Grupo: Leonardo May, Luiz Felipe e Tiago Boeing

Proposta:
Grupo 6: Organização da Segurança da Informação (Normas ISO 27000). Lei de Proteção de Dados

O intuito principal deste artigo é de realizar um estudo e análise da LGPD - Lei Geral de Proteção de Dados. A mesma trata diretamente de questões de confidencialidade e segurança as informações relacionadas aos recursos de TI, como armazenamento dos dados, tratando especificamente dos dados que permitem a identificação individual, como dados de nome, CPF, e-mail ou número de telefone.

Os principais pontos da lei são a qualificação de como os dados são utilizados e armazenados.
A lei se qualifica em três principais tipos de dados:

Dados pessoais: aqueles que de alguma forma permitem identificar o indivíduo, como RG, número de telefone, e-mail, CPF e outros.

Dados sensíveis: são informações que podem levar a discriminação da pessoa por escolhas pessoais como orientação ou preferências sexuais, orietanção politica, entre outros.

Dados anonimizados ou pseudo anônimos: O primeiro trata de dados que não possam ser rastreados ou que com eles não consiga chegar a uma pessoa natural. Portanto, a lei não se aplica a esses dados. Em contrapartida dados pseudo anônimos são dados que de alguma forma dificulta o rastreamento, porém não há uma garantia de 100% que não possa chegar a um indivíduo

Termos que compõem o LGPD:
- Dados pessoais;
- Dados sensíveis;
- Tratamento de dados;
- Titular dos dados;
- Consentimento aos dados;
- Anonimização e pseudo anônimos;
- Controlador e processador.

Portanto, a lei tem o intuito de garantir que as pessoas tenham controle de como seus dados são usados, bem como proteger os cidadãos do uso indevido deles e responsabilizados quem armazena e faz uso desses dados.

Iso 27000
- **ISO/IEC 27000** – Princípios e Vocabulário, define a nomenclatura utilizada nas normas seguintes da família 27000.
- **ISO/IEC 27001** – Tecnologia da Informação. Técnicas de segurança. Sistemas de Gestão de Segurança da Informação – Requisitos. Única norma da família 27000

que é passível de certificação acreditada - todas as seguintes são apenas guias de boas práticas.

- **ISO/IEC 27002** – Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação - não dispõe de esquema de certificação acreditada
- **ISO/IEC 27003** – Tecnologia da informação - Técnicas de Segurança - Sistemas de gestão de segurança da informação - Guia de Boas Práticas - - não dispõe de esquema de certificação acreditada
- **ISO/IEC 27004** – Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Monitorização, medição, análise e avaliação - não dispõe de esquema de certificação acreditada
- **ISO/IEC 27005** – Tecnologia da informação - Técnicas de segurança - Gestão de risco da segurança da informação - não dispõe de esquema de certificação acreditada

Estudo de caso:

Em setembro de 2018, uma falha de segurança no site da British Airways resultou no vazamento de dados pessoais e financeiros de 500 mil clientes. Sendo a companhia aérea multada em 183,39 milhões de libras esterlinas, ou aproximadamente R$ 897 milhões, pelo Information Commissioner's Office (ICO), órgão do Reino Unido que trata da privacidade dos usuários.
https://tecnoblog.net/297840/british-airways-multa-recorde-vazamento-dados/