# SEGURANÇA DIGITAL

## CERTIFICADO DIGITAL

É um documento eletrônico que associa uma chave pública a uma identidade (pessoa física, empresa ou sistema)
Onde, mostra se a autenticação da assinatura esta correta, se o tal realmente assinou.

## SEGURANÇA DIGITAL

conjunto de práticas, tecnologias e medidas adotadas para proteger sistemas, redes, dados e usuários contra acessos não autorizados, ataques cibernéticos, vazamentos e fraudes.

## 🔐 CRIPTOGRAFIA

A criptografia é a técnica de codificar informações para garantir sua confidencialidade, integridade e autenticidade durante o armazenamento ou a transmissão.

## 📜 LGPD (LEI GERAL DE PROTEÇÃO DE DADOS) – BRASIL

Objetivo:
Proteger os dados pessoais dos indivíduos e garantir o uso de modo seguro.

Princípios:
Finalidade: uso claro e específico dos dados.
Necessidade: coleta mínima e essencial.
Transparência: o titular deve saber como seus dados são usados.
Segurança: medidas para evitar vazamento ou perda.
Responsabilização: as empresas devem responder por falhas.
Direitos dos titulares:
Acesso aos dados
Correção de dados incompletos ou errados
Exclusão dos dados

## CRIPTOGRAFIA ASSIMÉTRICA

Utiliza um par de chaves:
Chave pública: pode ser compartilhada com todos.
Chave privada: deve ser mantida em segredo.
A chave pública criptografa os dados, e apenas a chave privada pode descriptografar (e vice-versa).
exemplo: use a chave de um amigo para criptografar pois somente ele poderá utilizar e ver o que foi criptografado.

## EXEMPLOS DE ALGORITMOS:

- RSA
- ECC (Criptografia com Curvas Elípticas)
- ElGamal
- DSA (Digital Signature Algorithm)

## CRIPTOGRAFIA SIMÉTRICA

Utiliza uma única chave para criptografar e descriptografar a informação.
Mais rápida que a criptografia assimétrica.
um embraralhamento de caracteres, por exemplo l30n4rd0 = Leonardo.