**SO**

**AULA 2 - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

**Norma ISO**

**Definição**

Conjunto de padrões técnicos e diretrizes desenvolvidos pela Organização Internacional de Normalização (ISO) para promover a qualidade, segurança e eficiência em diversos setores industriais e comerciais.

Setores que atende:

* Indústria: ISO 9001
* Tecnologia da informação: ISO/EC 27001
* Saúde: ISO 13485
* Construção civil: ISO 45001
* Alimentício: ISO 22000

**ISOs relacionadas à PSI**  
ISSO 27001:

* Norma principal para gestão da segurança da informação:
* Define requisitos para implementar um SGSI (Sistema de Gestão da Segurança da Informação)

ISSO 27002:

* Complementa a 27001;
* É um guia paque fornece distrizes práticas de controle a serem seguidas como:
  + Controle de acesso;
  + Uso aceitável de recursos;
  + Classificação da informação.
* A 27002 nos mostra como implementar as medidas.

**Política Nacional de Segurança**

Aprovada em 26 de dezembro de 2018 pelo decreto nº9.637/2018

É um documento que define os princípios...

**Setor Privado**

Empresas privadas não precisam seguir normas ISO/EC. Mas seu uso é recomendado por segurança.

**Setor Público**

Empresas públicas devem adotar medidas baseadas nas normas **ABNT NBR ISO/IEC 27001 e 27002** – seguindo a PNSI.

**LEGISLAÇÃO**

**Marco Civil da Internet**

**Definição**

O Marco Civil da Internet ou Lei nº 12.965/2014 é uma lei brasileira que estabelece direitos e deveres para o uso da internet no Brasil.

Ela foi sancionada em 23 de abril de 2014 como uma resposta à ausência de uma legislação específica sobre o uso da internet no Brasil.

Ela garante direitos fundamentais na internet. como liberdade de expressão, privacidade, proteção de dados pessoais e neutralidade da rede.

**Princípios Fundamentais (Art.3º)**

* Garantia da liberdade de expressão, comunicação e manifestação de pensamento;
* Proteção da privacidade e dos dados pessoais;
* Neutralidade da rede – tratamento isonômico (igualdade) de dados, sem discriminação por conteúdo ou serviço;
* Preservação da estabilidade, segurança e funcionalidade da rede;
* Responsabilidade dos agentes conforme sua atividade;
* Abertura e colaboração para o desenvolvimento da internet.

**Direito dos Usuários (Art.7º)**

Estabelece direitos básicos do cidadão na internet.

* Privacidade e sigilo das comunicações;
* Proteção dos dados pessoais;
* Informação clara sobre coleta e uso de dados;
* Conexão estável e sem discriminação
* Consentimento para uso de dados.

**Neutralidade da Rede (Art.9º)**

Obriga os provedores a tratar todo o tráfego de forma isonômica (igual).

Não pode haver:

* Prioridade para certos sites/apps (ex: Netflix mais rápido que Youtube);
* Bloqueio ou lentidão de serviços concorrentes.

**Guarda e fornecimento de dados (Art.10º)**

Determina regras sobre o armazenamento e fornecimento de registros (logs) e dados pessoais.

* Dados pessoais só podem ser acessados com autorização judicial;
* Empresas devem garantir sigilo e segurança das informações.

**Penalidades (Art.12º)**

Define sanções para quem violar as regras do Marco Civil.

Sanções incluem:

* Advertência;
* Multa;
* Suspensão temporária das atividades;
* Proibição de atuar.

**Guarda de Registros (Art. 13º e 15º)**

Estabelece que:

* Provedores de conexão devem guardar logs de conexão por 1 ano;
* Provedores de aplicações devem guardar logs por 6 meses.

**Aplicação**

* Aplicável a qualquer operação de internet realizada no território nacional independentemente da sede da empresa;
* Envolve usuários, provedores de conexão, provedores de aplicações (apps, redes sociais), e o Estado

**Conclusão**

Com isso concluímos que o Marco Civil da Internet é uma base legal que protege o cidadão brasileiro, servindo como uma ferramenta de defesa de liberdade e segurança.

**Lei Geral da Proteção de Dados**

**Definição**

A LGPD (Lei nº 13.709/2018) é a legislação brasileira que regula a coleta, armazenamento, uso e compartilhamento de dados pessoais. Inspirada no GDPR europeu.

Foi sancionada em 14 de agosto de 2018 e entrou em vigor no dia 18 de setembro de 2020.

**Contexto de Criação**

* Inspirado e baseado no Regulamento Geral de Proteção de Dados europeu (GDPR);
* Com a grande evolução da digitalização, surgiu a necessidade de regulamentar o tratamento dos dados que navegam pela internet;

**ANPD**

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável por fiscalizar, regulamentar e orientar a aplicação da Lei Geral de Proteção de Dados (LGPD) no Brasil.

Tem como objetivo:

* Regulamentar a LGPD – Criar normas complementares para facilitar a aplicação da lei
* Fiscalizar e aplicar sanções – Investigar incidentes de dados e aplicar advertências, multas e outras penalidades.
* Orientar empresas, órgãos públicos e sociedade;

**Marco Civil x LGPD**

As duas leis estão no mesmo ambiente digital, porém tem suas diferenças:

* O Marco Civil da Internet engloba a internet em geral, garantido a liberdade, neutralidade, privacidade e segurança no uso.;
* Já a LGPD tem o objetivo de proteger a privacidade e os dados pessoais dos cidadãos em qualquer ambiente (digital ou físico).

Então entendemos que a LGPD está mais voltada aos dados pessoais, seja online ou offline, e o Marco Civil da Internet aplica-se a todos usuários, provedores, empresas que atuam no **ambiente da internet**.

**O que são dados pessoais?**

São informações que identificam ou tornam alguém identificável, como:

* Nome, CPF, RG, e-mail;
* IP, localização, hábitos de consumo;
* Dados sensíveis: religião, saúde.

**Fundamentos da Lei(Art.2º)**

A disciplina da proteção de dados pessoais tem como fundamentos:

* O respeito a privacidade – os dados pessoais é parte da vida privada do indivíduo;
* Autodeterminação informativa – A pessoa tem o direito de controlar seus próprios dados;
* A liberdade de expressão, de informação, de comunicação e de opinião
* A inviolabilidade da intimidade, da honra e da imagem – proteger a dignidade da pessoa no ambiente virtual;
* Desenvolvimento tecnológico – a lei não é contra tecnologia, mas quer garantir uso ético;

**Princípios do Tratamento de Dados (Art.6º)**

Define os 10 princípios fundamentais que devem ser seguidos ao tratar dados.

* Finalidade – uso claro e legítimo dos dados;
* Necessidade – uso mínimo necessário;
* Transparência – o titular deve ser informado;
* Segurança – proteção contra vazamento ou acessos indevidos;
* Prestação de contas – a empresa deve provar que está cumprindo a lei.

**Conceitos e Definições (Art.5º)**

Traz definições chave que norteiam toda a LGPD.

* Dado pessoal – qualquer informação relacionada a pessoa natural identificada ou identificável;
* Dado sensível – dados sobre origem racial, religião, política, saúde, orientação sexual etc;
* Titular: pessoa a quem os dados pertencem;
* Controlador: quem decide como e por que os dados são tratados;
* Operador: quem executa o tratamento de dados em nome do controlador.