**FACIMP - WYDEN**

Wilton R S Junior

Wallace

Eduardo T. Sousa

Fillype Gabriel

**Plano Básico de Segurança da Informação**

**Imperatriz - MA  
2025**

Wilton R S Junior

Wallace

Eduardo T. Sousa

Fillype Gabriel

**Plano Básico de Segurança da Informação**

Projeto apresentado ao curso de Sistemas de Informação, para a disciplina de Introdução à Segurança da informação, como requisito para obtenção de nota.

**Imperatriz - MA  
2025**

**- Atribuição de papéis:**Wilton R S Junior - **Coordenador / Editor Chefe**

Fillype Gabriel - **Analista de Ameaças e Vulnerabilidade**

Eduardo T. Sousa - **Analista de Boas Práticas e Gestão de Risco**

Wallace - **Analista de Continuidade de Negócios**

**Sumário**

**1. Contexto e Princípios de Segurança da Informação**

1.1 Descrição do cenário

1.2 Inventário básico de recursos de TI

1.3 Princípios CID (Confidencialidade, Integridade, Disponibilidade)

**2. Ameaças, Vulnerabilidades e Normas**

2.1 Mapeamento de ameaças e vulnerabilidades

2.2 Normas, leis e regulamentações aplicáveis

**3. Boas Práticas e Gestão de Risco**

3.1 Boas práticas recomendadas

3.2 Estrutura de mitigação de riscos

**4. Plano de Continuidade de Negócio**

4.1 Processos críticos

4.2 Estratégias de recuperação

4.3 Plano de contingência

**5. Referências**

1. **Contexto e Princípios de Segurança da Informação**

**1.1 Descrição do cenário**

**Nome da Empresa:** Ponto Verde

**Tipo:** Marketplace fictício de comércio eletrônico (e-commerce).

**Descrição:**

O Ponto Verde é um marketplace, uma plataforma online que conecta vendedores e compradores de produtos diversos. A empresa opera nacionalmente, com milhares de transações diárias, e armazena dados sensíveis de usuários, como informações pessoais, dados de pagamento e histórico de compras.

Um marketplace lida com grandes volumes de dados sensíveis, incluindo informações de clientes (nome, endereço, CPF), dados financeiros (cartões de crédito, transações bancárias) e dados de fornecedores (contratos, informações comerciais).

**1.2 Inventário básico de recursos de TI**

Servidores de aplicação: servidores web e de aplicação hospedados em nuvem (ex.: AWS, Azure) e/ou locais, executando o software do marketplace e o sistema de autenticação.

Bancos de dados: repositório relacional de dados (ex.: MySQL) contendo cadastros de usuários, produtos, pedidos e transações financeiras; inclui mecanismos de backup locais e em nuvem.

Rede e segurança: firewalls de perímetro, roteadores e switches gerenciáveis que controlam o tráfego de rede; redes privadas virtuais (VPN) para acesso administrativo remoto seguro; sistemas de detecção e prevenção de intrusão (IDS/IPS).

Sistemas de pagamento: integrações com provedores de pagamento digital (gateway de pagamento) e terminais POS virtuais, para processar transações de cartão de crédito/débito em ambiente seguro.

Serviços de mensagens e comunicação: servidores de e-mail corporativo, chat interno do site e sistema de notificações para intermediar a comunicação entre clientes e vendedores.

Recursos físicos e usuários: estações de trabalho, notebooks e dispositivos móveis dos administradores e funcionários; aplicações de backoffice para atendimento ao cliente e gestão do marketplace; infraestrutura de armazenamento em rede (NAS) e nuvem para arquivos estáticos (imagens de produtos, documentos).

**1.3** **Princípios CID (Confidencialidade, Integridade, Disponibilidade)**

A confidencialidade garante que as informações sejam acessadas apenas por pessoas ou sistemas autorizados

Neste ambiente, isso significa proteger dados de clientes e vendedores contra acessos indevidos ou vazamentos. Ataques do tipo man-in-the-middle (MITM), por exemplo, podem interceptar fluxos de informação e comprometer a confidencialidade dos dados em trânsito

A integridade assegura que os dados sejam mantidos corretos, autênticos e não adulterados. Ou seja, toda transação ou atualização no sistema deve ocorrer de forma controlada, de modo que alterações não autorizadas possam ser detectadas e revertidas. A disponibilidade garante que sistemas e informações estejam acessíveis a usuários autorizados quando necessário

Em um marketplace, a indisponibilidade de servidores web ou de bancos de dados impede a realização de vendas e impacta processos críticos de negócio. Em resumo, a tríade CID constitui os pilares fundamentais da segurança da informação: proteger dados sensíveis de acessos não autorizados, assegurar sua correção e manter os serviços operacionais

**2 Ameaças, Vulnerabilidades e Normas**

**2.1 Mapeamento de ameaças e vulnerabilidades**

No contexto do marketplace online, as principais ameaças incluem ataques cibernéticos direcionados a aplicativos web, infraestruturas de rede e usuários finais. Exemplos de ameaças relevantes são:

* Malwares: software malicioso desenvolvido para comprometer a confidencialidade, integridade e disponibilidade dos dados e sistemas. Ex.: trojans que infectam servidores ou estações de trabalho para roubo de credenciais.
* Ransomwares: variante de malware que sequestra dados (criptografa arquivos) e exige pagamento de resgate para liberação. Pode paralisar serviços críticos do marketplace e forçar a empresa a negociar sob forte pressão.
* Ataques de Negação de Serviço (DoS/DDoS): inundação de tráfego malicioso que sobrecarrega servidores ou rede, tornando o site lento ou totalmente inacessível. Isso pode interromper vendas online e gerar perdas financeiras, além de desviar atenção para outros ataques.
* Phishing e engenharia social: envio de e-mails, mensagens ou sites falsos disfarçados de comunicação confiável para induzir usuários (clientes ou funcionários) a divulgar credenciais ou dados pessoais Estes ataques crescentes visam obter acesso indevido às contas e sistemas.
* Roubo de credenciais e acesso indevido: senhas fracas ou reutilizadas podem ser comprometidas por ataques de força bruta ou por engenharia social. Um invasor que obtenha credenciais administrativas pode manipular dados discretamente.

**2.2 Normas, leis e regulamentações aplicáveis**

O Plano de Segurança da Informação deve seguir normas e legislações relevantes, tanto nacionais quanto internacionais, garantindo proteção de dados e conformidade legal.

* Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)

Regula o tratamento de dados pessoais, visando proteger a privacidade e a liberdade dos indivíduos. Exige consentimento, base legal para uso de dados, e impõe sanções em caso de vazamento. Em um marketplace, a maioria dos dados de clientes e vendedores está sujeita à LGPD.

* ISO/IEC 27001:2022

Norma internacional para Sistemas de Gestão de Segurança da Informação (SGSI). Fornece um modelo para implementar e aprimorar controles técnicos, físicos e organizacionais (como políticas de segurança, controle de acesso e capacitação de pessoal). Segui-la assegura práticas auditáveis e eficazes no marketplace.

* Marco Civil da Internet (Lei nº 12.965/2014)

Define princípios e direitos para o uso da internet no Brasil. Garante privacidade, neutralidade da rede e proteção de dados. O artigo 7º exige consentimento para coleta e divulgação de dados pessoais e restringe o compartilhamento com terceiros, o que reforça a necessidade de políticas de privacidade e registro de atividades dos usuários.

* Decreto nº 7.962/2013 (Lei do E-commerce)

Regulamenta o Código de Defesa do Consumidor no ambiente digital. Obriga a exibição clara de informações sobre produtos, serviços e fornecedores. Também exige confirmação imediata de compras e canais eficientes de atendimento ao cliente, promovendo transparência e confiança nas transações online.

3. Boas Práticas e Gestão de Risco

# 3.1 Boas Práticas Recomendadas

O Analista de Boas Práticas e Gestão de Risco da Ponto Verde propôs a adoção das seguintes políticas, processos e ferramentas com base nas normas ISO 27001, LGPD e boas práticas do setor:

## Políticas e Processos

* + - **Política de Senhas Fortes:** Exigência de senhas complexas, troca periódica e autenticação multifator (MFA).
    - **Política de Backup e Recuperação:** Backups automáticos diários com armazenamento redundante e testes mensais de restauração.
    - **Controle de Acesso:** Privilégios mínimos, com revisões trimestrais dos acessos concedidos.
    - **Política de Atualizações e Patches:** Atualização contínua dos sistemas operacionais, CMS e plugins.
    - **Gestão de Incidentes:** Procedimento documentado para resposta rápida e registro de incidentes de segurança.

## Ferramentas

* + - **Antivírus e EDR (Endpoint Detection and Response):** Monitoramento proativo de endpoints.
    - **Firewall com inspeção profunda (Next-Gen):** Proteção contra ataques em tempo real.
    - **WAF (Web Application Firewall):** Mitigação de ataques como SQL Injection e XSS.
    - **CDN com Mitigação de DDoS:** Proteção contra ataques de negação de serviço.
    - **Sistema de monitoramento (SIEM):** Correlação e alerta sobre eventos suspeitos.

# 3.2 Estrutura de Mitigação de Riscos

O plano de mitigação descreve como tratar cada risco identificado na análise de vulnerabilidades. A tabela abaixo resume os principais riscos e suas respectivas medidas de controle:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risco** | **Impacto** | **Probabilidade** | **Classificação** | **Ação de Mitigação** |
| **Vazamento de dados de clientes** | Alto | Médio | Alto | Criptografia de dados sensíveis, política de acesso restrito, monitoramento de  logs. |
| **Ataques DDoS ao site** | Alto | Alto | Crítico | Contratação de CDN com mitigação DDoS, redundância  de servidores. |
| **Phishing e engenharia social** | Médio | Alto | Alto | Treinamentos periódicos, simulações de phishing, políticas  de conscientização. |
| **Malware nos dispositivos administrativo s** | Alto | Médio | Alto | Antivírus/EDR atualizados, proibição de pendrives, segmentação de  rede. |
| **Falhas de configuração (ex: senhas fracas)** | Médio | Alto | Alto | Adoção de MFA, revisão periódica de configurações, hardening de  sistemas. |
| **Interrupção do sistema de pagamento** | Alto | Médio | Alto | Gateway de pagamento alternativo, monitoramento em  tempo real. |

## Classificação do Tratamento de Riscos

* + - **Aceitar**: Apenas se o custo do controle for maior que o risco.
    - **Mitigar**: Implantação de medidas de controle para reduzir a probabilidade e/ou impacto.
    - **Transferir**: Uso de seguros cibernéticos ou terceirização de serviços (ex: pagamento).
    - **Eliminar**: Encerrar atividades ou serviços que tragam riscos inaceitáveis.

1. **Plano de Continuidade de Negócio**

O PCN visa garantir a retomada rápida e eficiente das atividades críticas do marketplace diante de incidentes, minimizando prejuízos operacionais, financeiros e à reputação.

* 1. **Processo Críticos**

Em caso de incidentes graves (falhas de TI, desastres naturais, ataques massivos), os processos de negócio mais críticos devem ser prioritariamente recuperados. Destacam-se:

* Autenticação e autorização: gestão de login e controle de acesso de clientes e vendedores, sem os quais não há transação possível.
* Processamento de transações: sistemas de pagamento e processamento de pedidos, que garantem a concretização de vendas e o fluxo financeiro.
* Comunicação com clientes e vendedores: serviços de mensageria interna e notificações, essenciais para confirmar pedidos, atualizações de entrega e suporte.
* Serviço de atendimento ao cliente: canais de contato (SAC, chat, e-mail) que atendem dúvidas e reclamações, sustentando a confiança do usuário.
* Infraestrutura de servidores e rede: servidores web, bancos de dados e equipamentos de rede que mantêm o site e sistemas disponíveis aos usuários.
* Armazenamento de dados: bases de dados de usuários, produtos e histórico de transações, necessários para retomada de operações e provas em auditoria pós-incidente.

**4.2 Estratégias de recuperação**

* Para manter a continuidade, devem ser adotadas estratégias de recuperação e alta disponibilidade:
* Redundância de sistemas (servidores em cluster e balanceamento de carga) para evitar pontos únicos de falha.
* Replicação e backups em locais alternativos (off-site), garantindo recuperação de dados em caso de perda.
* Infraestrutura de failover, com ambientes redundantes (data center secundário ou nuvem) prontos para assumir automaticamente em caso de queda.
* SLA com fornecedores de hospedagem e rede, assegurando suporte emergencial e limites de indisponibilidade.
* Testes periódicos de recuperação (DR drills) para validar procedimentos de restauração e treinar a equipe, identificando e corrigindo falhas no plano.

**4.3 Plano de contingência**

Define ações, responsáveis e canais de comunicação para incidentes graves:

* Coordenação: formação de um Comitê de Crise, liderado por um coordenador geral (ex.: Diretor de TI), que avalia a situação, autoriza ações emergenciais e mantém a governança do incidente.
* Responsabilidades: equipes específicas com papéis pré-definidos—infraestrutura (restauração de sistemas), banco de dados (recuperação de informações), desenvolvimento (verificação de integridade da aplicação) e comunicação (contato com imprensa, órgãos reguladores e usuários).
* Comunicação de emergência: definição de canais prioritários (telefone, e-mail, SMS) para notificar diretores, corpo técnico, órgãos como ANPD e usuários afetados, garantindo transparência e minimizando impactos reputacionais.
* Ações imediatas: procedimentos para isolar sistemas comprometidos, acionar rapidamente backups e iniciar failover, validando a integridade dos sistemas críticos para evitar danos adicionais.
* Resposta a incidentes e lições aprendidas: plano de contenção e erradicação detalhado, incluindo análise forense e correção de vulnerabilidades exploradas; após a normalização, realização de reuniões de avaliação para atualizar o plano e prevenir ocorrências futuras.

Essas diretrizes garantem que, mesmo diante de falhas de TI, ataques ou desastres, o marketplace retome suas operações de forma coordenada e eficiente, reduzindo riscos financeiros, mantendo a confiança dos usuários e assegurando conformidade com padrões de segurança.

**5. Referências**

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet).

BRASIL. Decreto n. 7.962, de 15 de março de 2013. Regulamenta a Lei n. 8.078/1990 (Código de Defesa do Consumidor) no comércio eletrônico.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005. Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.

ISO/IEC 27001:2022. Information technology – Security techniques – Information security management systems.