|  |  |  |
| --- | --- | --- |
| Descrição: Descrição: cabecalho2009_logo | Descrição: Descrição: cabecalho2009_linha1 | |
| Desenvolvimento Etapa 2 – Projeto Fundamentos de Sistemas. | |
| Descrição: Descrição: cabecalho2009_linha2 | |
|  |  |
|  |  |

## Escolher 1 processo de negócio entre os que foram identificados na etapa 1 e detalhá-lo usando uma ferramenta de construção de fluxograma.

https://miro.com/welcomeonboard/MkRmK2hpRHNNb2N1bVM0ZERoYWdqL0ZVbnBJSzh2OVBEUnlLWVNXRWc2SHFCVVBxeDhnazNUandQWFdCdXEvdm5VQkY1Q3A2MFc1ak1pdnZNVFVBemVYRTgwWkN6VllWL0Y0VFB1NHl1bmJPcEgzckZ0RG9iOVJmMWNabExGd0QhZQ==?share\_link\_id=133120212243

## Identificar os componentes suscetíveis a eventos de segurança da informação que fazem parte do processo de negócio escolhido vistos no MF de Fundamentos de Segurança.

### **Bases de Dados de Clientes**

**Riscos:**   
Vazamento de dados pessoais, fraudes, espionagem industrial, perda de dados, falha na rotina de backup.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Classificação de risco | **Falha no backup** | **Espionagem** | **Perda de dados** | **Vazamento de dados** | **Fraudes** |
| A - Ação imediata | A | A | A | A | A |
| B - Ação média e a curto prazo | B | B | B | B | B |
| C – Monitoramento e gestão | C | C | C | C | C |
| D – Risco controlável | D | D | D | D | D |

**Componentes vulneráveis:**

Servidores de banco de dados, aplicativos de gestão de clientes (CRM), interfaces de programação de aplicativos (APIs).

### **Canais de Atendimento ao Cliente**

**Riscos:**

Interceptação de comunicações, phishing, ataques DDoS , transferência indevida de dados pessoais.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Classificação de risco | **Interceptação de comunicações** | **Ataques DDoS** | **Phishing** | **Transferência indevida de dados** |
| A - Ação imediata | A | A | A | A |
| B - Ação média e a curto prazo | B | B | B | B |
| C – Monitoramento e gestão | C | C | C | C |
| D – Risco controlável | D | D | D | D |

**Componentes vulneráveis:**

Plataformas de chat, e-mail, telefone, aplicativos móveis, portais de autoatendimento.

### **Sistemas de Autenticação e Autorização**

**Riscos:**

Acesso não autorizado, sequestro de sessão, ataques de força bruta.

|  |  |  |  |
| --- | --- | --- | --- |
| Classificação de risco | **Ataques de força bruta** | **Acesso não autorizado** | **Sequestro de sessão** |
| A - Ação imediata | A | A | A |
| B - Ação média e a curto prazo | B | B | B |
| C – Monitoramento e gestão | C | C | C |
| D – Risco controlável | D | D | D |

**Componentes vulneráveis:**

Servidores de autenticação, mecanismos de autenticação (senhas, tokens), firewalls.

### **Redes de Comunicação**

**Riscos:**

Interceptação de dados, ataques de homem no meio, perda de dados.

|  |  |  |  |
| --- | --- | --- | --- |
| Classificação de risco | **Perda de dados** | **Interceptação de dados** | **Ataque de homem no meio** |
| A - Ação imediata | A | A | A |
| B - Ação média e a curto prazo | B | B | B |
| C – Monitoramento e gestão | C | C | C |
| D – Risco controlável | D | D | D |

**Componentes vulneráveis:** Roteadores, switches, firewalls, VPNs, Wi-Fi.

### **Aplicativos de Gestão de Serviços**

**Riscos:** Injeção de SQL, cross-site scripting (XSS), falhas de autenticação.

|  |  |  |  |
| --- | --- | --- | --- |
| Classificação de risco | **Injeção de SQL** | **Cross-site scripting (XSS)** | **Falha de autenticação** |
| A - Ação imediata | A | A | A |
| B - Ação média e a curto prazo | B | B | B |
| C – Monitoramento e gestão | C | C | C |
| D – Risco controlável | D | D | D |

**Componentes vulneráveis:** Portais de gestão, sistemas de billing e plataformas de suporte técnico.

### **Dispositivos de Rede dos Clientes**

**Riscos:** Botnets, ataques de negação de serviço e espionagem.

|  |  |  |  |
| --- | --- | --- | --- |
| Classificação de risco | **Espionagem** | **Botnets** | **Ataques de negação de serviço** |
| A - Ação imediata | A | A | A |
| B - Ação média e a curto prazo | B | B | B |
| C – Monitoramento e gestão | C | C | C |
| D – Risco controlável | D | D | D |

**Componentes vulneráveis:**

Modems, roteadores, dispositivos IoT.

### **Parceiros de Negócios**

**Riscos:** Vazamento de dados, ataques à cadeia de suprimentos.

|  |  |  |
| --- | --- | --- |
| Classificação de risco | **Ataques à cadeia de suprimentos** | **Vazamento de dados** |
| A - Ação imediata | A | A |
| B - Ação média e a curto prazo | B | B |
| C – Monitoramento e gestão | C | C |
| D – Risco controlável | D | D |

**Componentes vulneráveis:**

Interfaces de troca de dados, sistemas dos parceiros.

## Mapear itens relacionados à TI invisível na organização.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Setor | Item de TI não catalogado | Proprietário | Usuários | Risco | Obs. |
| Vendas | Armazenamento em nuvem pessoal | João Silva | Toda a equipe de vendas | Perda de dados, falta de controle de acesso | Utilizado para armazenar arquivos de clientes |
| Marketing | Aplicativo de colaboração não aprovado | Ana Souza | Equipe de marketing | Vazamento de dados confidenciais, não conformidade com a política de segurança | Utilizado para compartilhar informações estratégicas |
| Operação | Dispositivo IoT não registrado | Equipe de produção | Operadores de rede | Vulnerabilidades de segurança, interferência em processos críticos | Utilizado para monitoramento de conexões |

Recomenda-se a leitura da NBR ISO/IEC27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação (2019).

## Identificar dispositivos pessoais utilizados na organização.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Setor | Dispositivo | Proprietário | Usuários | Risco | Obs. |
| Atendimento ao Cliente | Smartphone pessoal | Atendente João Silva | João Silva | Vazamento de dados de clientes, infecção por malware | Utilizado para acessar sistemas internos e dados de clientes |
| Suporte Técnico | Notebook pessoal | Técnico Maria Santos | Maria Santos | Instalação de software não autorizado, acesso remoto não seguro | Utilizado para acessar sistemas internos e realizar diagnósticos remotos |
| Vendas | Tablet pessoal | Vendedor Pedro Almeida | Pedro Almeida | Perda de dados de clientes, acesso a redes não seguras | Utilizado para apresentar produtos e coletar assinaturas |
| Marketing | Pendrive | Analista de Marketing Ana Oliveira | Equipe de Marketing | Introdução de malware, perda de dados de campanhas | Utilizado para transportar arquivos de campanhas |
| Desenvolvimento | Raspberry Pi | Desenvolvedor Carlos Pereira | Carlos Pereira | Ataques a sistemas internos, desenvolvimento de aplicações não autorizadas | Utilizado para testes e prototipagem |

Recomenda-se assistir o seguinte conteúdo do MF: Legislação em TI.

Unidade 2: Tema 4.

Recomenda-se a leitura da NBR ISO/IEC27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação (2019).

## Identificar riscos de segurança física e lógica discutidos no MF de Fundamentos de Segurança da Informação e encontrados no contexto organizacional estudado.

|  |  |  |
| --- | --- | --- |
| Ativo | Ameaça | Vulnerabilidade |
| Base de dados de clientes | Vazamento de dados | Configuração incorreta do banco de dados, acesso não autorizado |
| Sistemas de CRM | Ataque cibernético, perda de dados | Vulnerabilidades em software, falta de atualização |
| Canais de comunicação (e-mail, chat) | Interceptação de comunicações, phishing | Configuração de rede inadequada, falta de criptografia |
| Dispositivos móveis (smartphones, tablets) | Perda ou roubo, malware | Senhas fracas, aplicativos não confiáveis |
| Redes Wi-Fi públicas | Ataques de man-in-the-middle, interceptação de dados | Senhas fracas, ausência de criptografia |
| Lojas físicas | Acesso não autorizado, roubo de equipamentos | Controles de acesso insuficientes, câmeras de segurança inoperantes |
| Documentos impressos | Perda ou roubo, acesso não autorizado | Armazenamento inadequado, falta de controle de acesso |

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

### **Política de Segurança da Informação**

PSI-001-2024

Versão 1.0

Classificação: Interna

Última revisão: 03/11/2024

1. Introdução ............................................................................................................................... 6

1.1. Objetivo ............................................................................................................................ 6

1.2. Escopo .............................................................................................................................. 7

1. Princípios de Segurança .......................................................................................................... 7  
   2.1. Segurança da informação................................................................................................. 7

2.2. Confidencialidade ............................................................................................................ 7

2.3. Integridade ...................................................................................................................... 8

2.4. Disponibilidade ................................................................................................................ 8

1. Glossário ................................................................................................................................. X
2. Gerenciamento de Acesso ...................................................................................................... X

3.1. Gerenciamento de Acesso ............................................................................................... X

3.2. Autenticação .................................................................................................................... X

3.3. Autorização ...................................................................................................................... X

1. Segurança Física e Ambiental ................................................................................................. X

5.1. Proteção de Instalações ...................................................................................................X

5.2. Controle de Acesso Físico ................................................................................................ X

5.3. Segurança Ambiental ....................................................................................................... X

1. Segurança de Redes e Comunicações ..................................................................................... X

6.1. Proteção de Redes ........................................................................................................... X

6.2. Monitoramento e detecção de intrusões ........................................................................ X

1. Gestão de Incidentes de Segurança ........................................................................................ X

7.1. Resposta a Incidentes ...................................................................................................... X

7.2. Relatórios de Incidentes .................................................................................................. X

1. Conscientização e Treinamento em Segurança ...................................................................... X

8.1. Programa de Conscientização .......................................................................................... X

8.2. Treinamento em Segurança ............................................................................................. X

1. Avaliação e Melhoria Contínua ............................................................................................... X

9.1. Auditorias de Segurança .................................................................................................. X

9.2. Revisão de Políticas e Procedimentos ............................................................................. X

9.3. Análise de Riscos ............................................................................................................. X

9.4. Medição de Desempenho ............................................................................................... X

1. Conformidade Legal e Regulatória ......................................................................................... X

10.1. Conformidade com Leis e Regulamentações ................................................................ X

10.2. Gerenciamento de Vulnerabilidades e Patches ............................................................ X

1. Responsabilidades ................................................................................................................. X

11.1. Direção .......................................................................................................................... X

11.2. Equipe de Segurança da Informação ............................................................................ X

11.3. Funcionários ................................................................................................................. X

### **1.0. Introdução**

### **1.1. Objetivo da Política de Segurança da Informação**

### Estabelecer diretrizes que permitam aos colaboradores, associados, clientes e prestadores de serviços da ConectaTel seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa, das informações e do indivíduo. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da ConectaTel quanto à:

● Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

● Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

● Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, com as devidas autorizações.

### **1.2. Escopo da Política de Segurança da Informação**

Esta Política se aplica a todos os ativos de informação da ConectaTel, incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações da Conectatel. Esta política se aplica em todas as instalações físicas administradas ou utilizadas pela ConectaTel e entidades subsidiárias. Estrategicamente, esta política se aplica a todos executivos, diretores e acionistas da ConectaTel, isso é, aqueles responsáveis pelos planos de longo prazo da empresa com acesso a informações confidenciais financeiras, administrativas e operacionais. Taticamente, esta política se aplica a todos os gestores, gerentes e supervisores da ConectaTel responsáveis pelo gerenciamento e supervisão dos atendentes em nível operacional, dado que os mesmos possuem acesso direto a ativos confidenciais de clientes e funcionários da ConectaTel. Em nível operacional, esta política afeta a todos os funcionários de responsáveis pelo atendimento direto ao cliente, sejam eles atendentes de telemarketing, vendedores, estagiários ou jovens aprendizes, dado que na execução diária do exercício da profissão estes funcionários lidam com informações sensíveis e confidenciais de clientes, sejam essas informações novas sendo adicionadas ao sistema ou informações já salvas. Além disso, cabe notar que esta política não é válida para nenhum dos clientes que fazem uso dos serviços oferecidos pela ConectaTel, dado que os mesmos não têm acesso por definição aos ativos de segurança que a ConectaTel possui. É também necessário destacar que é obrigação de cada colaborador manter-se atualizado em relação à PSI e aos procedimentos e normas relacionadas, buscando ajuda do Departamento de Tecnologia da Informação caso não esteja totalmente seguro quanto à aquisição, uso ou descarte das informações.

### **2.0. Princípios de segurança**

### **1.1. Segurança da informação**

Definida como a proteção da informação de vários tipos de ameaça para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio.  
  
  
**1.2. Confidencialidade**

O princípio da confidencialidade determina que certa informação, fonte ou sistema deve estar acessível apenas a pessoas autorizadas. Caso um indivíduo não autorizado acesse, intencionalmente ou não, uma informação sigilosa, haverá quebra de confidencialidade.

**1.3. Integridade**  
  
  
 O princípio da integridade estabelece que certa informação deve ser correta, confiável e sem alterações não autorizadas. Ou seja, os dados devem permanecer intocados, por meio de precauções para que eles não sejam modificados ou eliminados sem autorização, para preservar sua confiabilidade e originalidade. Se isso não ocorrer, as informações podem ser interpretadas erroneamente, gerando rupturas no compliance do negócio e, em algumas situações, sanções relevantes.  
  
  
**1.4. Disponibilidade**  
  
  
 O princípio da disponibilidade determina que a informação deve estar sempre acessível para uso legitimo de pessoas autorizadas. Para garantir essa disponibilidade, e imperativo implementar uma seria de controles e práticas robustas que abordem tanto a prevenção quanto a mitigação de riscos.   
  
  
  
  
**3.0. Glossario**  
  
  
**Colaborador:** Empregado, estagiário ou menor aprendiz da instituição.   
  
**Dados:** Conjunto de fatos, valores ou ocorrências em estado bruto, que, quando processado ou agrupado, produzem informações.