



THE CYBER SKILL GAP

— YOUR PARTNER IN LEARNING —

WEBINAR SERIES 2019



WEBINAR DE HOJE:

BASTIDORES DA LGPD

AGENDA

Sobre Mim

Sobre o Livro

Sobre a Palestrante

Contexto

Princípios

Pontos Chave para Prática

SOBRE MIM

VAGNER NUNES

Tecnologista, conferencista, evangelista em segurança cibernética e executivo de negócios, com um histórico de trabalho na área de tecnologia da informação e gestão de associações, principalmente para empresas internacionais de IT/ICT.



SOBRE O LIVRO

THE CYBER SKILL GAP!

01

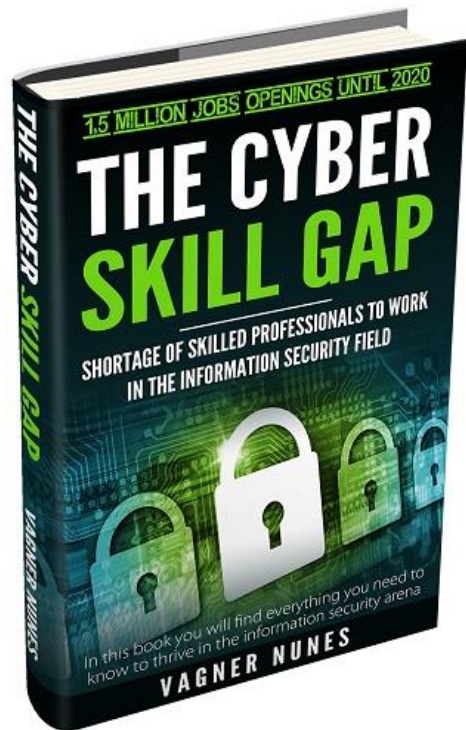
O livro explica de forma clara e concisa, por que esse fenômeno está acontecendo, quais serão as consequências para essa “escassez” e como os profissionais podem aproveitar as enormes oportunidades nessa área.

02

Altos salários e carreira de longo prazo tem um preço: o candidato deve ser um eterno aprendiz e dedicar muito tempo estudando e compreendendo a dinâmica dessa área.

03

Uma coisa é certa: as ameaças sempre aumentarão e você precisa estar preparado!



APOIADOR

CLAUDIO DODT

1. CUPOM DE DESCONTO - ISO 27001 - [Curso completo para certificação EXIN ISFS!](#)
2. CUPOM DE DESCONTO - PSI - [Construindo uma Política de Segurança da Informação \(PSI\)](#)

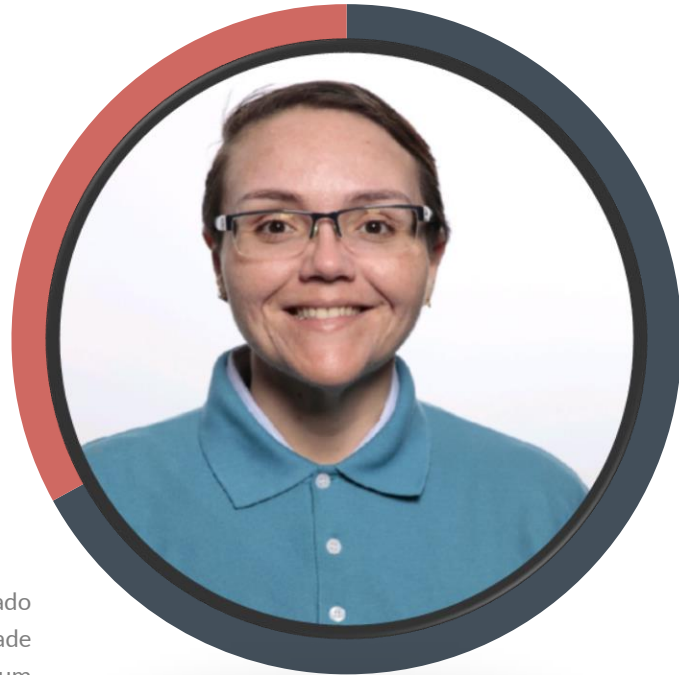


PALESTRANTE

ALESSANDRA MARTINS

Formada em Licenciatura em Informática pela Universidade do Estado do Amazonas, Especialista em Governança de TI pela Universidade Católica de Brasília, Certificações ISO 27002, ITIL v3, COBIT5, Scrum Master, KMP I, CTFL, e outras.

Atuando no Mercado de Tecnologia da Informação desde 2004, atuando há mais de 5 anos, voltada para Qualidade de Software, DevSecOps, Segurança da Informação, Governança de TI, SI e Corporativa.



CONTEXTO

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

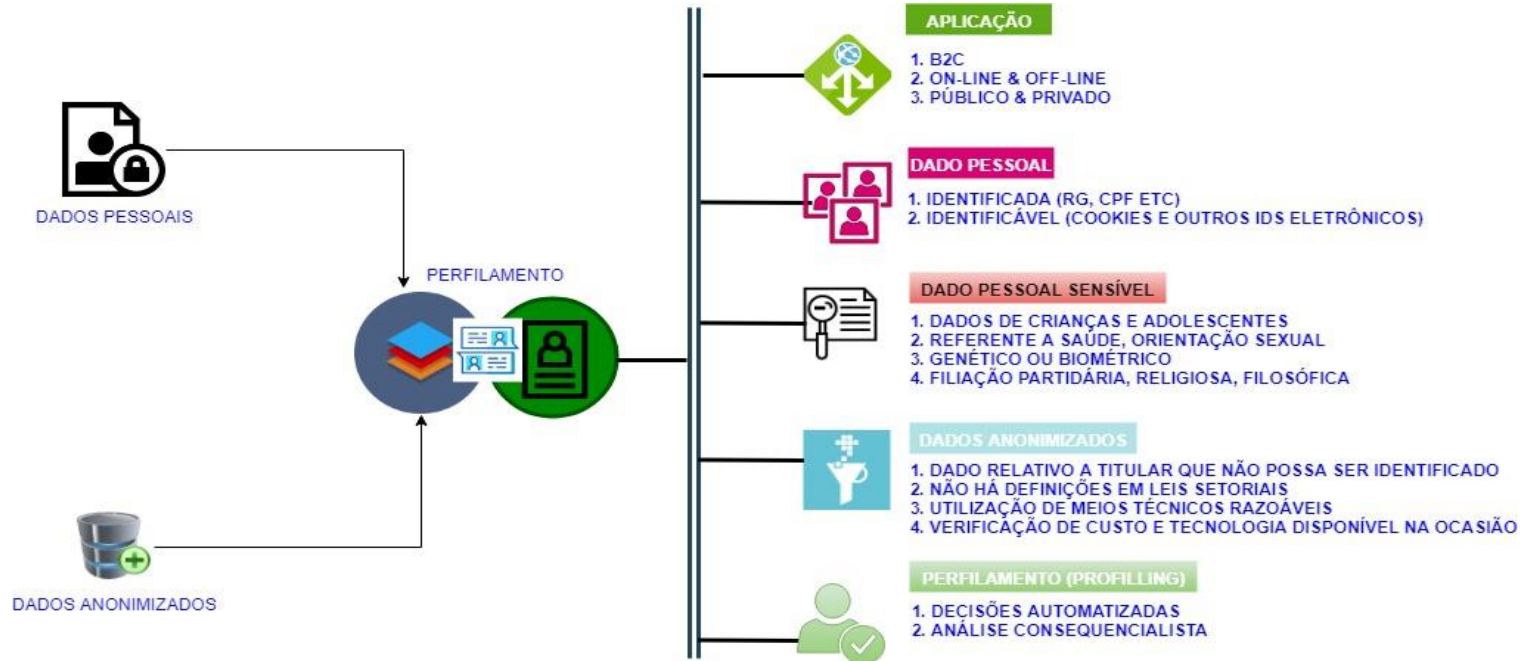
Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- A operação de tratamento seja realizada no território nacional
- A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei 13.853, de 2019)
- Os dados pessoais objeto do tratamento tenham sido coletados no território nacional

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

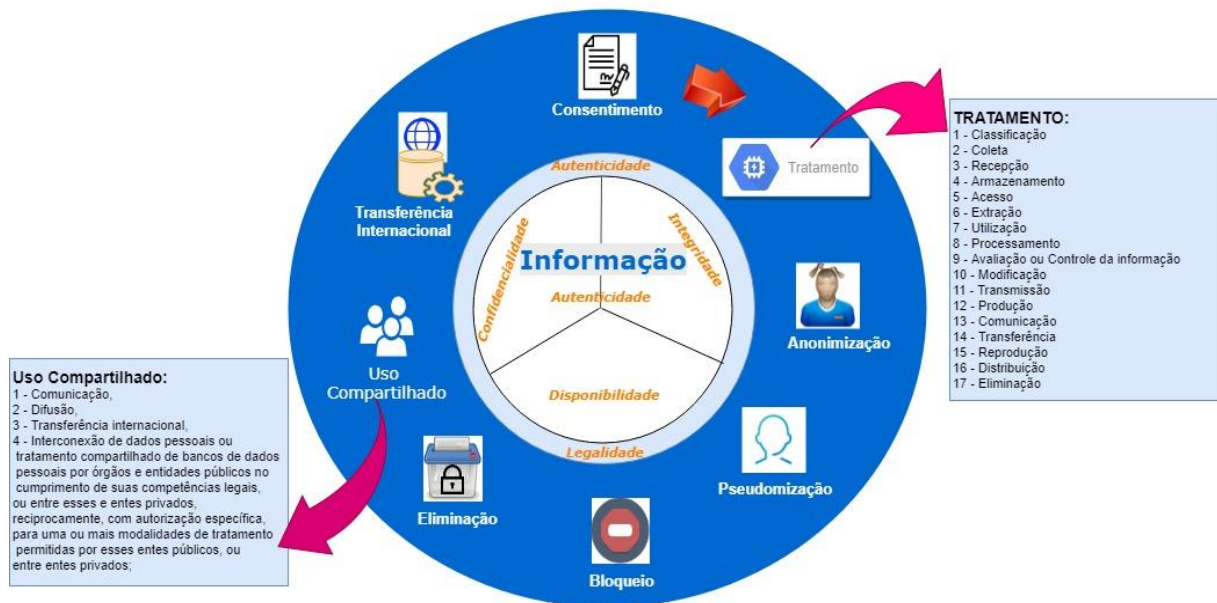
OBJETOS E ESCOPO



CONTEXTO DA LGPD

OPERAÇÕES

Ciclo de Operações da Informação - LGPD



PAPEIS



Pessoa Natural - Titular dos Dados, pessoa física particular, pessoa natural



Órgão de pesquisa- órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;



Agentes de Tratamento - refere-se ao conjunto do Controlador e Operador juntos



Autoridade Nacional de Proteção de Dados (ANPD) - órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional



Controlador - Responsável pela operações de tratamento dos dados pessoais, pessoa física ou jurídica de caráter público ou privado;



Encarregado - Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;



Operador - Quem executa o tratamento em nome do Controlador, pessoa física ou jurídica de caráter público ou privado;

DIREITOS



Quando o tratamento de Dados pessoais for Condição para o fornecimento de produto ou serviço ou para o exercício de direito, o **Titular deverá ser informado com destaque sobre este fato**

O Consentimento:

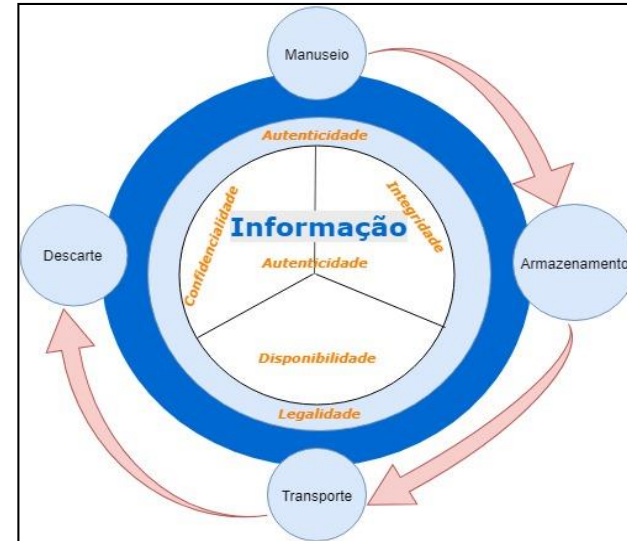
- Deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas;
- Será considerado nulo caso as informações fornecidas ao Titular tenham conteúdo enganoso ou abusivo, ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca;
- Caso seja dado por escrito, deverá constar de cláusula destacadas das demais cláusulas contratuais;
- Vedado o tratamento de dados pessoais mediante Vício de Consentimento;

DEVERES



POR ONDE COMEÇAR?

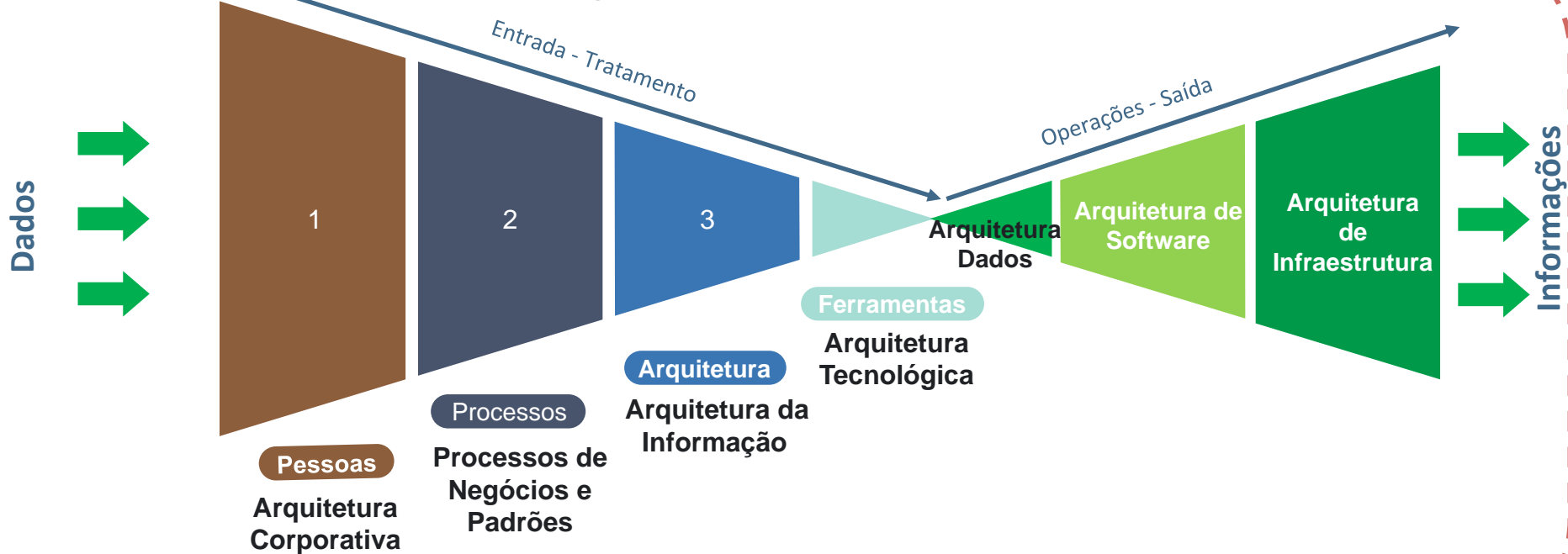
BASTIDORES



POR ONDE COMEÇAR?

BASTIDORES

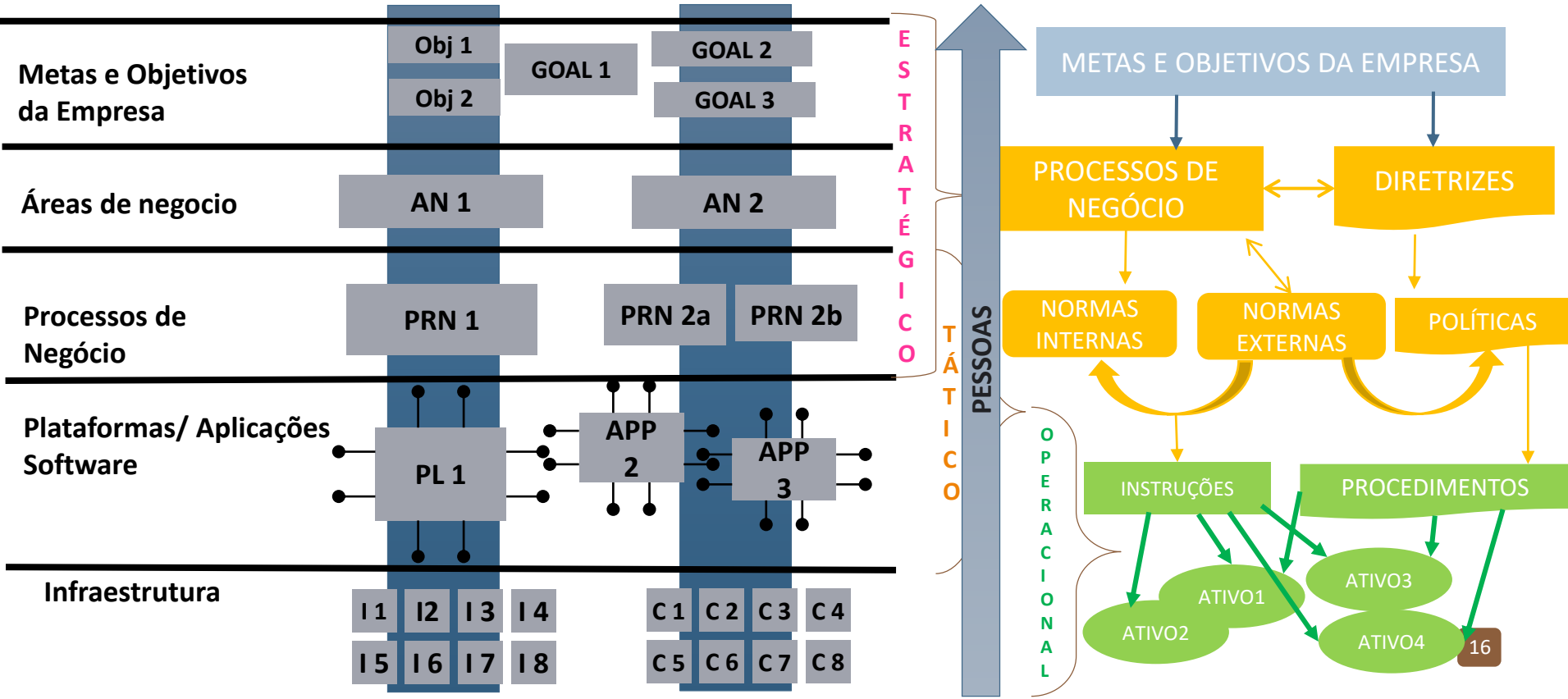
Arquiteturas Boas Práticas



POR ONDE COMEÇAR?

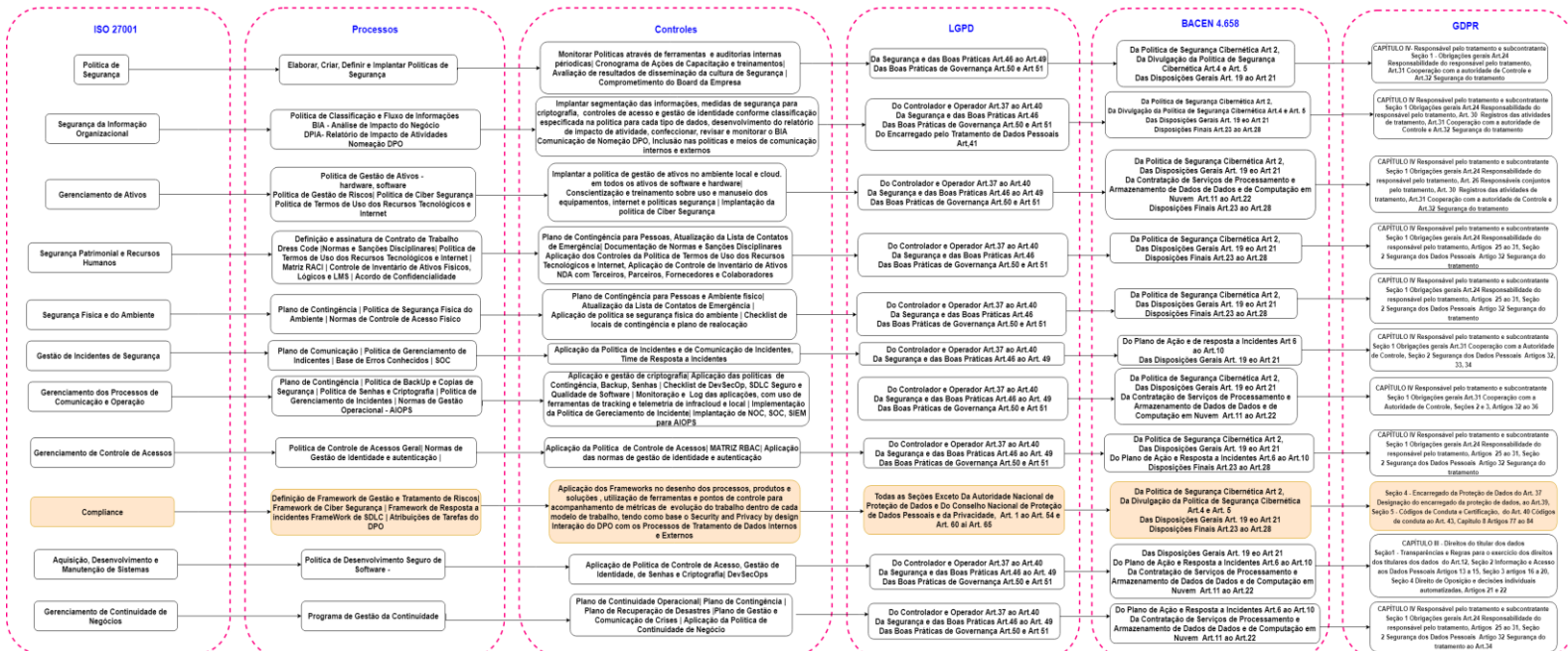
BASTIDORES

Como a Arquitetura pode Influenciar



GOVERNANÇA COMPARATIVO

Governança e Compliance Alinhamentos: Visão de Processos, Controles, Regulações



Security by Design Referências Utilizadas

OWASP TOP 10
NIST 800-61R2
ISO 27001
ISO 31000
NIST 800-30
NIST 800-34R1
NIST SP -800-190
NIST SP 1600-5B

Security by Design abordagem Prática

PSD - Plano de Segurança Digital utilizando SGSI
SDLC Seguro utilizando DEVSECOPS
Operações Confiáveis e Inteligentes com AIOPS



Privacy by Default
Somente os Dados
Estritamente Necessários



Solicitação de Consentimento
do Titular dos Dados
para Processamento
Direito de Peticionamento



Governança de Dados



Proteção dos Dados
Security by Default
Governança de Segurança
da Informação



SDLC Seguro para
automação de processos
e utilização de algoritmos
Security by Design



Utilização das Informações
obtidas mediante tratamento
legal - **Privacy by Design**



Exclusão Segura dos Dados
mediante termo de controle,
peticionamento, finalidade
ou obrigação legal

Privacy by Design Referências

Utilizadas e Atendidas
ISO 29100 LGPD 13.709
ISO 27018 BACEN 4.658
Decreto 9.637 Lei 13.853 (MP 869)

PRINCÍPIOS

PRIVACY BY DESIGN



1 - Proatividade e não reatividade - Prevenir não remediar



2 - Embarcada no Design – Design visando a Privacidade



3- Segurança fim a fim - Proteção durante o ciclo de vida completo



4 - Respeito pela privacidade do Usuário - Mantenha centrado no usuário



5 - Privacidade como Configuração Padrão



6 - Funcionalidade Completa - Soma positiva não soma zero



7 - Visibilidade e Transparência - Mantenha aberto

Privacidade por Default significa que, uma vez que um produto ou serviço tenha sido liberado para o público, as configurações de privacidade mais rígidas devem ser aplicadas por padrão, sem nenhuma entrada manual do usuário final.

Além disso, quaisquer dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto devem ser mantidos apenas durante o tempo necessário para fornecer o produto ou serviço. Se mais informações do que o necessário para fornecer o serviço forem divulgadas, a "privacidade por padrão" foi violada.

PRINCÍPIOS

SECURITY BY DESIGN

1 - Minimizar a superfície de área de ataque

Através da utilização de patterns de desenvolvimento de código e boas práticas de desenvolvimento seguro.

2 - Estabelecimento de Padrões

Através da utilização de senhas fortes, ciclo de vida de senhas, autenticação multifator e tokens.

3 - Princípio do Menor Privilégio

Através da criação de contas com a menor quantidade de privilégios necessários para executar seus processos de negócios. Isso engloba direitos de usuário, permissões de recursos, como limites de CPU, memória, rede e permissões do sistema de arquivos.

4 - Princípio da Defesa em Profundidade

Utilizando um controle que seria razoável, mais controles que abordam riscos de diferentes maneiras são melhores. Os controles, quando usados em profundidade, podem tornar vulnerabilidades extremamente difíceis de explorar e, portanto, improváveis de ocorrer.

5 - Falhar com Segurança

Os aplicativos geralmente não processam transações por vários motivos. A forma como eles falham podem determinar se um aplicativo é seguro ou não, por exemplo se expõe, endpoints, paths, strings de conexão etc.

PRINCÍPIOS

SECURITY BY DESIGN

6 - Não Confie nos Serviços

Todos os sistemas externos com parceiros, integradores, brokers, devem ser tratados de maneira semelhante, os dados devem ser sempre verificados para garantir a segurança de exibição ou compartilhamento com o usuário final.

7 - Separação de deveres

Através da determinação de papéis que têm diferentes níveis de confiança do que usuários normais. Em particular, os administradores são diferentes dos usuários normais, utilizando RBAC para atribuição de permissionamento.

8 - Evitar a segurança por obscuridade

A segurança de um aplicativo não deve depender do conhecimento do código-fonte mantido em segredo. A segurança deve se basear em muitos outros fatores, incluindo políticas razoáveis de senha, defesa em profundidade, limites de transação de negócios, arquitetura de rede sólida e controles de fraude e auditoria.

9 - Mantenha a Segurança simples

Onde os desenvolvedores devem evitar o uso de negativos duplos e arquiteturas complexas quando uma abordagem mais simples seria mais rápida e simples.

10 - Correção de Problemas de Segurança da maneira correta

Quando um problema de segurança for identificado, é importante desenvolver um teste para ele e entender a causa raiz do problema. Quando padrões de design são usados, é provável que o problema de segurança seja difundido entre todas as bases de código, portanto é essencial desenvolver a correção correta sem introduzir regressões.

COMPARATIVO

PSBD 1 ao 10



CiberSegurança

- Política de CiberSegurança
- Política de Classificação e Fluxo da Informação
- Política de Desenvolvimento Seguro
- Política de Senhas
- Normas de Criptografia
- Gestão de Identidade e Controle de Acesso



Resposta a Incidentes

- Política Corporativa de Segurança da Informação
- Política de Gestão de Incidentes
- Plano de Gestão de Comunicação e Crises
- Análise de Impacto do Negócio - BIA
- CIRT
- Base de Conhecimento



Continuidade de Negócios

- Programa de Gestão da Continuidade
- Política de Continuidade do Negócio
- Plano de Recuperação de Desastres
- Plano de Contingência
- Plano de Continuidade Operacional
- Política de Gestão de Ativo
- Gestão de Defeitos



Educação e Conscientização

- Plano de Segurança Física e do Ambiente
- Política de Segurança Patrimonial e Recursos Humanos
- Cronograma de Ações e Eventos de Conscientização sobre Segurança da Informação e Pessoal
- Cronograma de Educação e Capacitação



THAT'S ALL

OBRIGADO!