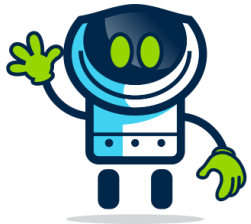


THE CYBER SKILL GAP

— YOUR PARTNER IN LEARNING —

WEBINAR SERIES 2019

WEBINAR DE HOJE:

BASTIDORES DA LGPD

AGENDA

- Sobre Mim
- Sobre o Livro
- Sobre a Palestrante
- Fundamentos
- Princípios
- Conceitos e Aplicabilidade no día a dia

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.

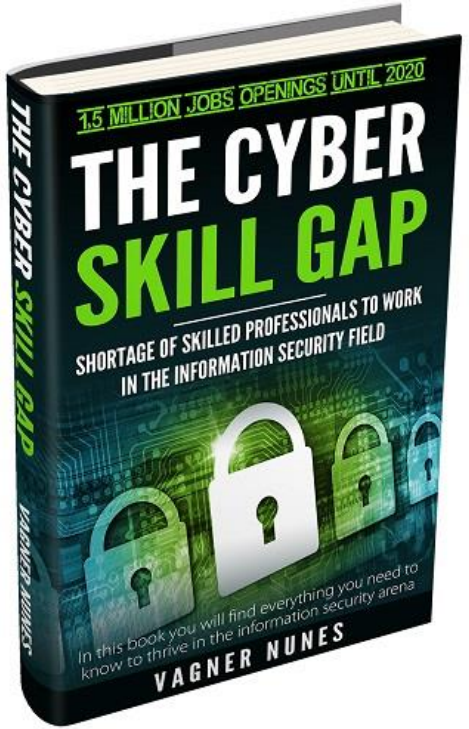
SOBRE O LIVRO

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, Projeots, DevSecOPs, Segurança da Informação, Governança de TI, SI e Corporativa.

FUNDAMENTOS

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

1. Respeito a Privacidade
2. Auto determinação informativa
3. A Liberdade de Expressão, de Informação, de Comunicação, de Opinião
4. A inviolabilidade da intimidade, da Honra e da Imagem
5. O Desenvolvimento Econômico e Tecnológico e a inovação
6. A Livre Iniciativa, A Livre Concorrência e a Defesa do Consumidor
7. Os Direitos Humanos, O Livre Desenvolvimento da Personalidade, A Dignidade e o Exercício da Cidadania Pelas Pessoas Naturais

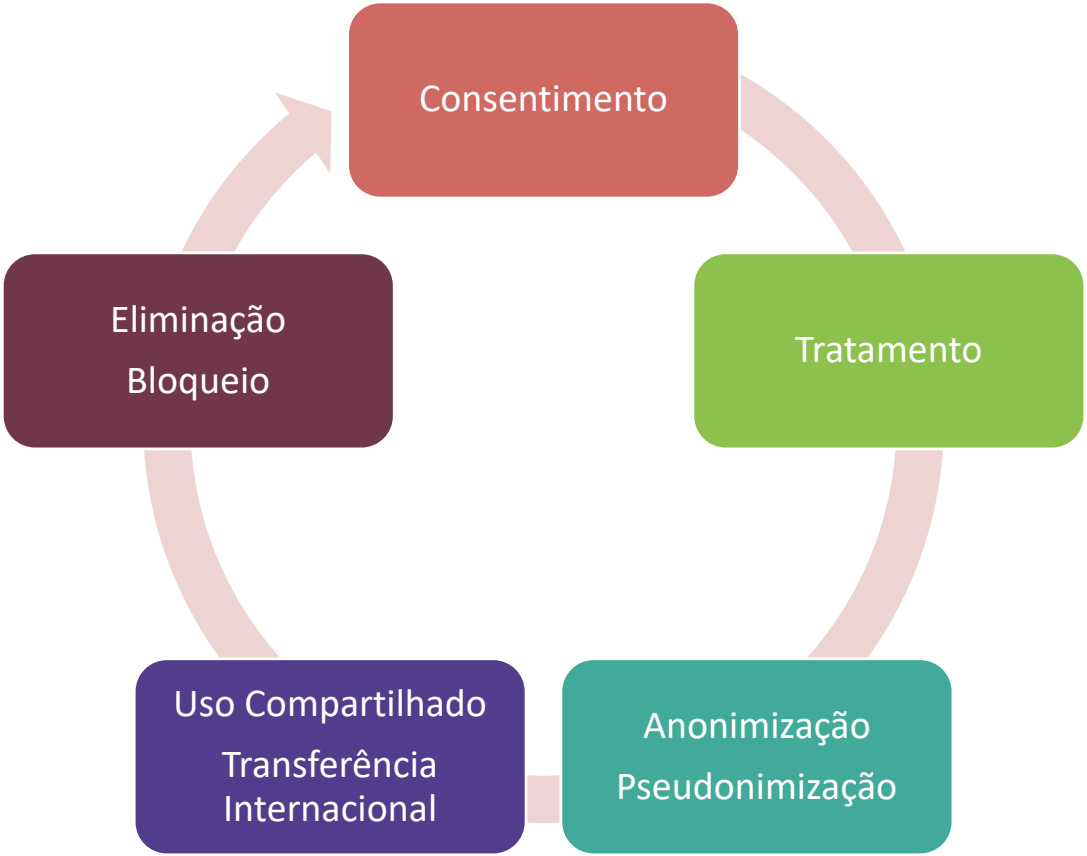
FUNDAMENTOS

OBJETOS E ESCOPO

Dados Pessoais	Dados Pessoais Sensíveis	Dados Anonimizados	Decisões Automatizadas
• CPF • RG • IP • Cookies • Geolocalização • Nome • Endereço	• Biometria • Saúde • Dados referente a orientação ou vida Sexual • Filiação Partidária, Filosófica, Sociológica	• Não identificável • Pseudonimizados • Reversível • Tecnologia e Meios Tecnicos Razoáveis	• Profiling • Análise Consequencialista

FUNDAMENTOS

OPERAÇÕES



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 & DEVERES

PRINCÍPIOS

PRIVACY BY DESIGN

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

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.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

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

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

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.

SEGURANÇA PILARES

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 Criptografía
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

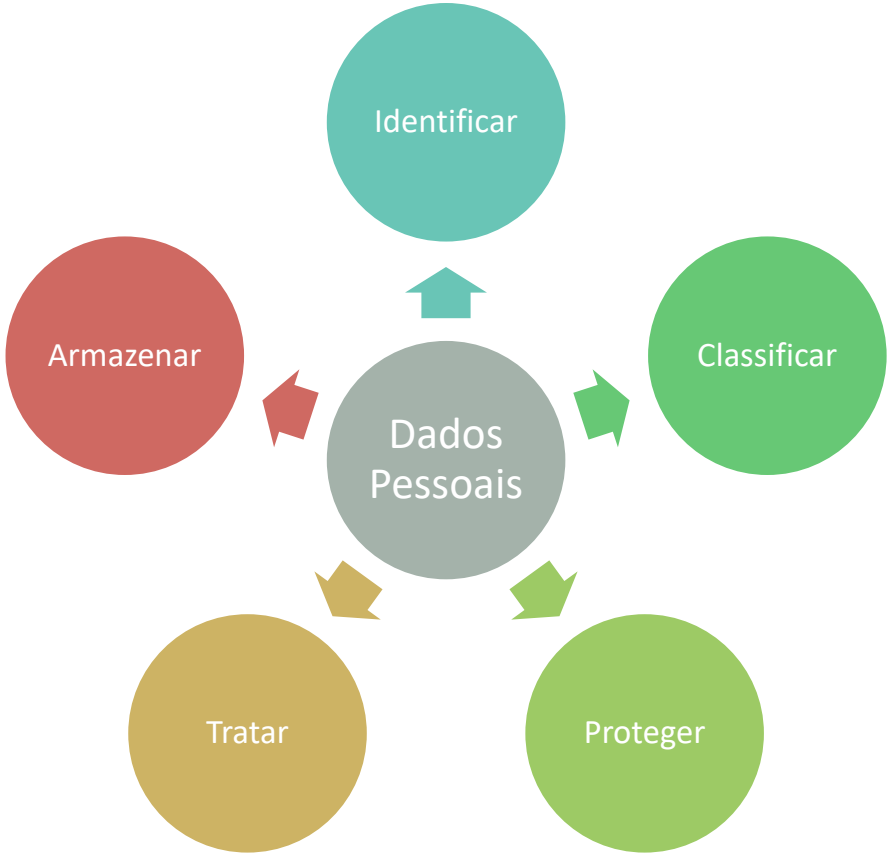
Programa de Gestão da Continuidade
Política de Continuidade do Negócio
Plano de Recuperação de Desastres
Plano de Contingência
Plano de Continuidade Operacional
Política de Gestão de Ativo
Gestão de Defeitos

Educação e Conscientização

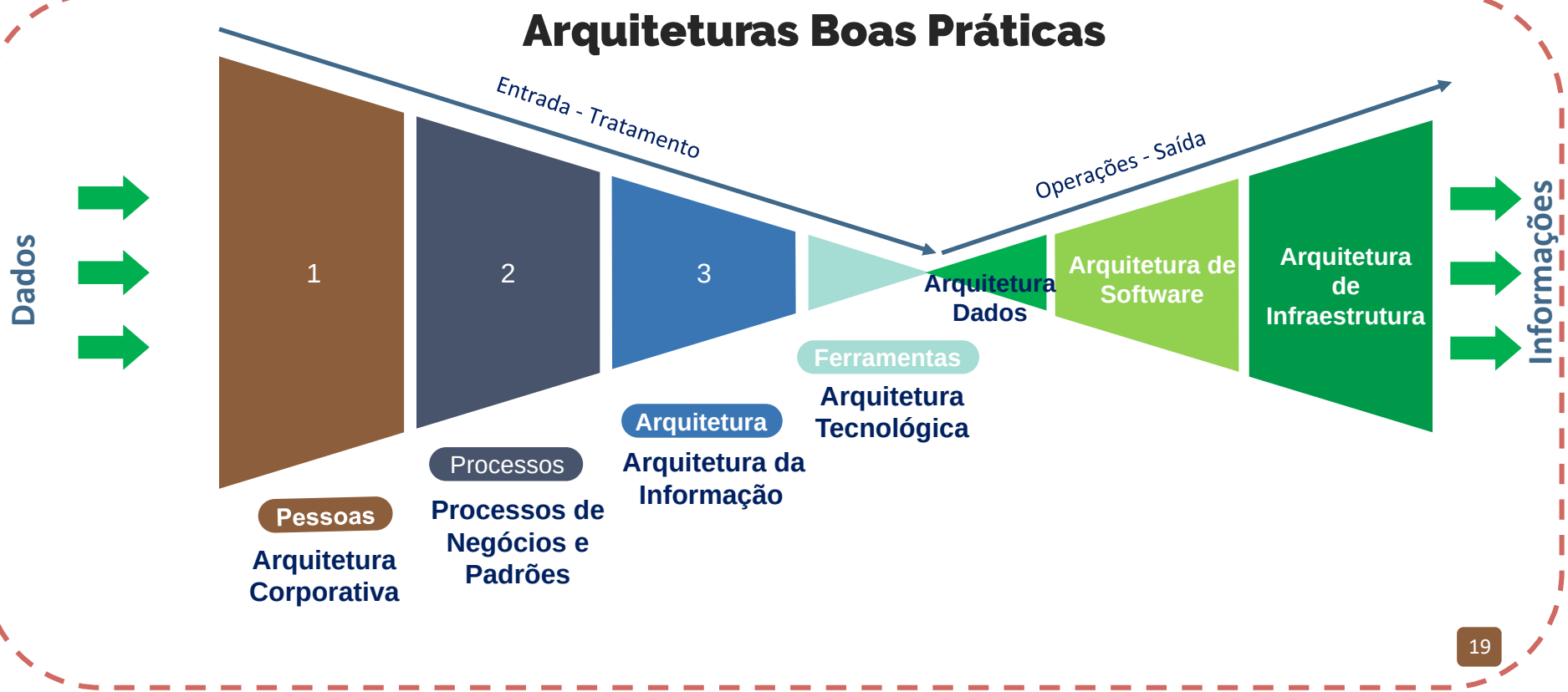
Plano de Segurança Física e do Ambiente
Política de Segurança Patrimonial e Recursos Humanos
Cronograma de Ações e Eventos de Conscientização sobre Segurança da Informação e Pessoal
Cronograma de Educação e Capacitação

POR ONDE COMEÇAR?

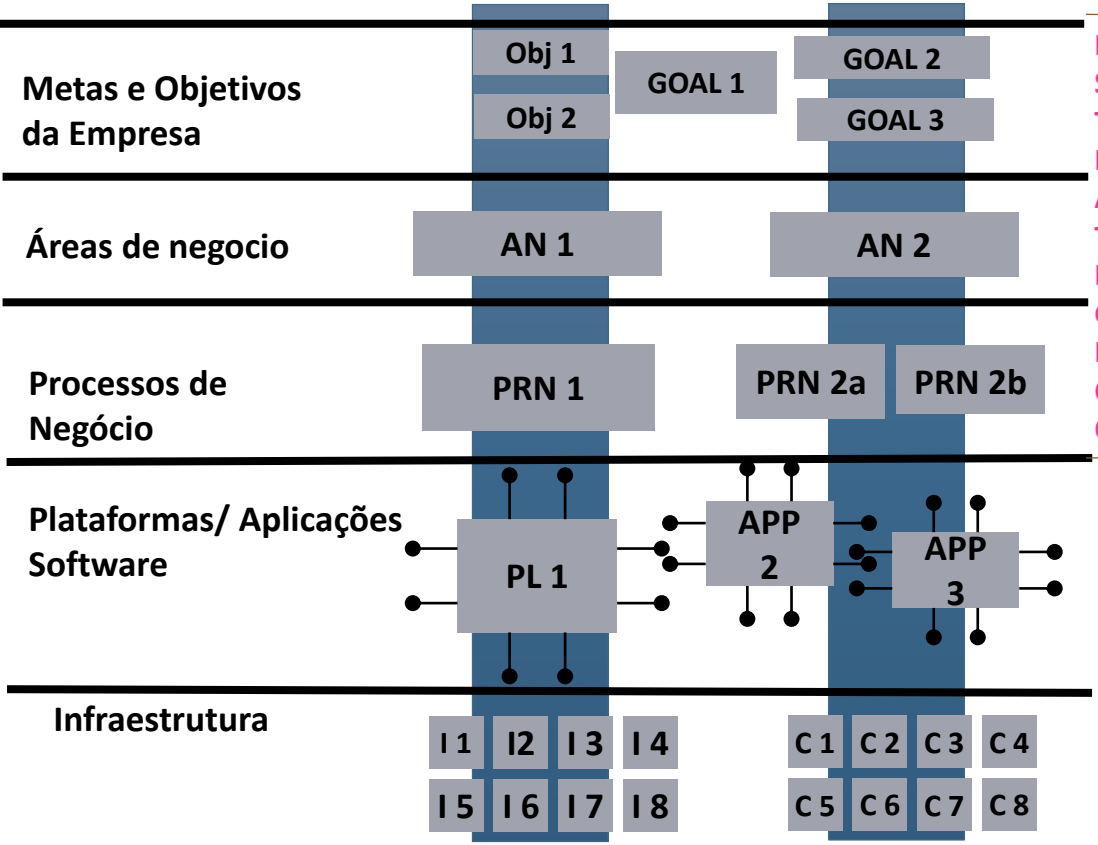
CONCEITOS E APLICABILIDADE

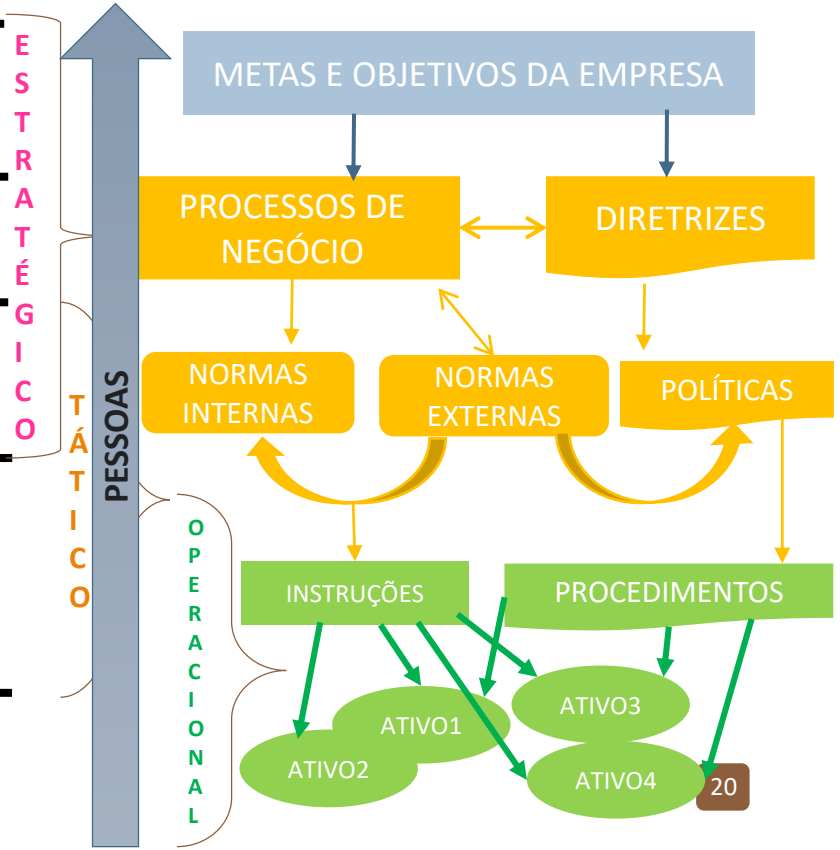


CONCEITOS E APLICABILIDADE

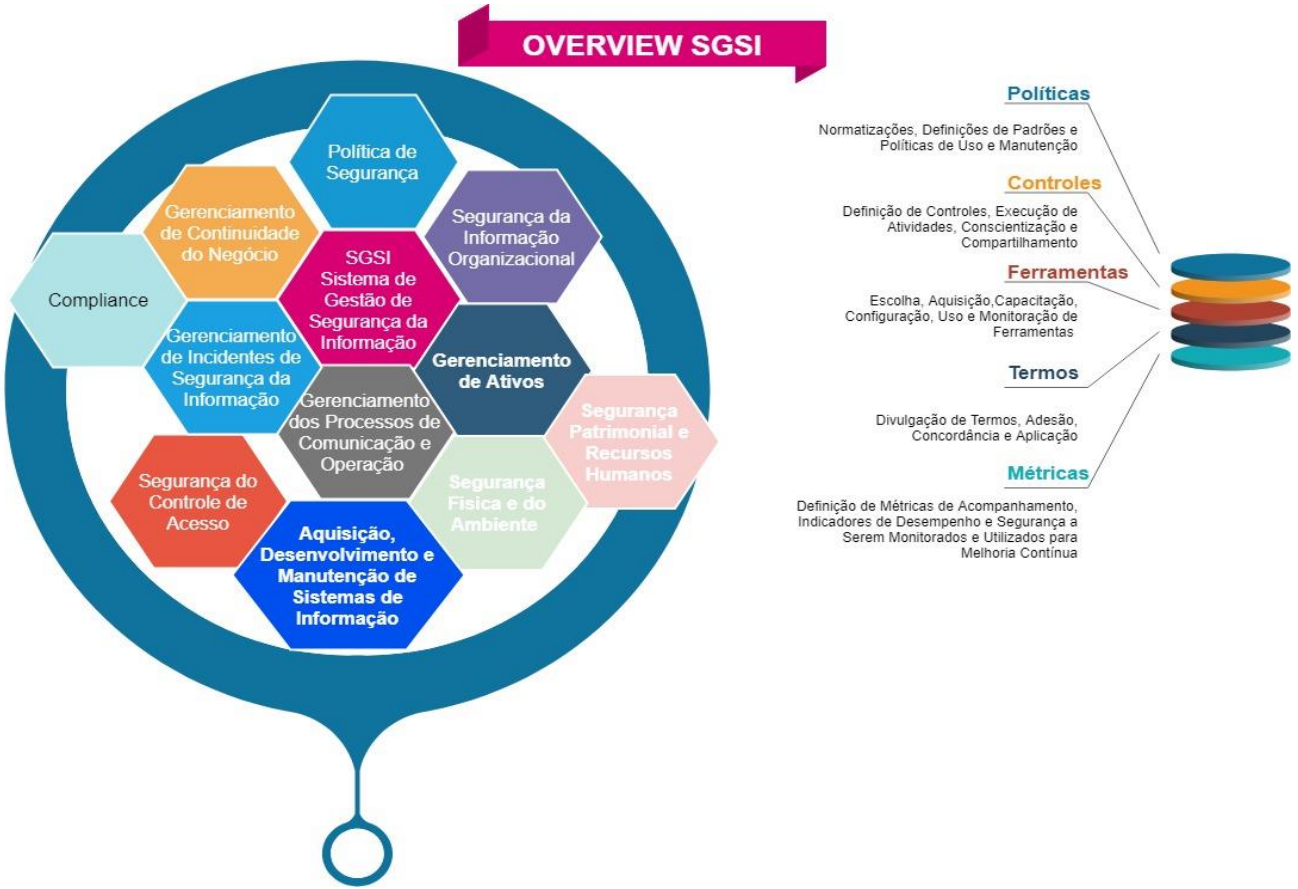


CONCEITOS E APLICABILIDADE





CONCEITOS E APLICABILIDADE



THAT´S ALL

OBRIGADO!