


mindthesecc

/SÃO PAULO

MAIS UM
EVENTO:  **Flipside**
SECURITY • BEYOND TECHNOLOGY

REALIZAÇÃO:  **Green Helmet**

Usable Security, Experiência do Usuário e como isso esta relacionado ao Privacy by Design?

Alessandra Monteiro Martins
Head GPS | DPO

Head GPS | DPO D1 Alessandra Monteiro 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, PDPFe outras.

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

ROTEIRO:

MITOS & CILADAS

CONTEITOS:
SEGURANÇA DA INFORMAÇÃO
GOVERNANÇAS
ARQUITETURAS
CICLOS DE VIDA

PRINCÍPIOS:
DATA PROTECTION BY DEFAULT
PRIVACY BY DESIGN E BY DEFAULT
SECURITY BY DESIGN
USABLE SECURITY
UX - USER EXPERIENCE

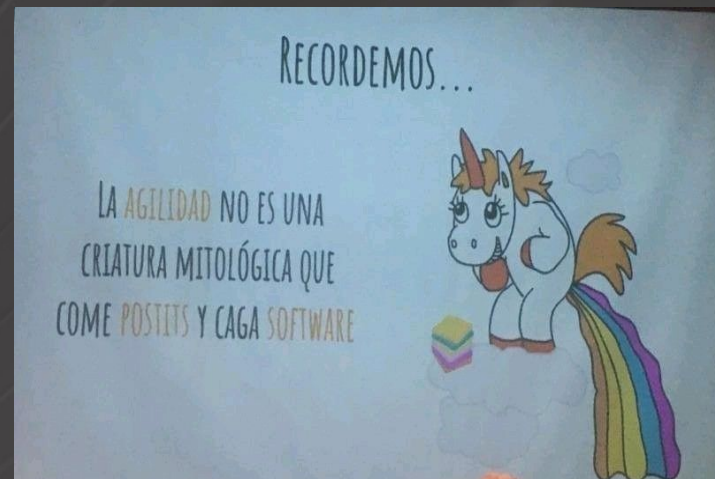
NEGÓCIOS
BOAS PRÁTICAS

mindthesec[®]
/SÃO PAULO

Mitos e Ciladas:

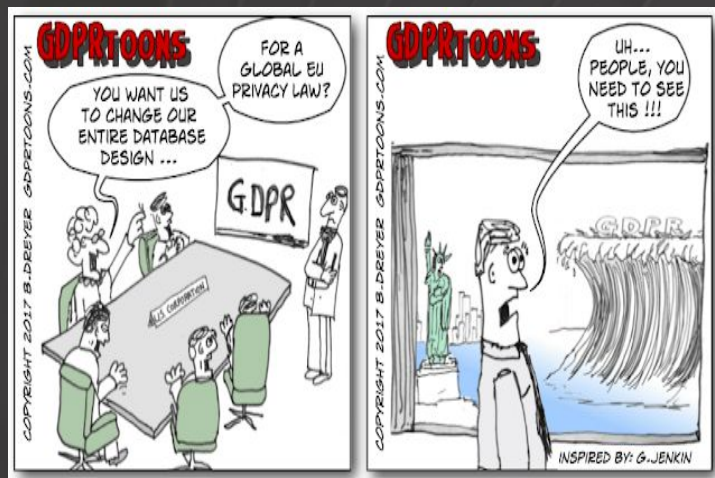


DEV + SEC + OPS

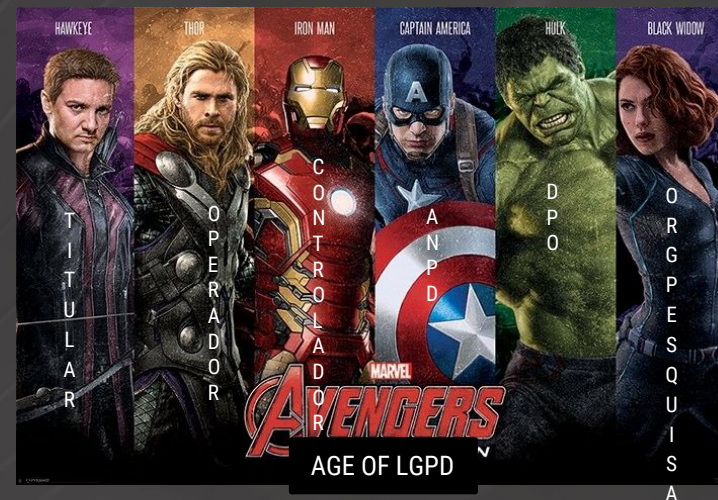


AGILIDADE

Mitos e Ciladas:



LEIS



PAPÉIS

Mitos e Ciladas:



UNUSABLE SECURITY



ALERTAS

Mitos e Ciladas:



SPAM ANÚNCIOS

"Faking security is the path to the dark side. Faking leads to false hope. False hope leads to false security. False security leads to suffering."

Totally real quote from Star Wars.



pagerduty SECURITY TRAINING FEB 2016 PUBLIC

CILADAS

Mitos e Ciladas:

What Yoda meant to say:

Java/Flash leads to
Vulnerabilities.

Vulnerabilities leads to
anger.

Anger leads to hate.

Hate leads to suffering.



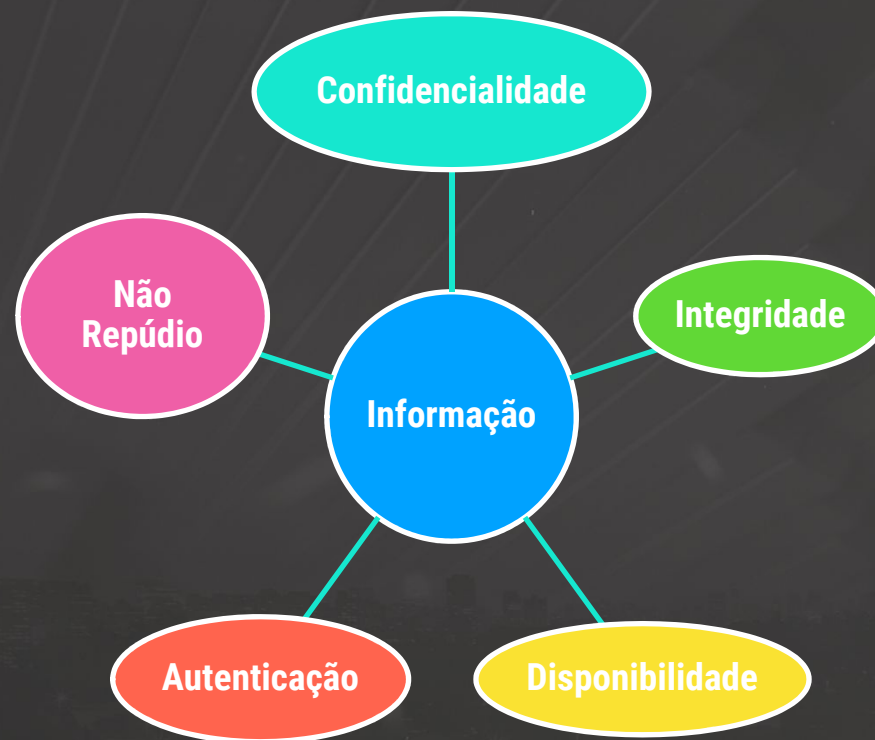
@nixcraft

VULNERABILIDADES

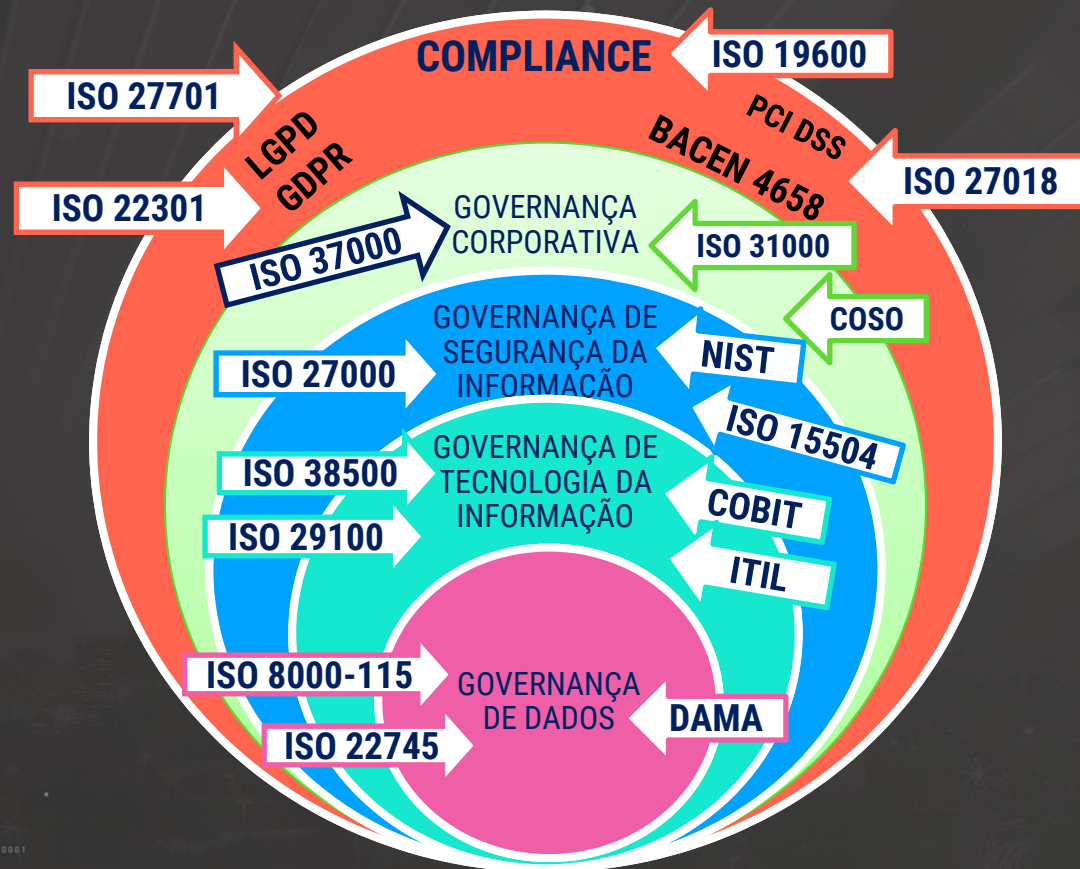


I.A SEM SUPERVISÃO

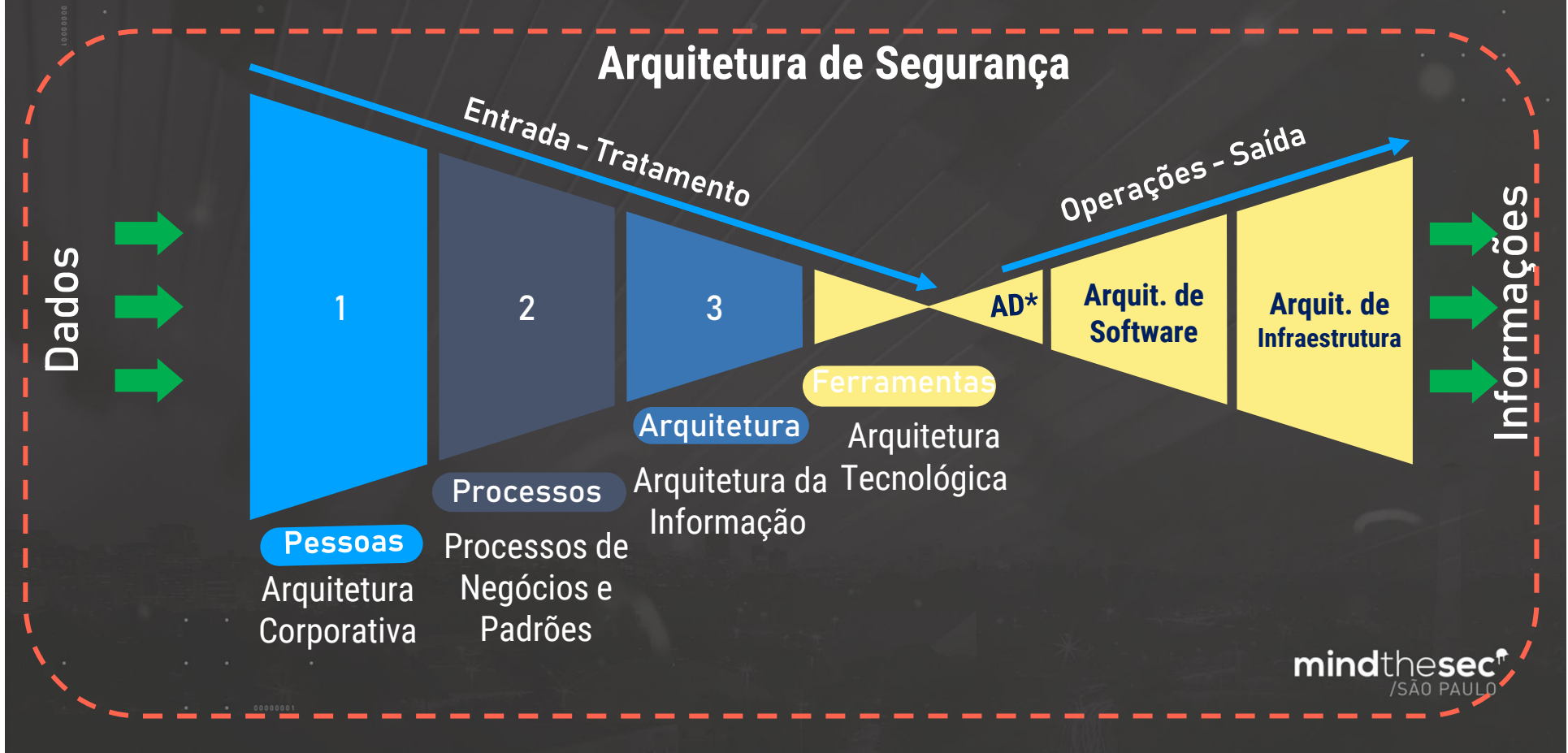
Conceitos: Segurança da Informação



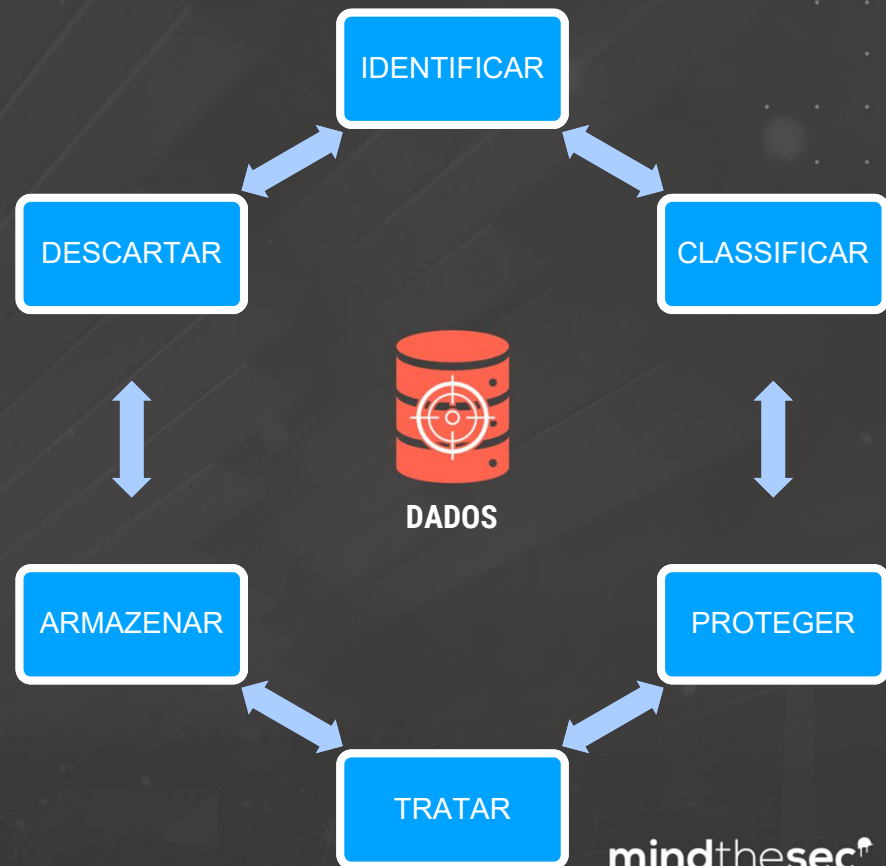
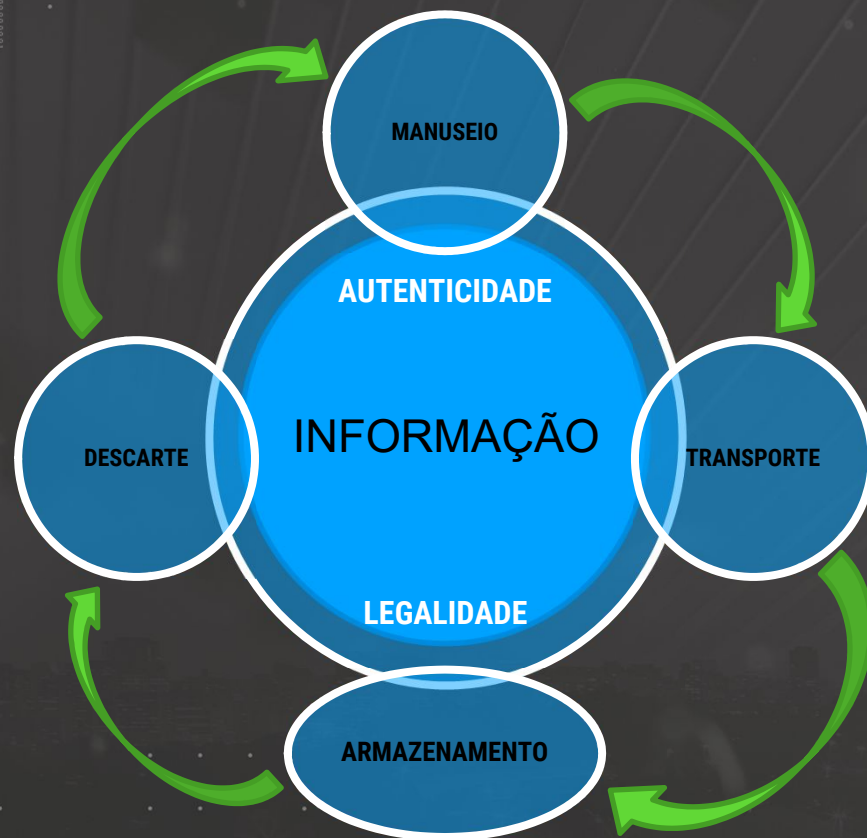
Conceitos: Governanças



Conceitos: Arquiteturas



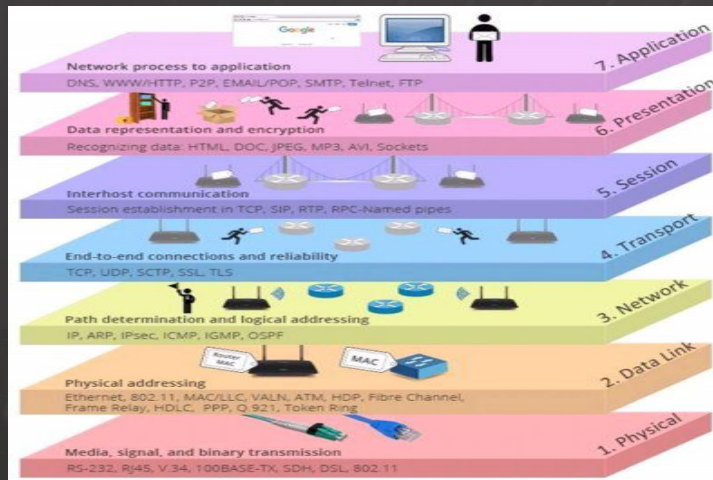
Conceitos: Ciclos de Vida



Princípios: Data Protection by Design e by Default

BY DESIGN:

“UMA ABORDAGEM QUE GARANTE QUE SEJAM ABORDADAS AS QUESTÕES DE PRIVACIDADE E PROTEÇÃO DE DADOS NA FASE DE DESIGN DE QUALQUER SISTEMA, SERVIÇO, PRODUTO OU PROCESSO E DEPOIS DURANTE TODO O CICLO DE VIDA.” ico.org.uk



BY DEFAULT:

“UMA ABORDAGEM QUE EXIGE QUE SEJAM PROCESSADOS APENAS OS DADOS NECESSÁRIOS PARA ATINGIR O OBJETIVO ESPECÍFICO PELO QUAL OS DADOS FORAM COLETADOS. É PRECISO ESPECIFICAR QUAIS DADOS SERÃO COLETADOS E TRATADOS ANTES DO INÍCIO DO PROCESSAMENTO, INFORMANDO ADEQUADAMENTE AS PESSOAS, PROCESSANDO APENAS OS DADOS ESPECIFICADOS E NECESSÁRIOS” ico.org.uk

DEVSECOPS + AGILE



mindthesec[®]
/SÃO PAULO

Princípios: Privacy by Design e by Default



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.

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
- 2 - Estabelecimento de Padrões
- 3 - Princípio do Menor Privilégio
- 4 – Princípio da Defesa em Profundidade
- 5 – Falhar com Segurança
- 6 - Não Confie nos Serviços
- 7 - Separação de deveres
- 8 - Evitar a segurança por obscuridade
- 9 - Mantenha a Segurança simples
- 10 - Correção de Problemas de Segurança da maneira correta

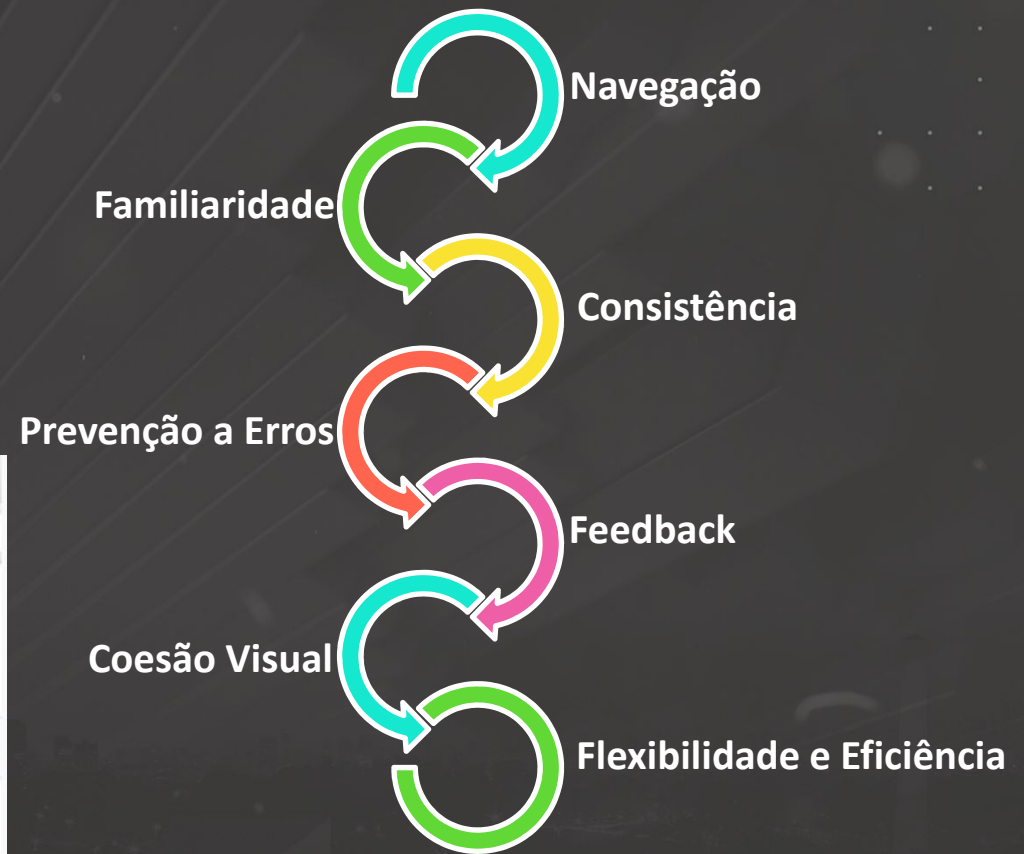
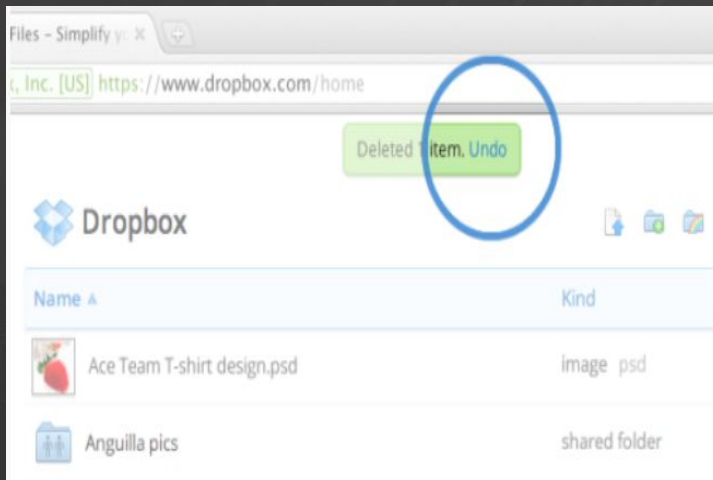
Princípios: USABLE SECURITY

SEGURANÇA E USABILIDADE ENTRAM EM HARMONIA QUANDO UM SISTEMA INTERPRETA CORRETAMENTE OS DESEJOS (EXPECTATIVAS) DO USUÁRIO



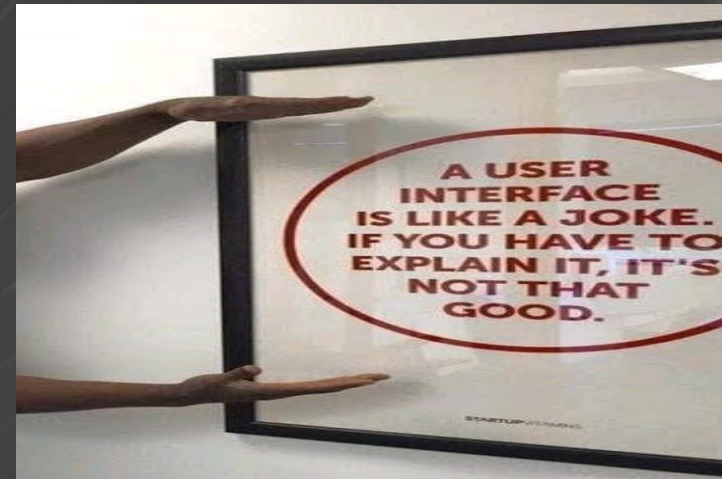
UX: User Experience

- ✓ Eficácia
- ✓ Eficiência
- ✓ Envolvimento
- ✓ Tolerância a erro
- ✓ Facilidade de Aprendizado



Negócios: Relacionamento US, UX e PbD

“ Usabilidade é mais do que apenas facilidade de uso. Você precisa garantir que os projetos sejam eficientes, eficazes, envolventes, fáceis de aprender e tolerantes a erros, se desejar que eles sejam bem-sucedidos. Obviamente, existem limitações no valor da usabilidade e, às vezes, é necessário fazer trocas para garantir a viabilidade econômica, por exemplo...”IDF



Negócios: Relacionamento US & UX

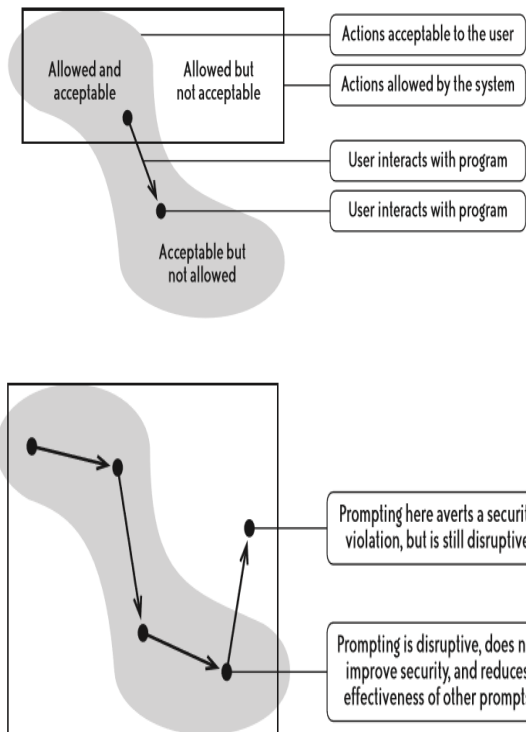


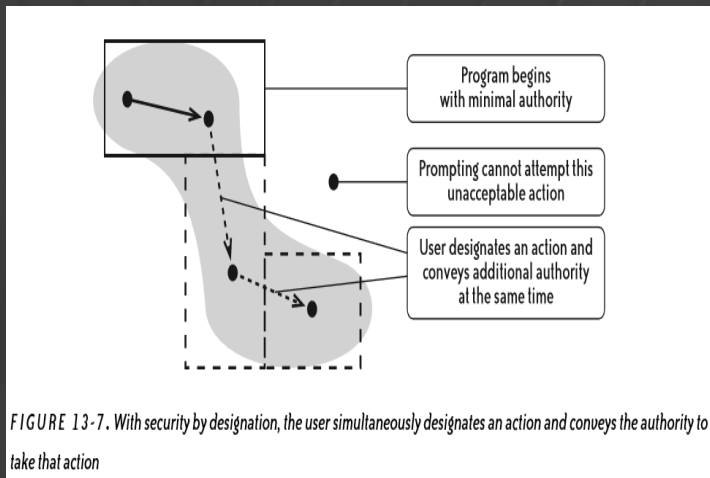
FIGURE 13-6. With security by admonition, the system has to guess when to warn the user of potential dangers

A Segurança por Advertência consiste em fornecer notificações às quais o usuário participa para manter a segurança.

Os usuários geralmente desejam usar coisas em que não confiam completamente.

Poucos Avisos ou a falta deles colocam os usuários em risco, avisos em excesso irritam o usuário. Quanto maior a discrepância entre ações aceitáveis e permitidas, mais severamente somos forçados a comprometer entre segurança e usabilidade.

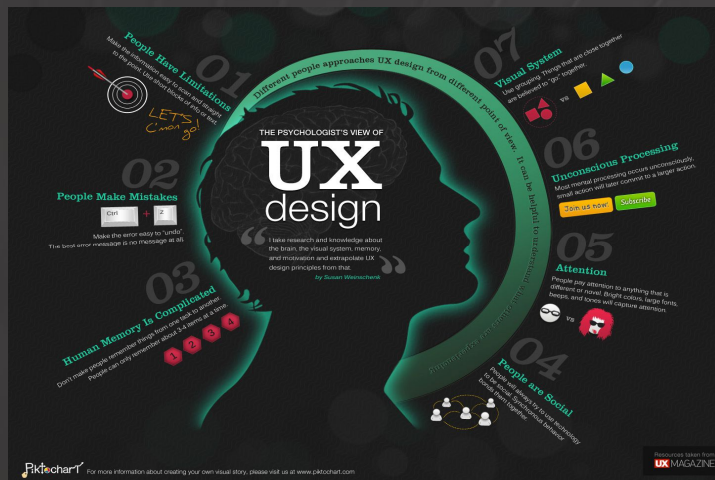
Negócios: Relacionamento US & UX



Segurança por Designação - O usuário designa uma ação simultaneamente e transmite a autoridade para executar a ação.

A combinação da autorização com a designação de intenção em uma única ação do usuário mantém uma correspondência dinâmica e próxima entre o conjunto permitido e o conjunto de ações aceitável. Os usuários não precisam estabelecer uma política de segurança detalhada antecipadamente e não precisam expressar suas intenções duas vezes.

Boas Práticas: Relacionamento US, UX e PbD



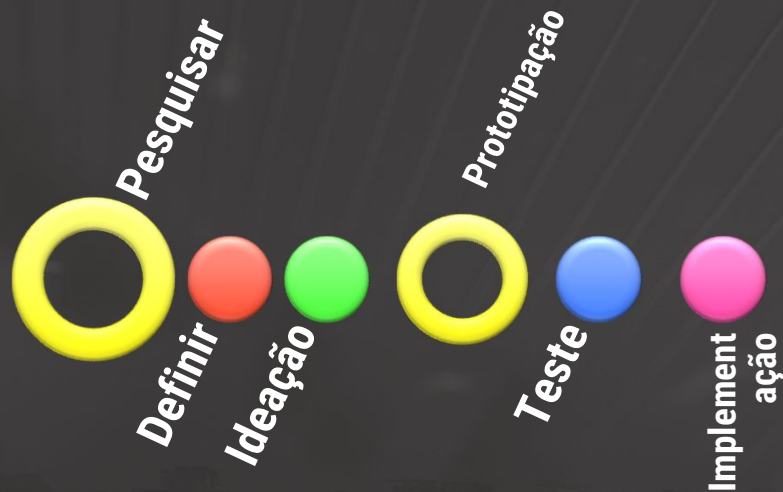
MÉTRICAS USABILIDADE

- VELOCIDADE
- EFICIÊNCIA
- FÁCIL APRENDIZADO (DIDÁTICO)
- FÁCIL MEMORIZAÇÃO
- PREFERÊNCIA DO USUÁRIO

UX METAS E MÉTRICAS

- FÁCIL DE ACHAR
- CREDIBILIDADE
- UTILIDADE
- ACESSIBILIDADE
- DESEJÁVEL: PROVER VALOR AO CLIENTE
- USABILIDADE
- ISO/IEC 9241-210:2019 HCD- ERGONOMIA DE SISTEMA DE INTERAÇÃO HUMANA

Boas Práticas: Relacionamento US, UX e PbD



PERMISSÃO E AUTORIDADE – APLICAR A SEGURANÇA CONFORME O CONTEXTO:

- ✓ 1. Combine a maneira mais confortável de executar tarefas com a menor concessão de autoridade.
- ✓ 2. Conceda autoridade a outras pessoas de acordo com as ações do usuário indicando consentimento.
- ✓ 3. Ofereça ao usuário maneiras de reduzir a autoridade de outras pessoas para acessar os recursos do usuário.
- ✓ 4. Mantenha um conhecimento preciso da autoridade de outras pessoas como relevante para as decisões do usuário.
- ✓ 5. Mantenha um conhecimento preciso da autoridade do usuário para acessar recursos.

Boas Práticas: Relacionamento US, UX e PbD



- ✓ 6. Proteja os canais do usuário a agentes que manipulam autoridade em nome do usuário.
- ✓ 7. Permita que o usuário expresse políticas de segurança seguras em termos adequados à tarefa do usuário.
- ✓ 8. Faça distinções entre objetos e ações ao longo de limites relevantes para a tarefa.
- ✓ 9. Apresente objetos e ações usando aparências distinguíveis e verdadeiras.
- ✓ 10. Indique claramente as consequências das decisões que se espera que o usuário tome.

Boas Práticas: DATA PROTECTION BY DEFAULT

PRIVACY AND DATA PROTECTION



Adotar uma abordagem de "PRIVACY FIRST" com todas as configurações padrão de sistemas e aplicativos;

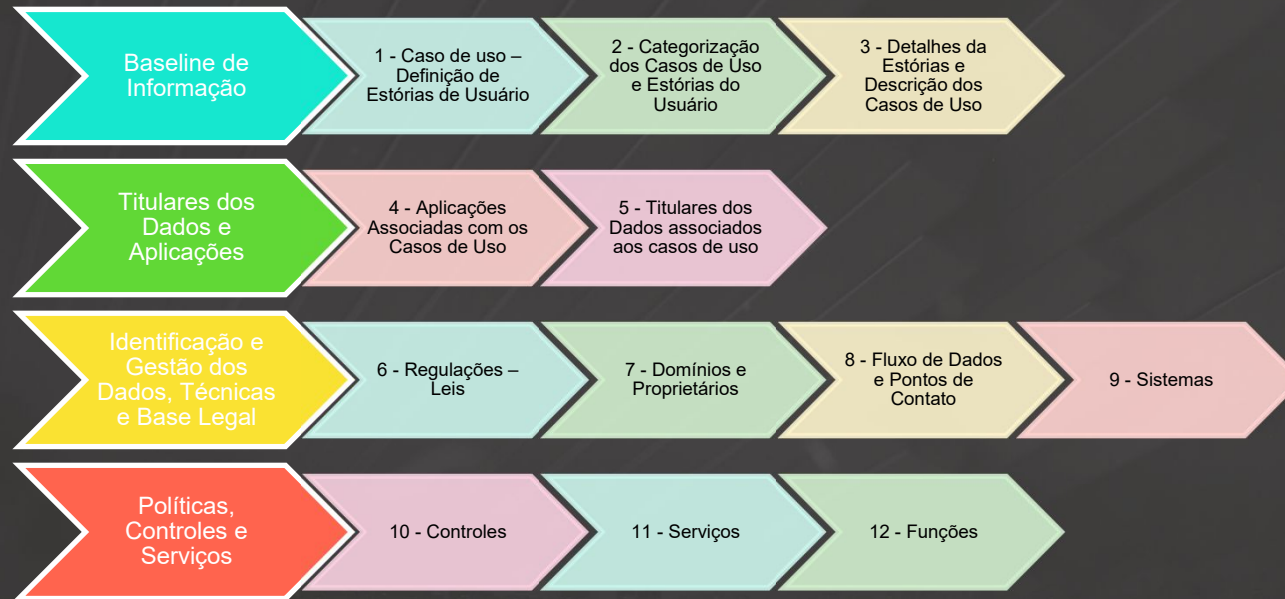
Garantir que você não forneça uma opção ilusória para as pessoas relacionadas aos dados que você processará;

Não processe dados adicionais, a menos que o Titular decida que você pode;

Garantir que os dados pessoais não sejam automaticamente disponibilizados ao público ou terceiros, a menos que o Titular decida fazê-lo; e

Forneça às pessoas controles e opções suficientes para exercer seus direitos.

Boas Práticas: Passos para o Privacy by Design



Referências: Sites livros Artigos

AGNER LUIZ – “Ergodesign e Arquitetura da Informação”. 3º ed. 2012.SENAC RJ.
KA-PING YEE. Artigo: “Guidelines and Strategies for SecureInteractionDesign”. Cap.30 pag 253 -280, 2005
<https://rebit.org.in/whitepaper/usable-security-identity-and-authentication>
<https://www.youtube.com/watch?v=DM8iYTBPVhQ>
<https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf>
<http://giftpicis.pw/Fail-4-Plumbing-Humor-or-should-we-say-quotpotty-humor-t.html>
<https://twitter.com/kasimerkan/status/630892630629613568>
<https://www.interaction-design.org/literature/article/an-introduction-to-usability>
<https://usabilla.com/blog/10-best-ux-infographics-2/>
<http://userexperienceproject.blogspot.com/2007/04/user-experience-wheel.html>
<http://www.gdprtoons.com/2017/10/gdpr-will-impact-many-us-businesses-by.html>
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>
<https://securitycommunity.tcs.com/infosecsoapbox/articles/2018/07/02/gdpr-and-privacy-management-are-you-gdpr-compliant>
<https://blog.minitab.com/blog/what-is-user-centered-design-and-why-is-it-important>
<https://pbd.cs.kau.se/courses/24/pages/oasis-privacy-management-privacy-by-design-for-software-engineering>
<https://www.anywherexchange.com/2017/12/azure-information-protection-end-user.html>

PERGUNTAS

mindthesec[®]
/SÃO PAULO

AGRADECIMENTO

monteiromartins@bol.com.br

@Ale_TI

