**

# 4 em cada 10 brasileiros afirmam receber fake news diariamente

https://www.youtube.com/watch?v=F5wqxZSLNok&t=2s


FAKE
NEWS
CNN

# Não-repúdio

É a capacidade de uma pessoa ou organização negar a autoria de uma ação realizada por ela. É a garantia de que uma mensagem ou transação foi realmente enviada ou realizada pela pessoa ou organização que afirma tê-la enviado ou realizado, e que essa pessoa ou organização não pode negar posteriormente a sua autoria.

**Ex.: em um contrato eletrônico assinado digitalmente, o não-repúdio garante que as partes envolvidas não possam negar posteriormente a autoria da assinatura, o que confere maior segurança jurídica ao documento.**

# Controle de acesso

É uma medida de segurança importante para garantir que apenas pessoas autorizadas tenham acesso a informações sensíveis. Envolve a criação de políticas e procedimentos para gerenciar o acesso a sistemas, aplicativos e dados. O objetivo é proteger informações confidenciais contra roubo, perda ou alteração não autorizada.

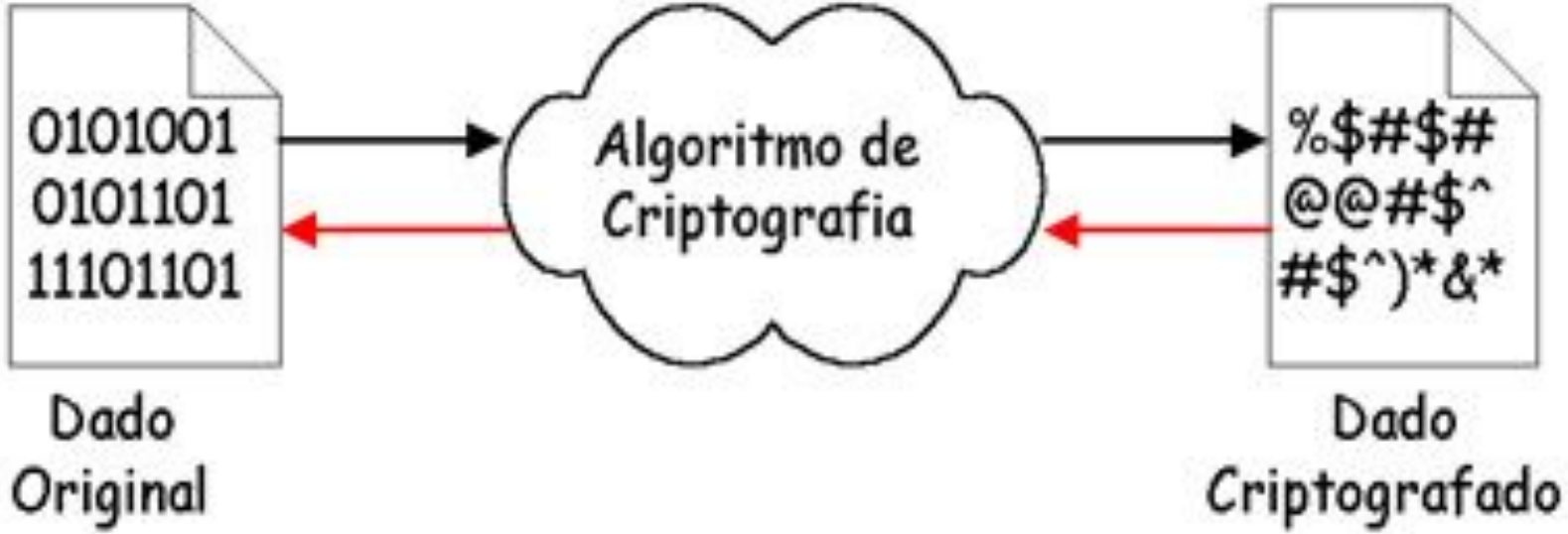
Existem várias técnicas que podem ser usadas para implementar o controle de acesso em uma organização, as mais comuns são **autenticação** e **autorização**

# Criptografia

É uma técnica utilizada para codificar informações de forma que apenas o destinatário correto possa decodificá-las. Isso é feito através do uso de um algoritmo de criptografia, que transforma a mensagem original em um formato ilegível para qualquer pessoa que não tenha a chave correta para decodificá-la.

Alguns dos mais conhecidos são o AES, RSA e DES

# Criptografia



# Gerenciamento de Riscos

É um processo fundamental para garantir a segurança da informação em uma organização. Ele envolve identificar, avaliar e tratar os riscos que podem afetar a confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio dos dados.

A primeira etapa é identificar os ativos que precisam ser protegidos, como sistemas, dados e informações sensíveis. Em seguida, é preciso avaliar os riscos associados a esses ativos, levando em conta a probabilidade de ocorrência e o impacto caso ocorram. Por fim, é necessário tratar os riscos identificados, com medidas de segurança adequadas para mitigá-los ou eliminá-los.

# GESTÃO DE RISCOS:
# O QUE É E PARA QUE SERVE?

# Gerenciamento de Risco

Exemplos de potenciais riscos para segurança da informação para empresas

**Roubo de dados**

**Espionagem industrial**

**Hackers de senhas**

**Funcionários não especializados / erros humanos**

**Softwares vulneráveis**

**Ataques de ransomware**

**Phishing**

**Ataques direcionado**

**Adware**

**DDoS**

# Conclusão

A segurança da informação é um tema fundamental para qualquer organização ou indivíduo que lida com dados sensíveis.

É necessário estar sempre atualizado e preparado para lidar com essas ameaças.

É imprescindível que todos os colaboradores de uma organização estejam conscientes da importância da segurança da informação e sejam treinados para agir de forma segura no ambiente digital