LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SEGURANÇA DA INFORMAÇÃO: CONEXÃO OU CONFUSÃO?

Profa. Dra. Cinthia Obladen de Almendra Freitas

PUCPR
GRUPO MARISTA

Agenda

- Introdução
- Aspectos Tecnológicos da Proteção de Dados Pessoais e da Segurança da Informação
- Normas ISO como Ferramental de Planejamento Tecnológico voltado à Implantação da LGPD
- Modelos de Boas Práticas: ITIL e COBIT
- Considerações Finais
- Referências

PUCPR
GRUPO MARISTA

Introdução

- LGPD afeta todos os setores que utilizam dados pessoais e informação para o exercício de suas atividades.

- O foco recai sobre os aspectos jurídicos da LGPD, mas o que muitos esquecem ou ainda não perceberam é que **a LGPD é uma lei de implementação tecnológica**.

- LGPD carrega um arsenal de termos técnicos da área de **SI** associados aos termos básicos da área de **CC**.

PUCPR
GRUPO MARISTA

Introdução

- Os termos “coleta de dados”, “tratamento de dados”, “anonimização”, “bloqueio”, “prevenção”, “riscos”, “medidas, salvaguardas e mecanismos de mitigação de riscos” e “relatórios de impacto à proteção de dados pessoais”; são alguns exemplos de aspectos tecnológicos que permeiam o texto legislativo.

- **Pergunta de pesquisa:** de que forma a área de SI, por meio de suas normas e boas práticas, pode servir como ferramental tecnológico aos procedimentos de implantação da LGPD?

Aspectos Tecnológicos da Proteção de Dados Pessoais e da SI

- **Paradoxo:** lei visa proteger dados e a segurança tem por base a informação!

Tipologia: dado, informação e conhecimento.
Fonte: adaptado de (DAVENPORT, 1998)

PUCPR
GRUPO MARISTA

Aspectos Tecnológicos da Proteção de Dados Pessoais e da SI

- Tratamento de dados (LGPD, art. 5º, inciso X)

Ciclo de vida dos dados.
Fonte: adaptado de (FREITAS; TEIDER, 2019)

Aspectos Tecnológicos da Proteção de Dados Pessoais e da SI

- **Segurança da Informação** é (Norma ABNT NBR ISO/IEC 17799, a partir de 2007 passou a ser ISO/IEC 27002):

> a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

Aspectos Tecnológicos da Proteção de Dados Pessoais e da SI

- Segurança da Informação tem por base algumas **propriedades**, a saber (ISO/IEC 27002):
  - Confidencialidade,
  - Integridade,
  - Disponibilidade da informação,
  - Autenticidade,
  - Responsabilidade,
  - Não repúdio,
  - Confiabilidade.

Normas ISO como Ferramental de Planejamento Tecnológico voltado à Implantação da LGPD

- As normas ISO/IEC da família 27000 foram preparadas para “prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).”

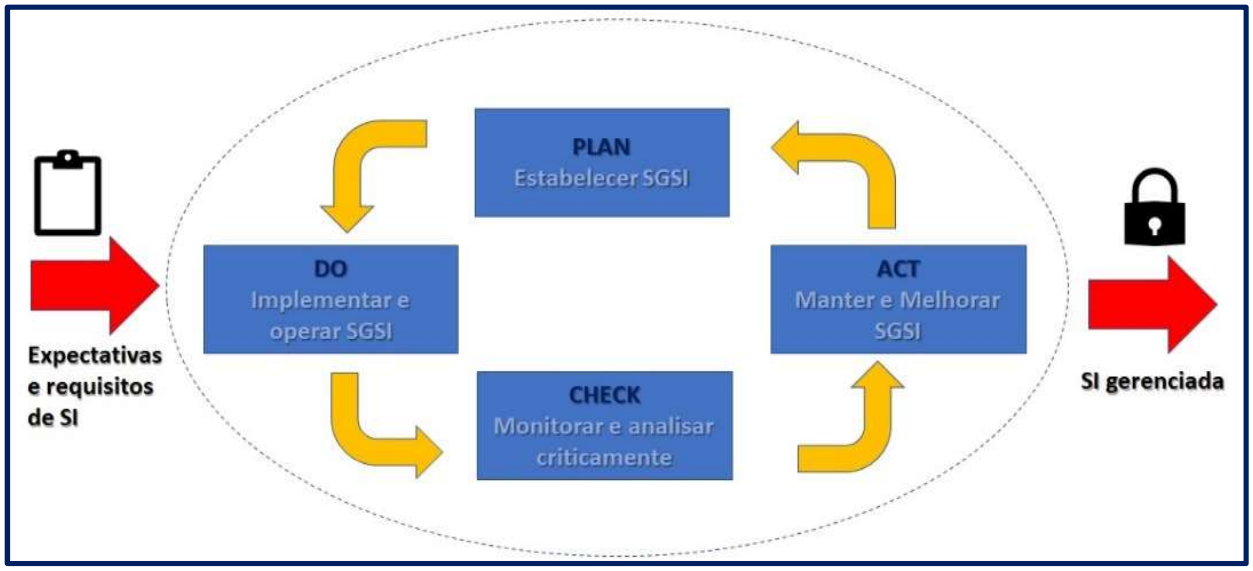
PUCPR
GRUPO MARISTA

Ciclo tecnológico de proteção de dados e segurança da informação na LGPD.
Fonte: adaptado de (FREITAS; TEIDER, 2019)

Quadro 01: Especificação das normas ISO 27000. Fonte: os autores.

Norma ISO	Conteúdo
ISO 27000	Generalidades, definições e diretrizes
ISO 27001	Técnicas de segurança para Sistemas de Gestão da Segurança da Informação (SGSI)
ISO 27002	Boas práticas para SGSI
ISO 27003	Diretrizes para implantação de um SGSI
ISO 27004	Indicadores de desempenho do SGSI
ISO 27005	Gestão de riscos de segurança da informação
ISO 27006	Requisitos e normas para organizações de auditoria e certificação pela ISO 27001/2
ISO 27007	Diretrizes para auditoria ISO 27001/2
ISO 27008	Diretrizes para auditoria de controles de SGSI
ISO 27010	Guia para a comunicação em gestão da segurança da informação
ISO 27014	Técnicas para governança da segurança da informação
ISO 27017	Controles específicos para computação em nuvem
ISO 27701 (antiga 27552)	Requisitos e exigências para estabelecer um Sistema de Gerenciamento de Informações de Privacidade

Normas ISO como Ferramental de Planejamento Tecnológico voltado à Implantação da LGPD – ISO/IEC 27001



Modelo PDCA aplicado aos processos do SGSI.
Fonte: adaptado de (FREITAS; TEIDER, 2019)

PUCPR
GRUPO MARISTA

Normas ISO como Ferramental de Planejamento Tecnológico voltado à Implantação da LGPD – ISO/IEC 27001

- Deve-se destacar alguns benefícios propostos pela norma ISO 27001, a saber:

  - Reduz o risco de responsabilidade pela não implementação ou determinação de políticas e procedimentos;
  - Oportunidade de identificar e corrigir pontos fracos;
  - A alta direção assume a responsabilidade pela SI;
  - Permite revisão independente do sistema de gestão da SI;
  - Oferece confiança aos parceiros comerciais, partes interessadas e clientes;
  - Melhor conscientização sobre segurança;
  - Combina recursos com outros Sistemas de Gestão;
  - Mecanismo para se medir o sucesso do SI.

Normas ISO como Ferramental de Planejamento Tecnológico voltado à Implantação da LGPD – ISO/IEC 27002

- No tocante à avaliação dos riscos, que já devem estar levantados e analisados, a ISO 27002 determina, em seu item 4.2, para cada um deles a decisão sobre o tratamento de risco e cujas opções possíveis incluem:

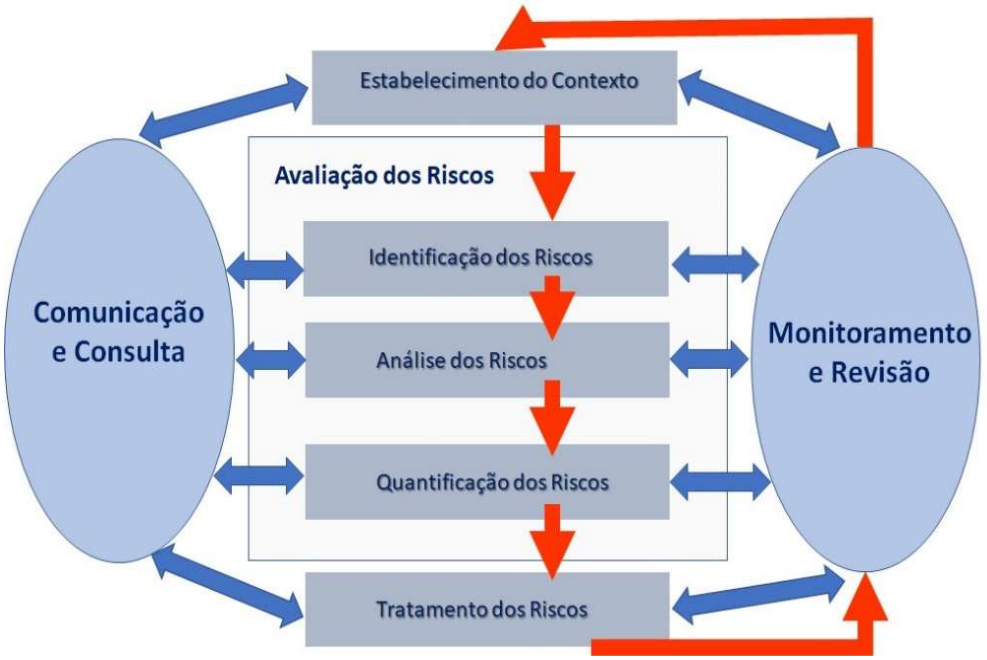
  a) aplicar controles apropriados para redução;

  b) conhecer e aceitar os riscos;

  c) evitar riscos, não permitindo algumas ações que os causem;

  d) transferir os riscos para terceiros (exemplo: fornecedores, seguradoras, entre outros).

Normas ISO como Ferramental de Planejamento Tecnológico voltado à Implantação da LGPD – ISO/IEC 27002



Avaliação de riscos tecnológicos e a LGPD.
Fonte: adaptado de (FREITAS; TEIDER, 2019)

PUCPR
GRUPO MARISTA

Normas ISO como Ferramental de Planejamento Tecnológico voltado à Implantação da LGPD – ISO/IEC 27701

- Aprimorar o SGSI já existente nas organizações, com requisitos adicionais e que tratam especificamente da privacidade de dados.

- Estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Informações de Privacidade – SGIP (*Privacy Information Management System* - PIMS) .

PUCPR
GRUPO MARISTA

Modelos de Boas Práticas: ITIL e COBIT

- **ITIL - *Information Technology Infrastructure Library***, modelo de boas práticas para gerenciamento de serviços de TI mais amplamente empregado no mundo.

- Aponta caminhos já consolidados de como fazer o gerenciamento da TI com foco no cliente e na alta qualidade dos serviços prestados.

Modelos de Boas Práticas: ITIL e COBIT

- **COBIT - *Control Objectives for Information and Related Technologies*** (Objetivos para Controle de Informações e Tecnologias Relacionadas), estrutura de gerenciamento e governança de TI provida pela ISACA (*Information Systems Audit and Control Association* - Associação de Auditoria e Controle de Sistemas de Informação).

Modelos de Boas Práticas: ITIL e COBIT

- **COBIT** - implantação da governança de TI, bem como controle dos processos.
- **ITIL** - gestão de serviços com atividades complementares.
- COBIT fornece controles implementáveis sobre governança e gerenciamento de TI, organizados em processos relacionados à TI, que suportam o cumprimento de vários requisitos de negócio, por exemplo: alocação de recursos, uso e proteção de dados, entre outros

Considerações Finais

- Segurança da Informação não somente pode servir como ferramental tecnológico aos procedimentos de implantação da LGPD, mas é essencial para a conformidade das organizações com a LGPD.
- Normas e modelos não apresentam fórmulas mágicas para um bom planejamento e aprimoramento do sistema de TI nas organizações, mas fornecem caminhos.

Considerações Finais

- A **LGPD** está dando a oportunidade de mudança de **paradigma**, ou seja, da coleta "**gulosa**" de dados para um **meio ambiente digital** saudável, seguro, ético e, por fim, bom para se viver.

CAVEDON, Ricardo ; FERREIRA, Heline S.; FREITAS, C.O.A.. O Meio Ambiente Digital sob a Ótica da Teoria da Sociedade de Risco: Os avanços da informática em debate. Revista Direito Ambiental e Sociedade, v. 5, p. 194-223, 2015.

FREITAS, C. O. A.; SANTOS, H. G. ; PASINATO, R. . A Segurança da Informação como Ferramental Técnico da Proteção de Dados Pessoais. In: Mariana Pereira Faria; Rafael Aggens Ferreira da Silva; Rhodrigo Deda Gomes. (Org.). Direito e Inovação - Volume 3. 1ed.Curitiba: NCA - Comunicação e Editora LTDA, 2020, v. 3, p. 233-265.

Obrigada!

cinthia.freitas@pucpr.br

PUCPR
GRUPO MARISTA