**Template da Etapa 3 – Projeto Fundamentos de Sistemas.**

**Equipe:**

*Breno Cordeiro*

*João Vitor Kuhn Kampff*

*Giovana*

*Pedro*

*Rayssa*

**ITEM 1 - Construir um modelo de sistema de informação (no formato de um quadro) que atenda ao processo escolhido no item 1 da etapa 2 apresentando ameaças/vulnerabilidades e proposta de solução.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Processo** | **Descrição do Processo** | **Ameaças e Vulnerabilidades** | **Soluções Propostas** | **Controles de Segurança** |
| Acolhimento do Cliente | Primeiro contato do cliente com o Service Desk. | Interceptação de dados, phishing, negação de serviço. | Sistema de autenticação forte, criptografia de dados, monitoramento de tráfego. | Autenticação de dois fatores, firewalls, IDS/IPS. |
| Classificação e Encaminhamento | Classificação da solicitação e encaminhamento para o setor responsável. | Erro de classificação, perda de dados, acesso não autorizado. | Sistema de classificação automatizada, controle de acesso baseado em perfis. | Log de auditoria, controle de acesso granular. |
| Resolução da Solicitação | Análise, diagnóstico e resolução da solicitação. | Acesso não autorizado a dados do cliente, demora na resolução, erros de configuração. | Controle de acesso aos sistemas, monitoramento de desempenho, gestão de incidentes. | PSI bem elaborada, SLAs, monitoramento proativo. |
| Fechamento da Solicitação | Confirmação da resolução com o cliente e encerramento do ticket. | Satisfação do cliente baixa, reabertura desnecessária. | Pesquisa de satisfação, sistema de feedback, autoatendimento. | KPIs de satisfação do cliente, gestão de conhecimento. |

**ITEM 2 - Definir *Hardware* de servidor completo para atender ao modelo de sistema de informação construído no item 1, justificando cada escolha e mostrando o CAPEX e OPEX.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Componente | Especificação | Qtd. | Justificativa | CAPEX (R$) | OPEX (Mensal, R$) |
| Servidor | Dell PowerEdge R650, Intel Xeon Gold 6330, 128GB RAM, 2x4TB SSD + 4x10TB HDD | 3 | Para suportar até 500 usuários simultâneos e um grande volume de dados. | R$50.000,00 cada | R$ 500,00~ (manutenção, cada) |
| Armazena-mento | RAID 10 com SSDs para sistema operacional e banco de dados, RAID 6 com HDDs para dados | 1 | Alta performance e redundância para os dados críticos. | R$30.000,00 | R$ 200,00~ (energia) |
| Rede | Cisco Catalyst 3850, Cisco ASA 5510 | 1 de cada | Switches gerenciados para alta disponibilidade e firewall para segurança. | R$20.000,00 | R$ 100,00~  (manutenção) |
| UPS | APC Smart-UPS SRT 1500VA | 2 | Para garantir a continuidade do serviço por até 15 minutos em caso de falha na energia. | R$5.000,00 cada | R$ 100,00 ~  (energia) |
| Software | CentOS 8, PostgreSQL, VMware vSphere | 1 de cada | Sistema operacional estável, banco de dados relacional e plataforma de virtualização. | R$10.000,00 | R$ 120,00~  (licenças) |

**ITEM 3 - Para este item a equipe terá de desenvolver um Script em C# que deverá ser entregue em um arquivo compactado com esse documento. Este script terá um menu com três opções de inventário do computador:**

* 1. ***Hardware***
  2. ***Software***
  3. ***Hardware e Software***

**Descrição dos fluxos escolhidos para análise e tratamento de riscos.**

### **Fluxo Informacional Atual (Rota Principal)**

Na maioria dos sistemas de **service desk**, o fluxo típico dos dados de usuários e incidentes segue os passos abaixo, incluindo vulnerabilidades e riscos:

1. **Coleta de Dados**:
   * **Fonte:** Formulários de incidentes, integração com sistemas de CRM ou relatórios diretos.
   * **Vulnerabilidades:** Entrada de dados não validada, exposições acidentais.
   * **Riscos:** Injeção de dados maliciosos, exposição de informações confidenciais.
2. **Processamento no Sistema Central**:
   * **Fonte:** Base de dados centralizada no servidor do service desk.
   * **Vulnerabilidades:** Configuração incorreta do banco de dados, permissões mal gerenciadas.
   * **Riscos:** Vazamento de dados, ataques cibernéticos ao banco.
3. **Distribuição e Tratamento**:
   * **Fonte:** Usuários internos (analistas de suporte, gerentes) acessam dados para resolver incidentes.
   * **Vulnerabilidades:** Controle de acesso fraco, senhas reutilizadas.
   * **Riscos:** Acesso não autorizado, erro humano.
4. **Notificação e Resolução**:
   * **Fonte:** Feedback enviado ao usuário final via e-mail, mensagens instantâneas ou notificações.
   * **Vulnerabilidades:** Comunicação sem criptografia, phishing.
   * **Riscos:** Interceptação de dados, manipulação de mensagens.

### **Rota Alternativa para o Fluxo de Informações**

A rota alternativa proposta se concentra em minimizar as vulnerabilidades da rota principal ao utilizar tecnologias adicionais, segmentação de informações e processos mais seguros:

#### **1. Coleta Segura e Descentralizada**

* **Estratégia:** Utilizar sistemas de coleta descentralizados (como formulários preenchidos em dispositivos seguros ou APIs com validação no frontend).
* **Implementação:**
  + Validação automática dos dados no frontend (ex: formato de e-mail, sanitização de inputs).
  + Dados coletados criptografados já no ponto de entrada (ex: TLS/SSL).
* **Benefício:** Reduz o risco de dados maliciosos atingirem o servidor principal.

#### **2. Processamento com Segmentação de Dados**

* **Estratégia:** Dividir os dados em repositórios separados com permissões específicas para diferentes equipes.
  + Informações críticas, como PII (informação pessoal identificável), ficam em um sistema isolado.
  + Dados não críticos (ex: descrição do problema) são acessíveis em um ambiente diferente.
* **Implementação:**
  + Aplicar políticas de zero-trust: cada camada do sistema precisa autenticar e autorizar acessos.
  + Usar contêineres para rodar módulos de processamento (ex: Docker ou Kubernetes) e proteger o banco.
* **Benefício:** Limita o impacto de ataques, mesmo que uma parte do sistema seja comprometida.

#### **3. Distribuição com Tokenização**

* **Estratégia:** Distribuir dados para os analistas de suporte usando tokens temporários em vez de acesso direto ao banco de dados.
* **Implementação:**
  + Os dados sensíveis são mascarados ou omitidos por padrão.
  + Tokens expiram automaticamente após o uso ou em um tempo limitado.
* **Benefício:** Acesso controlado e rastreável, reduzindo riscos de acesso indevido.

#### **4. Comunicação Protegida**

* **Estratégia:** Substituir canais vulneráveis por ferramentas mais seguras, como plataformas integradas de mensagens criptografadas.
* **Implementação:**
  + Notificações e e-mails enviados via protocolo seguro (SMTP com TLS).
  + Adicionar autenticação no destinatário final (ex: link temporário para visualizar informações).
* **Benefício:** Protege contra interceptação de dados e reduz o risco de phishing.

**ITEM 4 - Realizar uma análise de riscos/continuidade/contingência dos itens de segurança física e lógica encontrados no item 5 da etapa 2.**

### **1. Base de Dados de Clientes**

* **Ameaça:** Vazamento de dados.
* **Vulnerabilidades:** Configuração incorreta do banco de dados, acesso não autorizado.
* **Riscos:** Alta probabilidade de comprometimento da confidencialidade dos dados dos clientes, resultando em sanções legais, danos à reputação e perdas financeiras.

**Medidas de Mitigação:**

* Implementar políticas de acesso baseadas em função (RBAC).
* Configurar corretamente o banco de dados com criptografia em trânsito e em repouso.
* Realizar auditorias regulares de permissões e acessos.

**Plano de Contingência:**

Manter backups criptografados e segregados, com testes regulares de restauração. Implementar notificações automáticas de acessos não autorizados.

### **2. Sistemas de CRM**

* **Ameaça:** Ataque cibernético, perda de dados.
* **Vulnerabilidades:** Vulnerabilidades em software, falta de atualização.
* **Riscos:** Interrupção das operações de venda e atendimento ao cliente, possível exposição de dados sensíveis.

**Medidas de Mitigação:**

* Atualizar o software regularmente e aplicar patches de segurança.
* Utilizar firewalls e sistemas de prevenção de intrusões (IPS).
* Implementar autenticação multifator (MFA) para todos os usuários.

**Plano de Contingência:**

Ter um sistema redundante configurado (DRaaS) e um plano de comunicação para informar os clientes em caso de falha.

### **3. Canais de Comunicação (e-mail, chat)**

* **Ameaça:** Interceptação de comunicações, phishing.
* **Vulnerabilidades:** Configuração de rede inadequada, falta de criptografia.
* **Riscos:** Comprometimento da privacidade das comunicações, ataques direcionados (spear phishing).

**Medidas de Mitigação:**

* Implementar criptografia de ponta a ponta (E2EE).
* Treinar os funcionários para identificar phishing e adotar práticas de segurança.
* Usar SPF, DKIM e DMARC para proteger contra falsificação de e-mails.

**Plano de Contingência:**

Preparar respostas automatizadas e provisórias para incidentes de phishing e configurar mecanismos de bloqueio rápido de contas comprometidas.

### **4. Dispositivos Móveis (smartphones, tablets)**

* **Ameaça:** Perda ou roubo, malware.
* **Vulnerabilidades:** Senhas fracas, aplicativos não confiáveis.
* **Riscos:** Exposição de dados corporativos e controle remoto não autorizado dos dispositivos.

**Medidas de Mitigação:**

* Aplicar políticas de gestão de dispositivos móveis (MDM).
* Exigir autenticação biométrica e senhas fortes.
* Restringir a instalação de aplicativos de terceiros.

**Plano de Contingência:**

Configurar a capacidade de apagar remotamente os dispositivos comprometidos e manter backups regulares dos dados críticos.

### **5. Redes Wi-Fi Públicas**

* **Ameaça:** Ataques de man-in-the-middle, interceptação de dados.
* **Vulnerabilidades:** Senhas fracas, ausência de criptografia.
* **Riscos:** Roubo de credenciais, exposição de dados sensíveis, monitoramento não autorizado do tráfego.

**Medidas de Mitigação:**

* Proibir o uso de redes públicas para acesso a sistemas sensíveis.
* Implementar VPN para conexões externas.
* Utilizar WPA3 em todas as redes Wi-Fi internas.

**Plano de Contingência:**

Suspender conexões potencialmente comprometidas e investigar acessos irregulares.

### **6. Lojas Físicas**

* **Ameaça:** Acesso não autorizado, roubo de equipamentos.
* **Vulnerabilidades:** Controles de acesso insuficientes, câmeras de segurança inoperantes.
* **Riscos:** Perda de equipamentos, comprometimento físico de dados armazenados localmente.

**Medidas de Mitigação:**

* Instalar sistemas de controle de acesso físico com logs de entrada e saída.
* Garantir funcionamento contínuo das câmeras de segurança.
* Restringir áreas críticas com crachás biométricos.

**Plano de Contingência:**

Implementar planos de recuperação para danos físicos, como reposição rápida de equipamentos e sistemas.

### **7. Documentos Impressos**

* **Ameaça:** Perda ou roubo, acesso não autorizado.
* **Vulnerabilidades:** Armazenamento inadequado, falta de controle de acesso.
* **Riscos:** Vazamento de informações confidenciais, uso indevido de dados impressos.

**Medidas de Mitigação:**

* Armazenar documentos em locais seguros, como armários trancados.
* Implementar uma política de "mesa limpa" para documentos sensíveis.
* Adotar processos de descarte seguro, como fragmentação de papel.

**Plano de Contingência:**

Registrar documentos importantes em cópias digitais e armazenar em sistemas protegidos.

Ver o artigo “4 opções de mitigação no tratamento de riscos de acordo com a ISO 27001” em

<https://advisera.com/27001academy/pt-br/blog/2016/05/19/4-opcoes-de-mitigacao-no-tratamento-de-riscos-de-acordo-com-iso-27001/>