Você Está Preparado para o GDPR?

Antonio Plais

Antonio Plais

- Analista de negócios, arquiteto de negócios, professional certificado TOGAF 9.1 e ArchiMate 3
- Mais de 40 anos de experiência em TI, marketing, desenvolvimento de produtos e negócios
- Professor experiente e palestrante internacional
- Membro do Fórum ArchiMate do The Open Group

Sobre a Centus Consultoria

Arquitetura Corporativa

Gerenciamento de Decisões

Análise de Negócios

BiZZdesign

The Open Group Member

SAPIENS DECISION

THE DECISION MODEL

DECISION MANAGEMENT SOLUTIONS

IIBA International Institute of Business Analysis

BiZZdesign é uma empresa de software que suporta as organizações no **Desenho e Realização de Mudanças nos Negócios**

Isenção de responsabilidade: Este não é um aconselhamento jurídico

Todos os diagramas nesta apresentação foram modelados usando a extensão de Segurança, Risco e Conformidade da linguagem ArchiMate®, através da ferramenta BiZZdesign Enterprise Studio

Mensagem de Hoje

- O GDPR está chegando, e é melhor você prestar atenção!
  - Uma regulamentação rigorosa e abrangente sobre a proteção de dados
- Arquitetos podem desempenhar um papel fundamental para assegurar a conformidade
  - Aproveite a sua arquitetura de forma eficaz
- Analise e melhore a proteção de dados usando modelos de arquitetura
  - Suportado pela linguagem ArchiMate

O que é o GDPR?

Um monstro ameaçador…

O que é o GDPR?

- **Regulamento Geral sobre Proteção de Dados**: Regulamento rigoroso da UE (com poder de lei) sobre proteção da privacidade
- Entrará em vigor em 25 de Maio de 2018
- Se aplica a todas as organizações que operam na União Européia ou processam dados de residentes da UE, e não apenas aquelas localizados na UE → muitas **empresas americanas e estrangeiras, incluindo brasileiras**!
- **Multas de até 20 milhões de Euros ou 4% da receita anual a nível mundial**

O que são Dados Pessoais?

- *"Qualquer informação relativa a uma pessoa natural identificada ou identificável ('sujeito de dados'); uma pessoa natural identificável é uma que possa ser identificada, direta ou indiretamente, em particular através de referência a um identificador como nome, número de identificação, dados de localização, identificador on-line, ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social desta pessoa natural"*
- Desta forma, configurar um cookie ou armazenar um endereço IP de um visitante da UE já pode tornar você responsabilizável...

Princípios-chave do GDPR

1. Legalidade, equidade e transparência
2. Limitação da finalidade
3. Minimização de dados
4. Precisão
5. Limitação de armazenamento
6. Integridade e confidencialidade
7. Responsabilização

Requisitos do GDPR (1)

- Você é **sempre responsável**, mesmo se tiver terceirizado o processamento de dados
- **Proteção de dados por desenho e por padrão** para assegurar a confidencialidade, integridade, disponibilidade e resiliência
- Ter um processo para **testar, apreciar e avaliar** regularmente as medidas técnicas e organizacionais
- Designar um **Responsável pela Proteção de Dados**
- **Demonstrar** a conformidade!

Requisitos do GDPR (2)

- **Manter o controle** de todos os dados pessoais que você armazene e de todas as suas atividades de processamento, incluindo a **finalidade** deste processamento, **localização** dos dados, **terceiros** que os recebem
- Nenhum processamento ou perfilamento, sem **permissão explícita** do sujeito (salvo em condições aplicáveis específicas)
  - e não é permitido enterrar o consentimento no fundo de EULAs ou amarrá-lo desnecessariamente ao uso de serviços
- **Remover dados pessoais** a pedido do sujeito

Requisitos do GDPR (3)

- Realizar **avaliações de impacto na proteção de dados** para abordar os riscos aos **direitos e liberdades** das pessoas antes de implementar novos sistemas
- Para a tomada de decisões e perfilamento automatizados, fornecer "**informações significativas** sobre a lógica envolvida"
- **Reportar uma quebra** de segurança para as autoridades e as pessoas afetadas num prazo de 72 horas

O Papel dos Arquitetos

Como a Arquitetura Pode Ajudar a Assegurar a Conformidade

Por que a Arquitetura é a Chave

- Você precisa de uma visão geral ampla do uso de dados pessoais
  - Por que razão foi coletada, como ela é processada, quem tem acesso, onde é armazenada, que terceiros estão envolvidos, que ameaças internas e externas existem...
- A arquitetura é a **principal fonte** de informações
- **Segurança por desenho** é essencial para um estado futuro seguro e conforme

Passos a Dar (1)

1. **Colabore** com colegas para atender à conformidade
   - Trabalhe com seu DPO, CISO, CRO e assessoria jurídica
2. **Reúna** um 'inventário de privacidade':
   - **Classifique** todos os seus dados e avalie se eles se qualificam como pessoais
   - Descreva a **finalidade** para a qual foram coletados; você tem o consentimento do sujeito para usá-los?
   - Preste especial atenção às **categorias especiais de dados pessoais** (por exemplo, relacionados à saúde, biometria, política, religião, etnia). Seu uso só é permitido em circunstâncias muito específicas!

Passos a Dar (2)

3. **Analise** o uso de dados pessoais
   - Comece com áreas de alto risco e os dados mais sensíveis
   - Modele **fluxos de dados**: quais aplicativos, processos, pessoas e partes usam este dados, em quais locais, para qual finalidade?
4. **Avalie** os riscos para os dados confidenciais
   - Onde você está vulnerável? O que poderia dar errado?
5. **Defina** os controles e medidas mitigadoras
   - Use padrões como ISO/IEC 27001 como base

Passos a Dar (3)

6. **Priorize** os riscos, atribua orçamentos e planeje as mudanças
   - Avalie o custo das medidas versus o risco (perda esperada)
   - Integre com o seu portfólio e roteiros de projetos/mudanças
7. **Implemente** e **teste** medidas e controles
   - Evidentemente, isso é o mais importante!
8. **Demonstre** a conformidade!

E, naturalmente, **atualize** regularmente tudo isso!

Análise e Controle

Usando Modelos de Arquitetura para Mitigar Riscos e Garantir a Conformidade

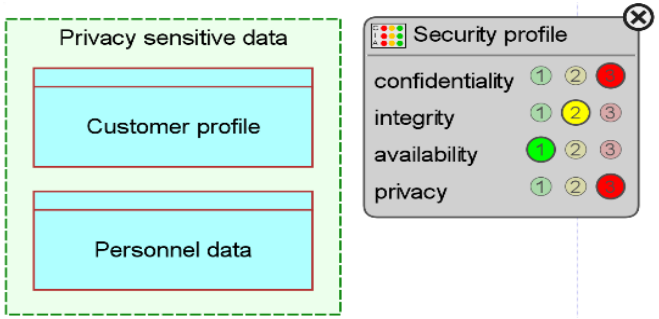
Analise e Mitigue os Riscos

- **Sistematicamente analise** ameaças e vulnerabilidades
- Desenvolva **medidas mitigadoras** em conformidade com a classificação de segurança dos dados
- No caso de sua segurança ser violada, **avalie rapidamente** o impacto potencial e tome as contramedidas adequadas
- Ativamente, **demonstre a conformidade** para os reguladores

Processo de Gerenciamento de Riscos Incorporado

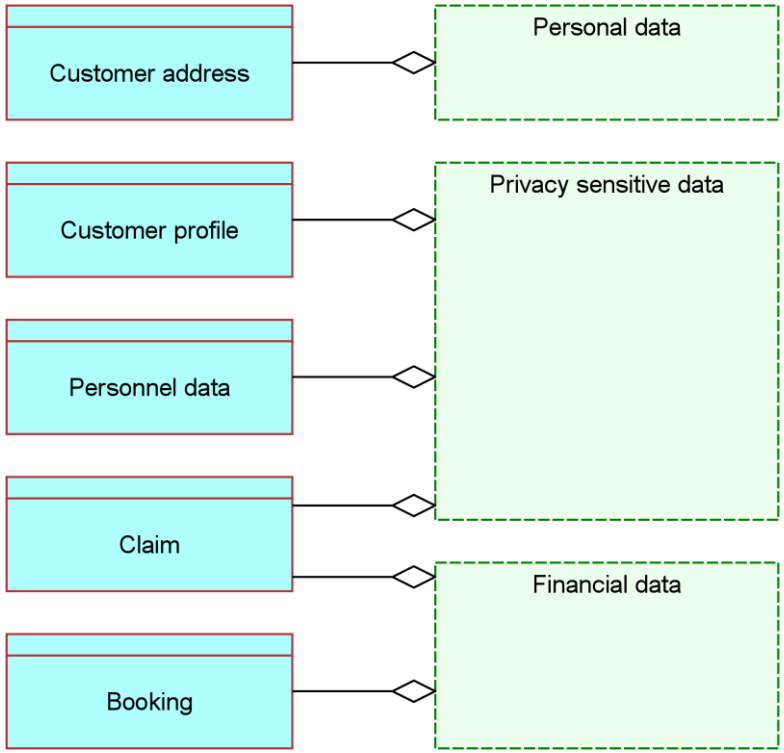
Com base em padrões internacionais como Open FAIR e ArchiMate

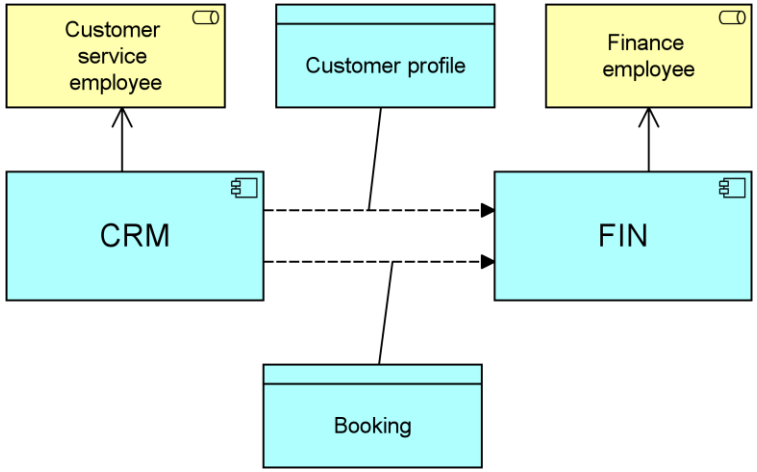
Use Modelos de Arquitetura



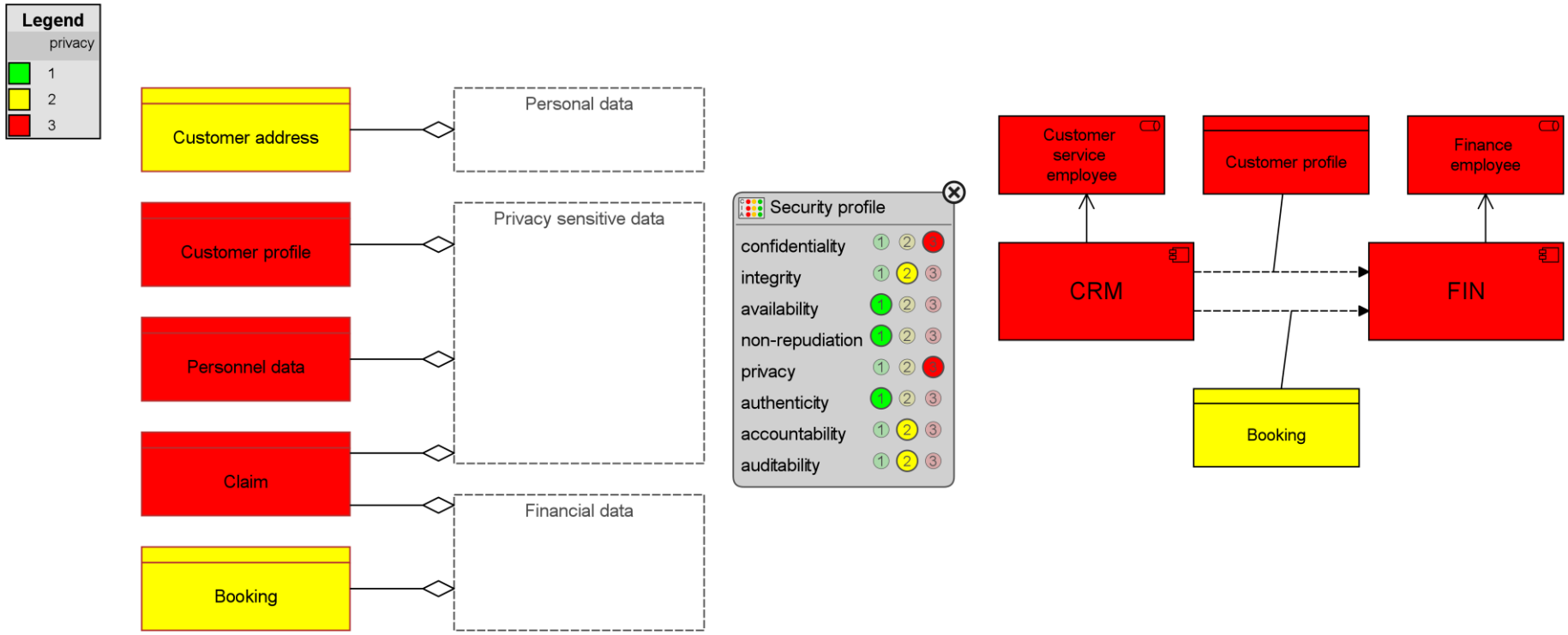
- **Classifique seus dados** com atributos de segurança e privacidade relevantes
- Use modelos de arquitetura para mostrar o **fluxo, locais** e **processamento** de dados pessoais através do panorama corporativo e de TI, e com terceiros
- Modele a finalidade de utilização para avaliar a **proporcionalidade** do uso de dados por organizações, aplicativos e indivíduos

Modelo de Arquitetura de Fluxos e Dados



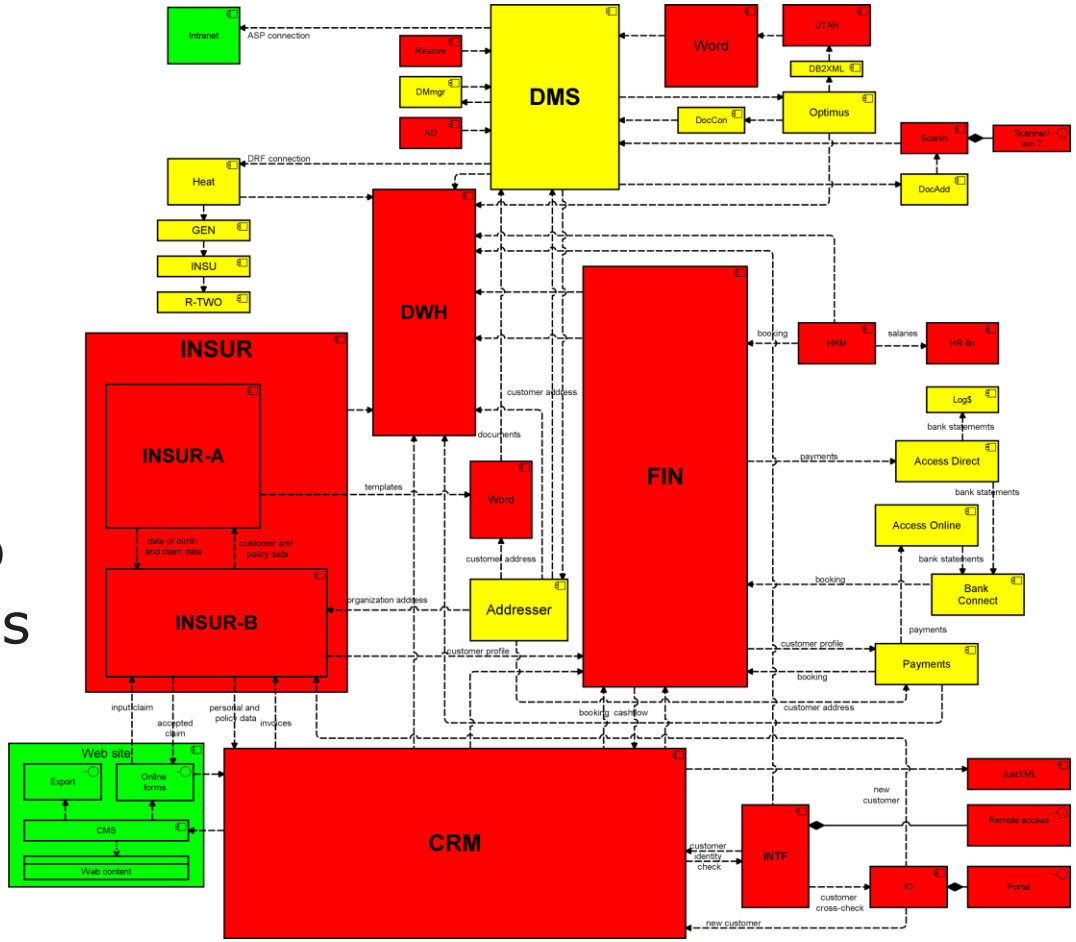


Modelo de Arquitetura de Fluxos e Dados

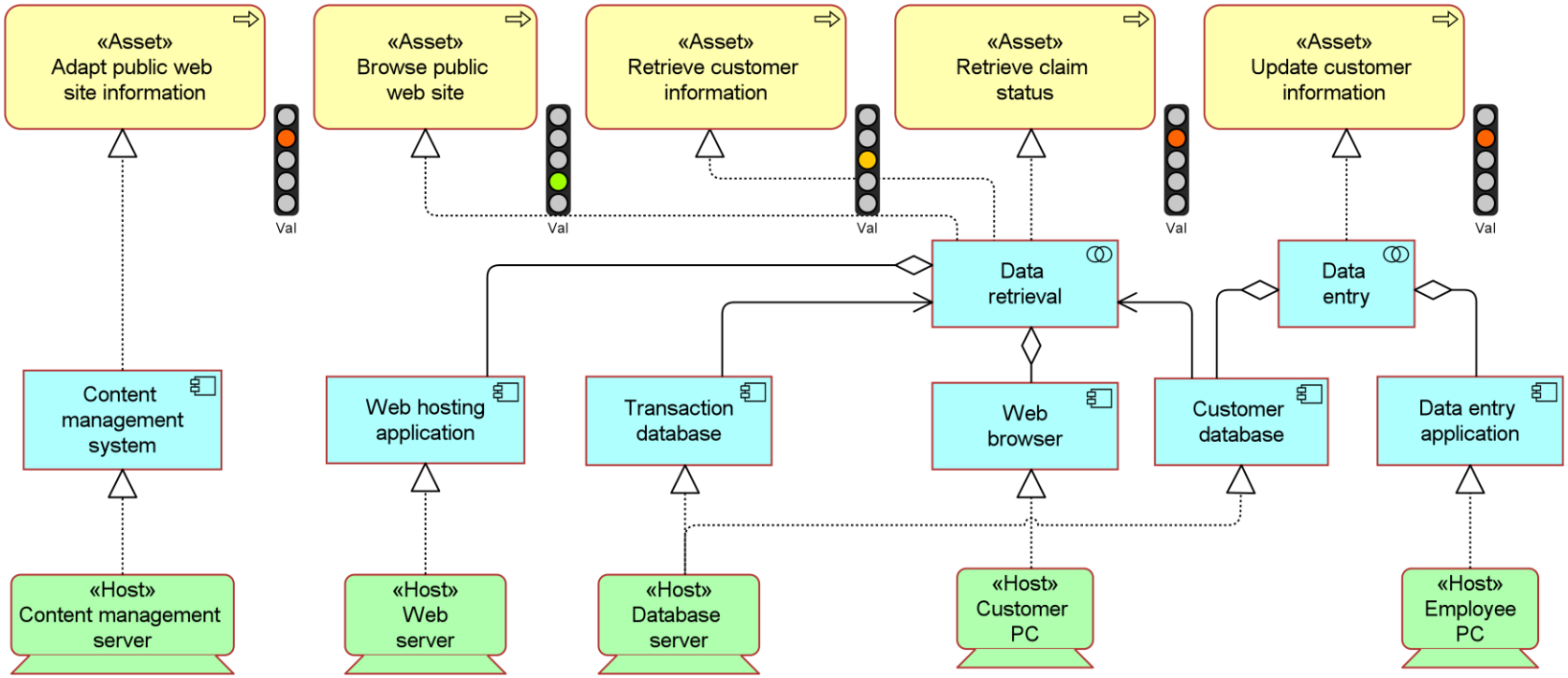


Mapa de Calor do Panorama

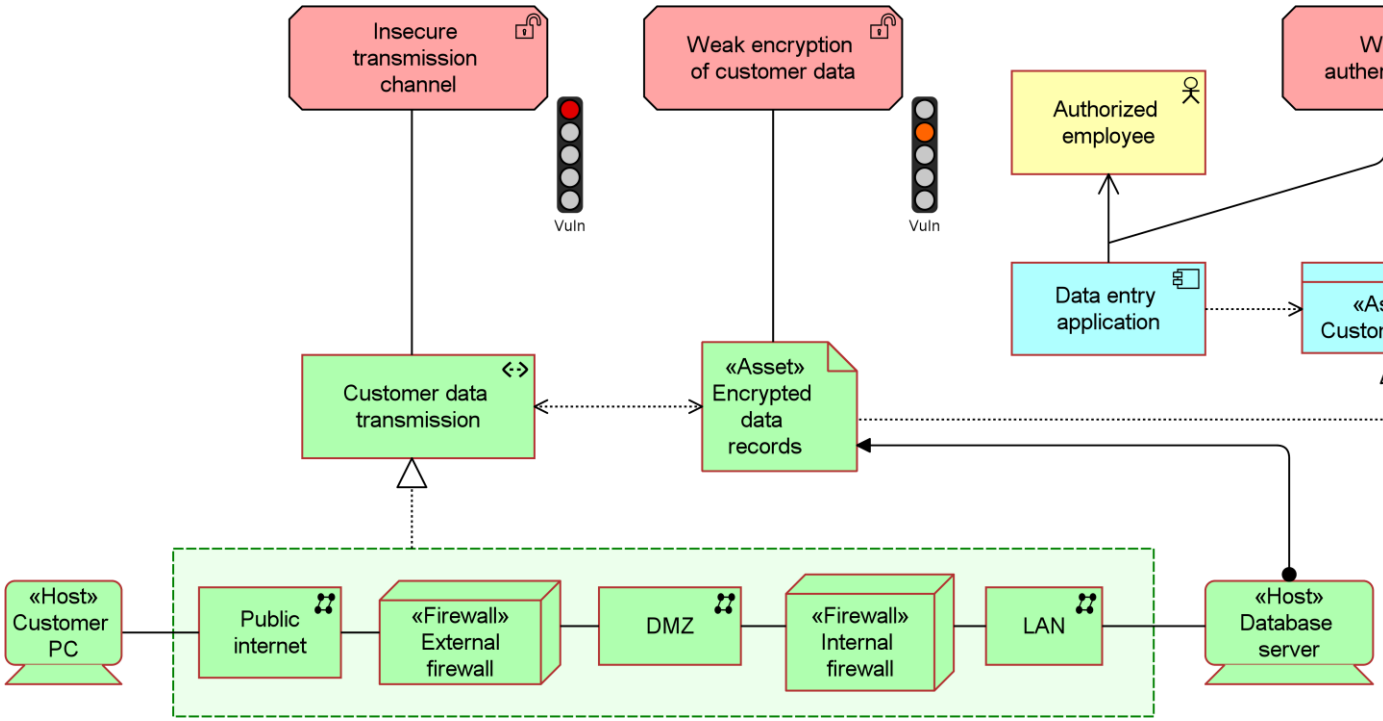
- Aplicativos coloridos conforme o nível de proteção necessário, baseado na classificação de privacidade dos dados que eles usam
- Alta visibilidade proporcionada por uma ferramenta e repositório de arquitetura corporativa



Análises Mais Avançadas

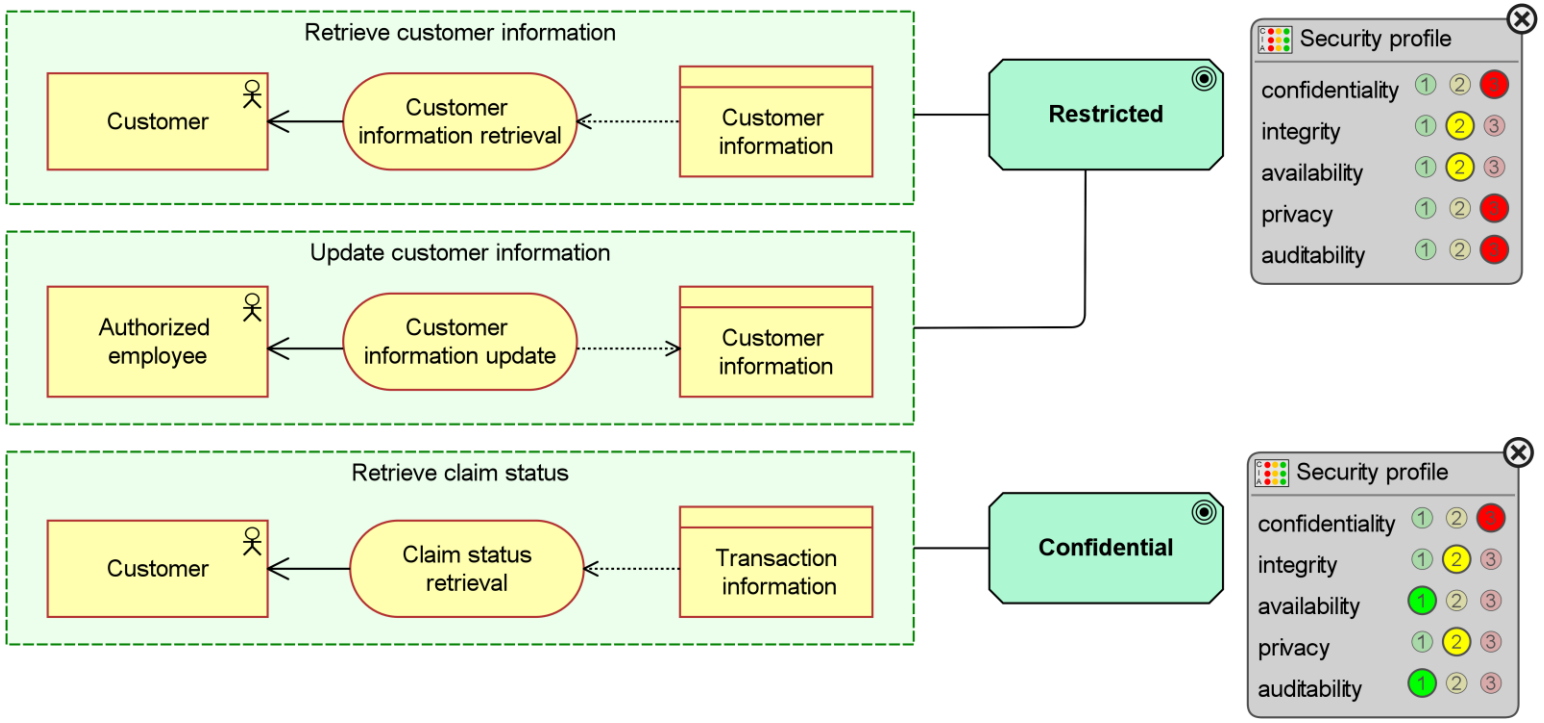


Analise as Vulnerabilidades



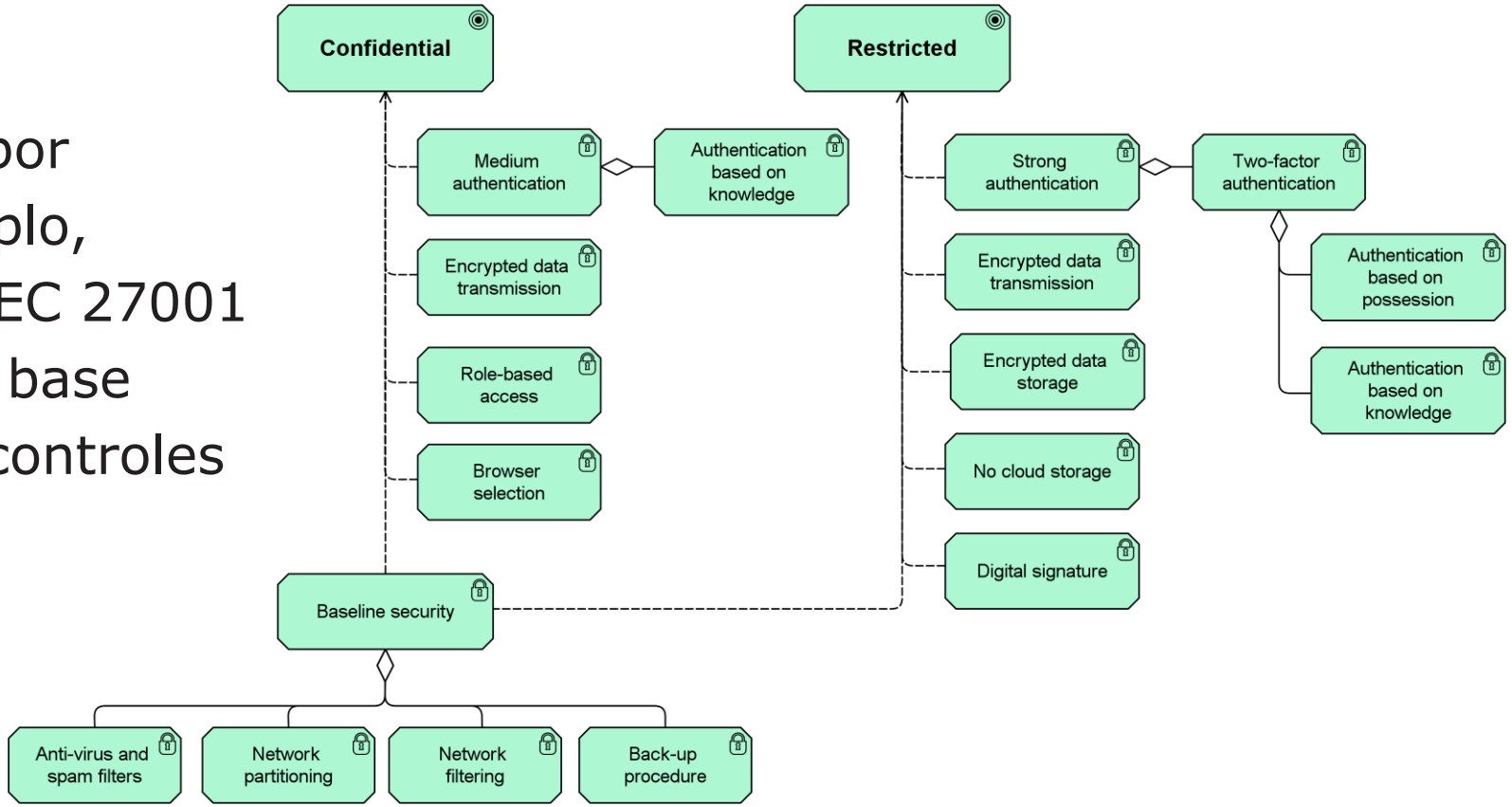
Você pode, também, importar dados a partir de análises externas, por exemplo, testes de penetração

Atribua Perfis de Segurança aos Ativos

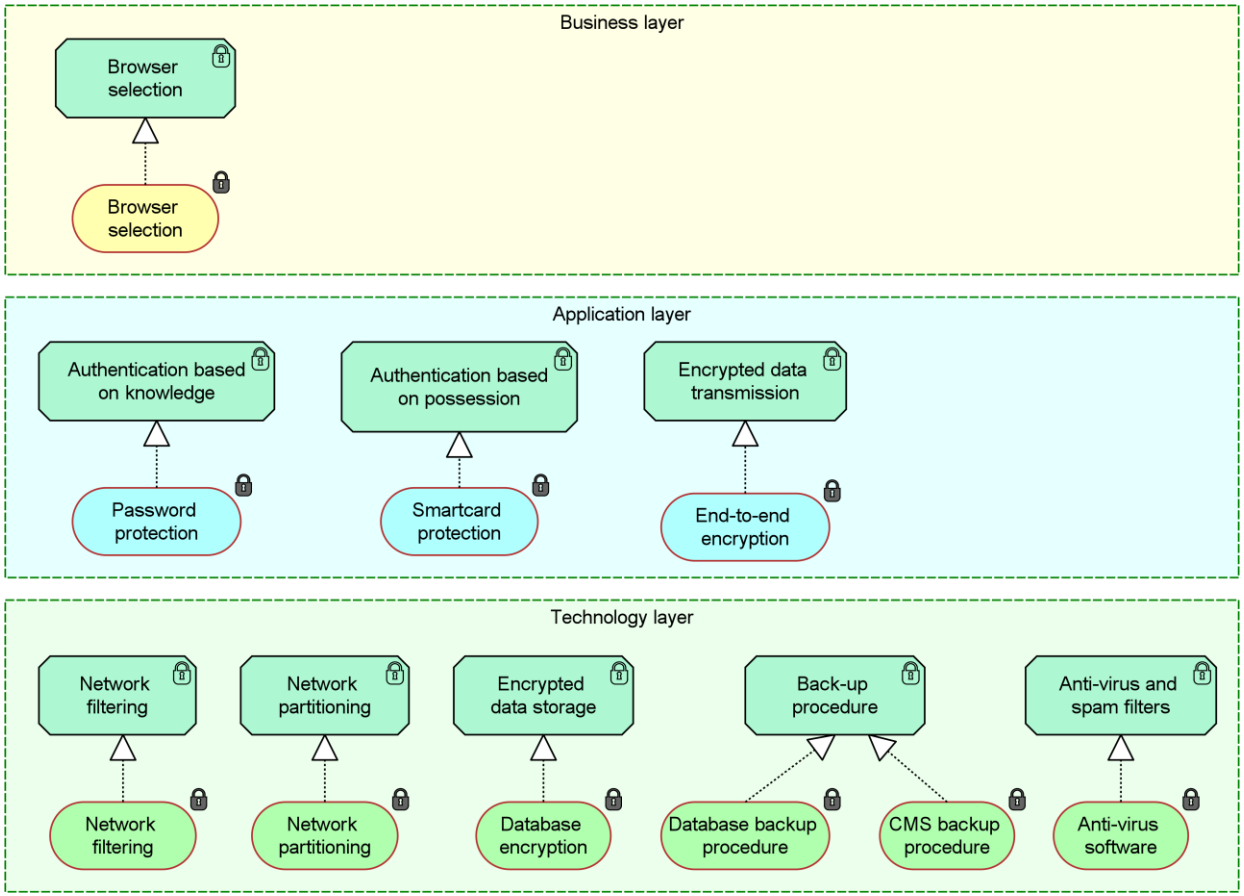


Defina as Medidas de Controle

Use, por exemplo, ISO/IEC 27001 como base para controles

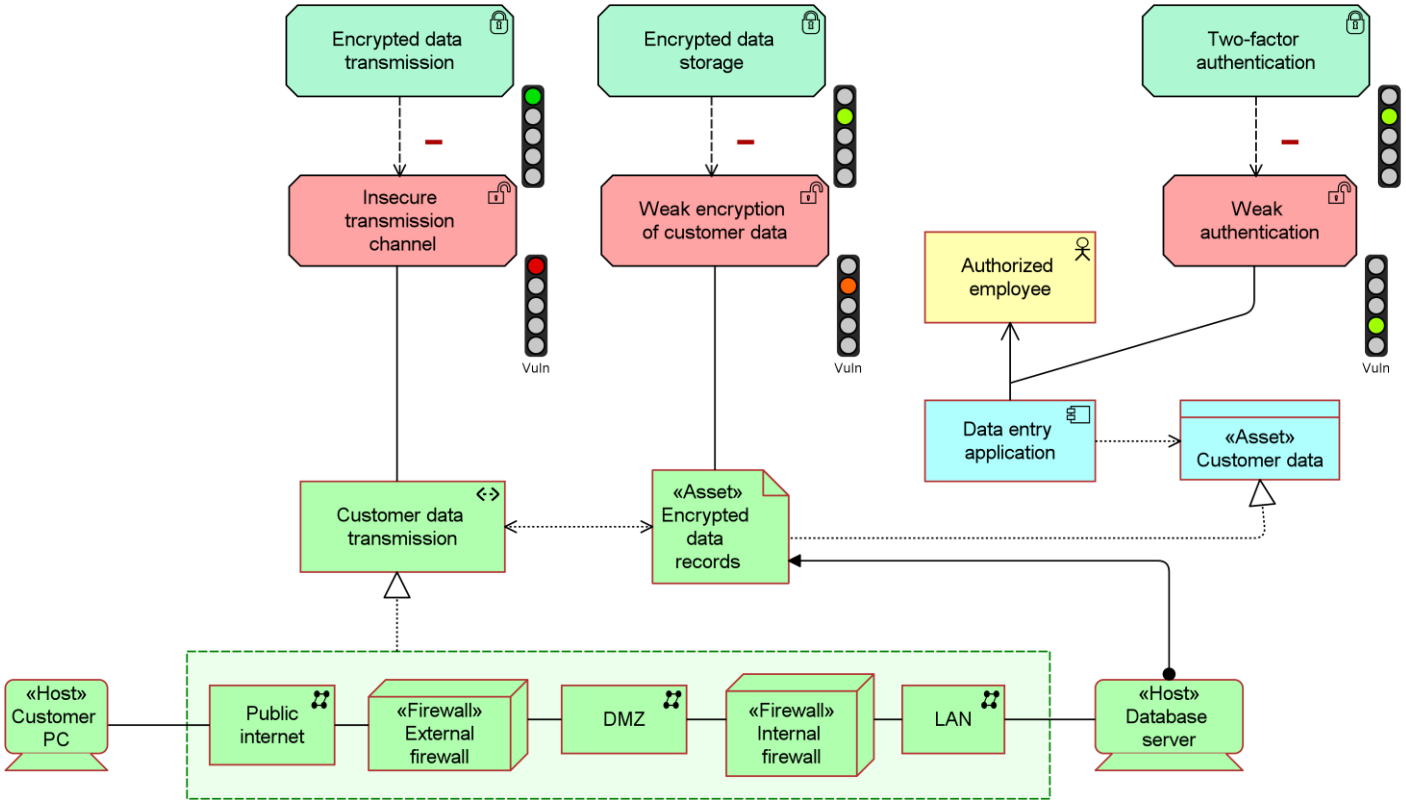


Realize as Medidas de Controle

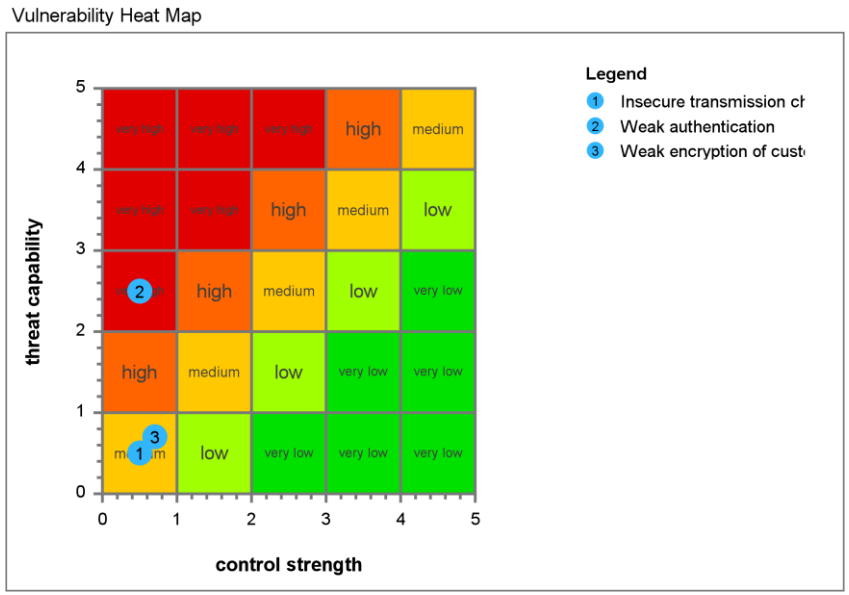


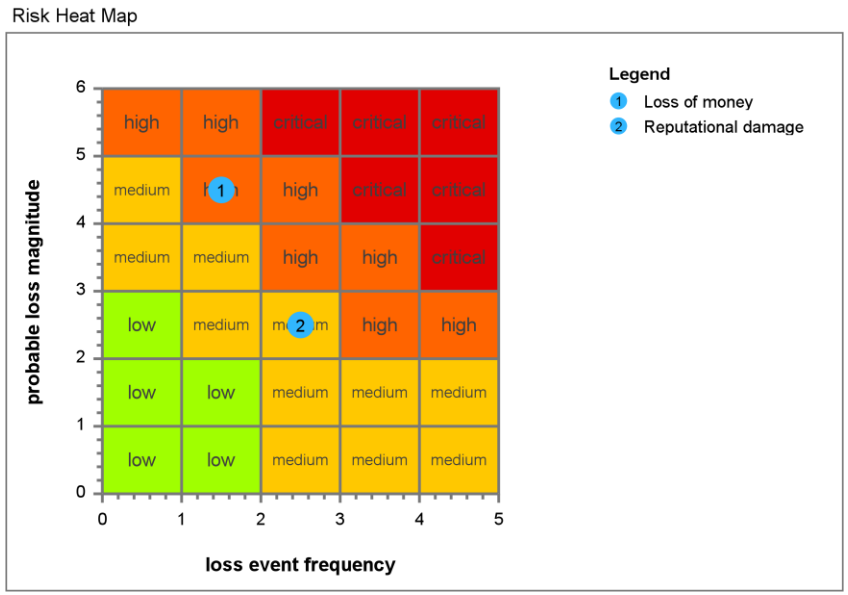
Como você deve realizar as medidas de controle definidas na etapa anterior?

Avalie o Efeito das Medidas de Controle



Mapas de Calor Fornecem Percepções



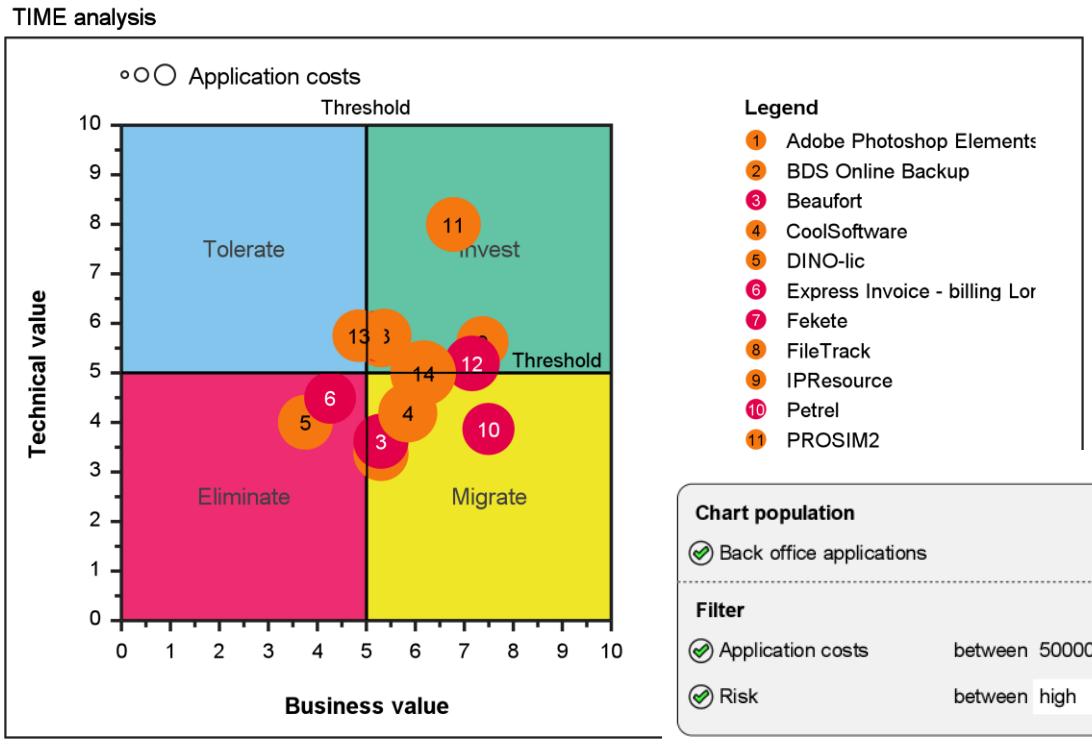


- Quais são as minhas vulnerabilidades mais críticas?
- O que devo fazer sobre isso?

Apóie as Decisões da Gerência

- Crie **painéis de controle** para suportar a visualização de risco e conformidade, priorizar os problemas e definir as medidas apropriadas
- Use funcionalidade de gerenciamento de portfólios para ajudar você a **decidir sobre investimentos** em segurança
- Ligue estes investimentos com o ciclo de vida e a evolução dos aplicativos, para criar **roteiros integrados**

Destacando Aplicações de Alto Risco



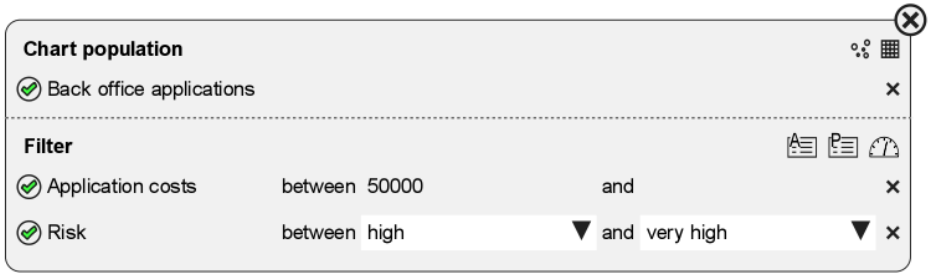


Gráfico do ciclo de vida de aplicativos filtrado para aplicativos de alto custo, alto risco

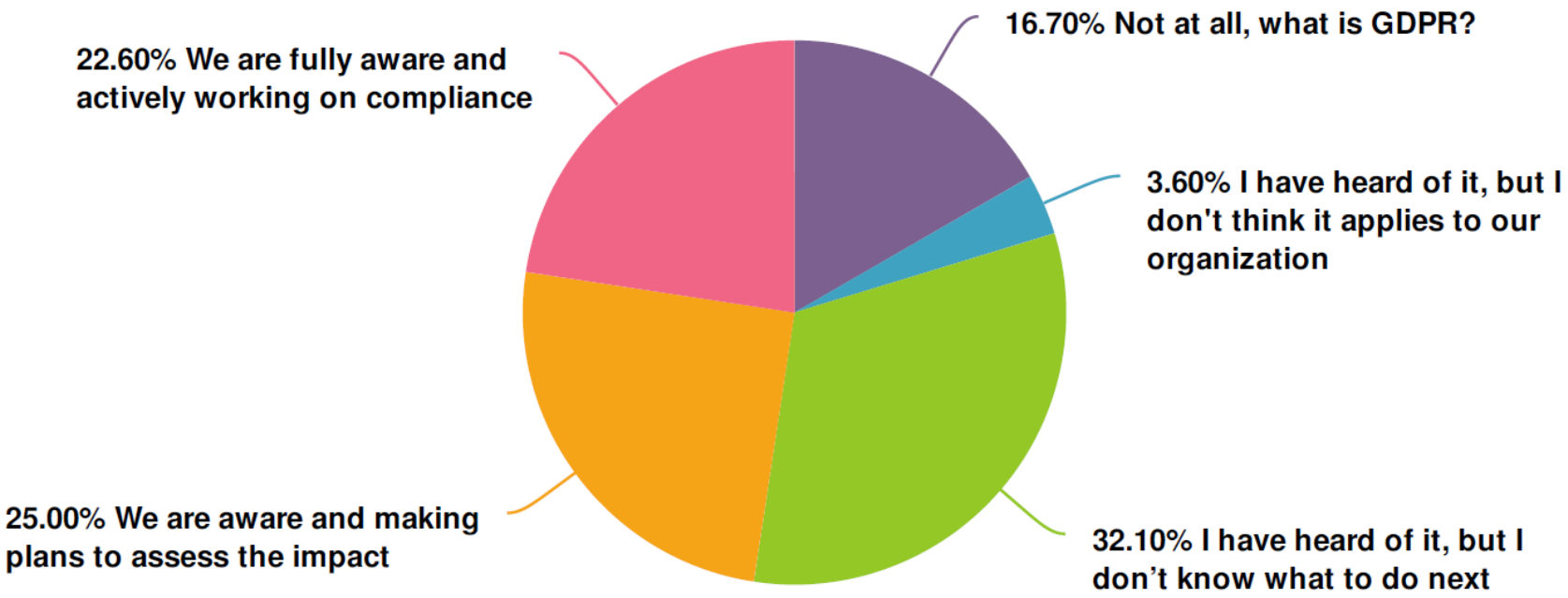
O Que se Segue?

Esteja Preparado a Tempo, Comece Hoje Mesmo!

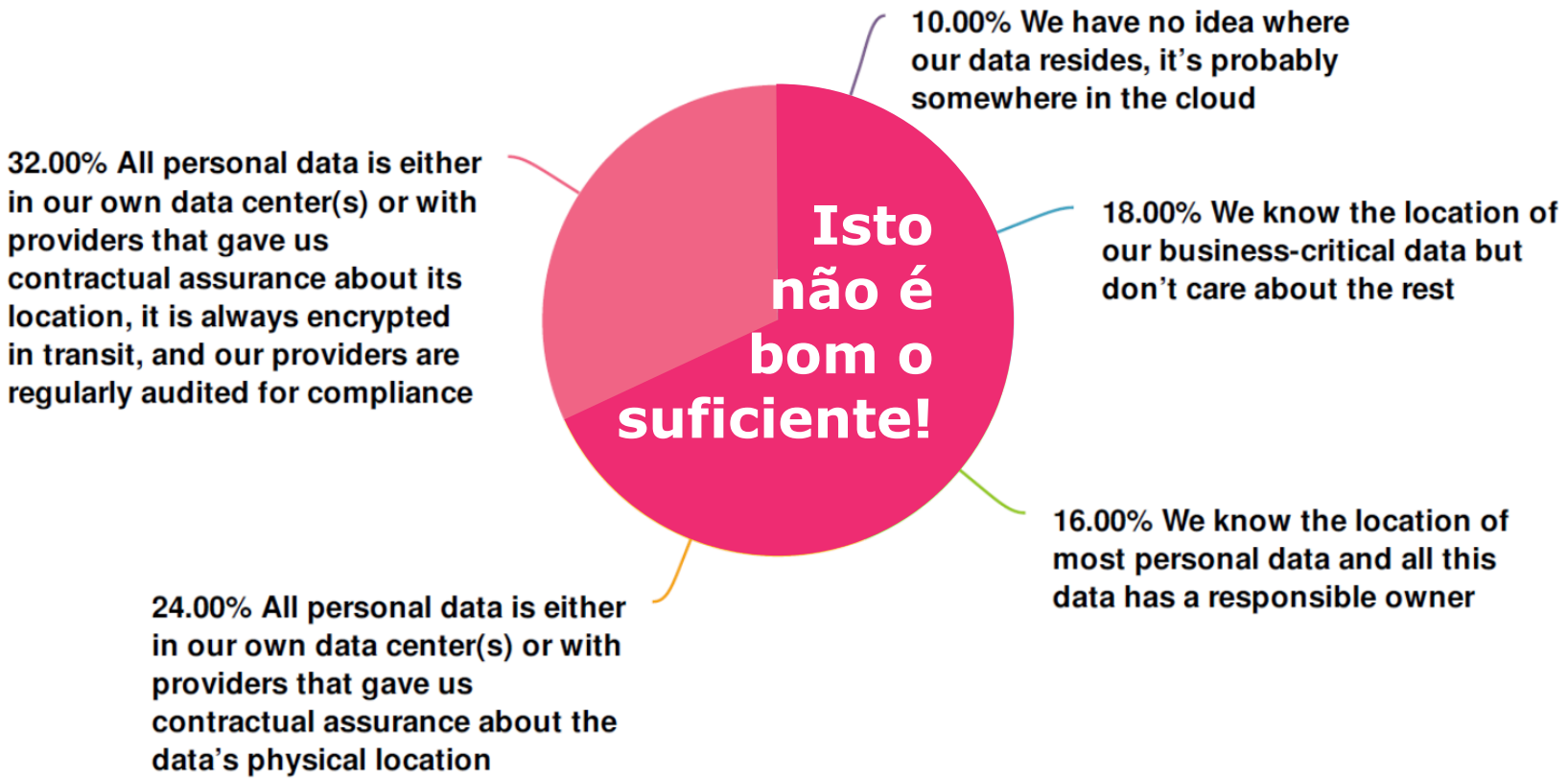
Teste GDPR

- Participe do nosso teste para ver quão pronto para o GDPR você está: http://www.surveygizmo.com/s3/3241516/how-ready-are-you-for-the-GDPR
- Dá a você uma primeira ideia das coisas que você pode precisar pensar a respeito
- Os resultados agregados estão disponíveis através de nosso blog, fique atento

"Você está ciente do GDPR?"



"Você conhece a localização de seus dados?"



Próximos Passos

- **Comece agora**: Monte uma equipe, avalie o que você precisa fazer e vá em frente
- Maio de 2018 está mais perto do que você imagina, e você pode precisar fazer um monte de trabalho
- Bom suporte de ferramenta é essencial, você não pode fazer isso nas costas de um guardanapo
- **A Centus-BiZZdesign está aqui para ajudar você!**

Como a BiZZdesign Suporta Você

- **Conteúdo** pré-preenchido o para o GDPR, tais como:
  - Exemplo de ameaças e riscos
  - Medidas de controle, por exemplo, com base no padrão ISO/IEC 27001
  - Análises aplicáveis
- **Consultoria** empacotada
  - Ajuda com o que você precisa para modelar, e como fazer isso
  - Ajuda a configurar as análises de risco e definir as medidas mitigadoras corretas

Benefícios da Solução BiZZdesign

- Pro-ativamente engajar os riscos de segurança e privacidade com uma **abordagem de segurança por desenho**
- **Aproveitar os modelos existentes** para a análise de risco
- Investir em segurança **onde ela é importante**
- Assegurar e **demonstrar a conformidade**
- Evitar pesadas multas e a perda de reputação…

E Finalmente Algumas Sugestões…

- O texto do GDPR: eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT
- Nosso teste GDPR: www.surveygizmo.com/s3/3241516/how-ready-are-you-for-the-GDPR
- Modeling Enterprise Risk Management and Security with the ArchiMate Language https://www2.opengroup.org/ogsys/catalog/W172
- An Introduction to the Open FAIR Body of Knowledge https://www2.opengroup.org/ogsys/catalog/W148

Antonio Plais

+55 31 99279-0290

antonioplais@centus.com.br

br.linkedin.com/in/antonioplais/pt

www.centus.com.br

centus
consultoria e negócios

BiZZdesign