Trabalho de Segurança da Informação

Etapa 1: Contexto e Princípios de Segurança da Informação

1.1. Cenário da Empresa

Nome da empresa: Midnight Sky
Segmento: Joalheria
Modelo de operação: Loja física + e-commerce
Tempo de existência: 6 meses
Porte: Médio
Número aproximado de funcionários: 20 colaboradores

A Midnight Sky é uma joalheria de médio porte que atua tanto no varejo físico quanto digital. Com uma proposta de sofisticação e exclusividade, a empresa comercializa joias premium por meio de uma loja física e uma plataforma de e-commerce com alcance nacional. A manipulação de dados sensíveis de clientes e informações financeiras torna a segurança da informação um fator crítico para a continuidade e reputação da empresa.

1.2. Inventário Básico de Recursos de TI

1.2.1. Hardware

- **Na loja física e escritório:**
  - 10 computadores (setores de vendas, estoque, administração, financeiro)
  - 3 estações de PDV com leitores de código de barras e terminais POS
  - Impressoras multifuncionais e fiscais
  - Equipamentos de rede (roteadores, switches)
  - Câmeras IP, DVR/NVR, alarmes e sensores
  - Dispositivos móveis (tablets e smartphones)
  - Servidor local para backups e arquivos internos (opcional)
- **Para o e-commerce:**
  - Servidores em nuvem (hospedagem do site e banco de dados)
  - Gateways de pagamento externos

1.2.2. Software

- ERP/PDV para controle de estoque, vendas e finanças
- Plataforma de e-commerce (Shopify, Loja Integrada etc.)
- CRM para gestão do relacionamento com clientes
- Software financeiro (ex: Conta Azul)
- E-mails corporativos (Google Workspace ou Microsoft 365)
- Ferramentas de comunicação interna (Slack, Teams, WhatsApp Business)
- Antivírus, firewall, software de backup e criptografia

- Sistema de monitoramento de câmeras
- Sistemas operacionais (Windows, macOS, Linux) e navegadores padrão

1.2.3. Redes

- Internet por fibra óptica (alta velocidade)
- Wi-Fi interno (rede segura para funcionários)
- Wi-Fi separado para clientes
- Rede cabeada para PDVs, câmeras e servidores
- VPN para acesso remoto seguro

1.2.4. Dados Sensíveis

- **Dados de Clientes:** Nome, CPF, RG, endereço, telefone, e-mail, histórico de compras, preferências; dados financeiros processados por gateways externos, sem armazenamento local.
- **Dados de Funcionários:** Identificação, endereço, contato, dados bancários, salário e histórico profissional.
- **Dados Financeiros da Empresa:** Contas, fluxo de caixa, dados fiscais e bancários.
- **Dados de Estoque e Produtos:** Informações técnicas e comerciais das joias.
- **Propriedade Intelectual:** Designs, campanhas de marketing, estratégias internas.
- **Dados de Sistemas:** Logs, senhas (criptografadas), configurações, chaves de API.

1.2.5. Ativos da Empresa

Os ativos da Midnight Sky incluem os equipamentos físicos (computadores, PDVs, impressoras, roteadores, dispositivos móveis, câmeras), sistemas e softwares utilizados na operação diária (ERP, plataforma de e-commerce, CRM, sistemas de segurança e comunicação), a infraestrutura de rede (internet, Wi-Fi, rede cabeada, VPN), bem como os dados sensíveis e estratégicos armazenados ou processados. Também são considerados ativos os recursos humanos (colaboradores e parceiros), os contratos com fornecedores e serviços de nuvem, e a propriedade intelectual da marca. Todos esses elementos são fundamentais para o funcionamento e o valor da empresa, devendo ser protegidos contra ameaças e falhas operacionais.

1.3. Princípios de Segurança Aplicados (CID)

A segurança da informação da Midnight Sky é estruturada com base nos três pilares fundamentais:

1.3.1. Confidencialidade

Refere-se à proteção dos dados contra acessos não autorizados.
Aplicações práticas:

- Controle de acesso baseado em níveis de permissão
- Autenticação com múltiplos fatores (MFA)
- Criptografia de dados em trânsito e em repouso
- Segmentação de redes
- Gateways seguros para transações financeiras

1.3.2. Integridade

Garante que as informações não sejam alteradas indevidamente e permaneçam corretas e confiáveis.
Aplicações práticas:

- Backups automáticos e verificação de integridade
- Trilhas de auditoria e logs de acesso
- Controle de versões de documentos e registros
- Proteção contra alterações por softwares maliciosos

1.3.3. Disponibilidade

Assegura que os sistemas e informações estejam acessíveis sempre que necessário.
Aplicações práticas:

- Infraestrutura em nuvem com SLA de alta disponibilidade
- Monitoramento proativo dos sistemas
- Failover automático e plano de contingência
- Conectividade redundante e equipamentos com manutenção preventiva

Etapa 2: Ameaças, Vulnerabilidades e Normas de Segurança

2.1. Mapeamento de Ameaças e Vulnerabilidades

A Midnight Sky, por atuar em dois ambientes distintos (loja física e e-commerce), está exposta a uma ampla variedade de ameaças, tanto no espaço cibernético quanto no físico. A seguir, estão listadas as principais ameaças e vulnerabilidades identificadas com base em seu contexto operacional e tecnológico.

Ameaças

- **Ameaças Cibernéticas:**
  - **Malware (vírus, ransomware, spyware):** Podem infectar estações de trabalho ou o servidor local, comprometendo dados internos e interrompendo as operações da loja.
  - **Phishing e Engenharia Social:** Tentativas de enganar funcionários ou clientes com e-mails, mensagens ou ligações falsas para obter senhas ou dados financeiros.
  - **Ataques DDoS:** Podem sobrecarregar o site de e-commerce, tornando-o indisponível e prejudicando as vendas online.
  - **Roubo de Credenciais:** Senhas mal protegidas podem ser vazadas,

permitindo acesso indevido a sistemas sensíveis (ERP, banco de dados, e-mails).
    - **Invasões a Sistemas/Redes:** Acesso não autorizado à infraestrutura de TI, com riscos de manipulação de estoque, alteração de dados financeiros ou vazamento de informações de clientes.
    - **Ameaças internas:** Funcionários mal-intencionados ou descontentes podem acessar ou vazar informações sigilosas.
- **Ameaças Físicas:**
    - **Roubo ou furto de equipamentos:** Desktops, notebooks, PDVs ou servidores podem ser subtraídos da loja ou escritório.
    - **Desastres naturais:** Inundações, incêndios ou quedas de energia podem afetar sistemas críticos ou destruir informações não armazenadas adequadamente.
    - **Furtos de informação:** Cópias de dados em mídias removíveis (pendrives, HDs) sem autorização.
- **Ameaças Humanas (não intencionais):**
    - **Erro humano:** Exclusão acidental de arquivos, uso de senhas fracas, configuração incorreta de dispositivos.
    - **Negligência:** Ignorar procedimentos de segurança, acessar sistemas de redes públicas, uso de dispositivos pessoais não autorizados.

Vulnerabilidades

- **Vulnerabilidades de Software:**
    - Sistemas operacionais, ERPs ou plataformas de e-commerce desatualizados, sem correções de segurança (patches).
    - Configurações padrão não modificadas (por exemplo, credenciais padrão de administrador).
    - Dados sensíveis armazenados sem criptografia.
    - Utilização de senhas fracas ou reutilizadas por múltiplos funcionários.
- **Vulnerabilidades de Rede:**
    - Falta de segmentação adequada entre Wi-Fi de clientes e rede interna.
    - Ausência de firewall ou firewall mal configurado.
    - Portas abertas desnecessárias em servidores ou roteadores.
    - Acesso remoto sem o uso de VPN ou autenticação multifator (MFA).
- **Vulnerabilidades Humanas e Processuais:**
    - Ausência de treinamento em segurança da informação para os colaboradores.
    - Inexistência de políticas de segurança claras (uso de senhas, dispositivos, acesso remoto).
    - Falta de um plano de backup estruturado ou testes regulares de restauração.
    - Controle de acesso físico deficiente (portas destrancadas, câmeras desligadas).

- Descarte inadequado de documentos impressos ou equipamentos contendo dados antigos.

2.2. Normas, Leis e Regulamentações Pertinentes

A Midnight Sky deve estar em conformidade com diversas normas e legislações que regem a proteção de dados e boas práticas em segurança da informação. A seguir, destacam-se as principais:

- **LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018):** Regulamenta o tratamento de dados pessoais de clientes e funcionários. A empresa deve obter consentimento para uso de dados, garantir direitos dos titulares e adotar medidas de segurança para prevenir vazamentos.
- **ISO/IEC 27001:** Norma internacional que define requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Embora não seja obrigatório, serve como base para implementação de políticas, controles e práticas estruturadas.
- **Marco Civil da Internet (Lei nº 12.965/2014):** Estabelece princípios para o uso da internet no Brasil, incluindo a proteção de dados pessoais, a neutralidade da rede e a responsabilidade dos provedores.
- **Normas internas de TI e segurança:** A empresa deve formalizar diretrizes internas sobre uso de dispositivos, senhas, e-mail corporativo, descarte seguro de informações, acesso físico às dependências e resposta a incidentes.
- **PCI DSS (Payment Card Industry Data Security Standard):** Ainda que a Midnight Sky não armazene dados de cartão, ela deve utilizar gateways de pagamento que estejam em conformidade com esse padrão, garantindo a segurança nas transações online.

Conclusão da Etapa 2

O mapeamento das ameaças e vulnerabilidades da Midnight Sky permite identificar os principais riscos que podem comprometer a segurança de seus ativos. A adoção e conformidade com normas e boas práticas é essencial para estruturar uma resposta eficaz a esses riscos. A próxima etapa se concentrará na implementação de boas práticas e em uma estrutura de gestão de risco alinhada a essas ameaças identificadas.

Etapa 3: Boas Práticas e Gestão de Risco

Política de Boas Práticas de Gestão de Riscos - Midnight Sky

1. Introdução e Âmbito de Aplicação

Esta Política de Boas Práticas de Gestão de Riscos estabelece os princípios e diretrizes para identificar, analisar, avaliar, tratar e monitorar os riscos que podem impactar os objetivos da Midnight Sky, protegendo seus ativos e dados sensíveis.

Aplica-se a todos os colaboradores, fornecedores e terceiros com acesso aos sistemas, dados ou instalações, abrangendo loja física e e-commerce.

2. Princípios Fundamentais da Gestão de Riscos

A gestão de riscos na Midnight Sky é guiada por:

- **Abordagem Proativa:** Identificar e tratar riscos antes de incidentes.
- **Integralidade:** Considerar riscos tecnológicos, operacionais, financeiros, legais e reputacionais.
- **Melhoria Contínua:** Revisar e aprimorar processos periodicamente.
- **Responsabilidade:** Definir responsabilidades claras em todos os níveis.
- **Decisão Baseada em Risco:** Usar a análise de riscos como fator chave em decisões estratégicas e operacionais.

3. Estrutura de Gestão de Riscos

A Midnight Sky adotará uma estrutura de gestão de riscos baseada em etapas contínuas:

3.1. Identificação de Riscos

Consiste em reconhecer e descrever os riscos que podem afetar a Midnight Sky.

- **Metodologia:** Workshops, brainstorming, análise de incidentes passados, checklists e consultas a especialistas.
- **Foco:** Ameaças à confidencialidade, integridade e disponibilidade dos ativos (hardware, software, redes e dados sensíveis).
- **Exemplos de riscos:** Ataques de malware, phishing, engenharia social, falhas de configuração de sistemas, vazamento de dados de clientes, interrupções no e-commerce, fraudes financeiras, acesso não autorizado a sistemas internos.

3.2. Análise de Riscos

Avaliar a probabilidade de ocorrência de um risco e o impacto potencial em caso de materialização.

- **Probabilidade:** Alta, Média, Baixa (considerando a frequência de eventos e a existência de controles).
- **Impacto:** Crítico, Alto, Médio, Baixo (considerando o dano financeiro, reputacional, legal e operacional).
- **Ferramentas:** Matriz de probabilidade x impacto para classificar o nível de risco.

3.3. Avaliação e Priorização de Riscos

Classificar os riscos com base em sua análise, priorizando aqueles que exigem atenção imediata.

- Riscos com alta probabilidade e alto impacto serão considerados de prioridade

máxima.
- Os riscos serão documentados em um registro de riscos (ou planilha de análise de risco), incluindo sua descrição, causa, consequências, probabilidade, impacto e nível de risco.

3.4. Tratamento de Riscos (Plano de Mitigação)

Definir e implementar ações para gerenciar os riscos identificados, de acordo com as seguintes estratégias:

- **Mitigação:** Reduzir a probabilidade ou o impacto do risco.
  - **Exemplos de ações de mitigação (boas práticas recomendadas):**
    - **Controle de Acesso:** Implementação de controle de acesso baseado em níveis de permissão para sistemas e dados, com autenticação de múltiplos fatores (MFA) para acessos críticos.
    - **Senhas Fortes:** Obrigação de uso de senhas fortes, com complexidade, rotação periódica e proibição de reutilização.
    - **Criptografia:** Criptografia de dados sensíveis em repouso (servidores, backups) e em trânsito (conexões SSL/TLS no e-commerce, VPN para acesso remoto).
    - **Backup e Recuperação:** Implementação de política de backup automático e verificação de integridade dos dados, com testes periódicos de recuperação.
    - **Antivírus e Firewall:** Manutenção de softwares antivírus e firewall atualizados em todos os equipamentos, incluindo os servidores em nuvem do e-commerce.
    - **Atualizações de Software:** Aplicação regular de patches de segurança e atualizações de sistemas operacionais, ERP, plataforma de e-commerce e outras aplicações.
    - **Conscientização e Treinamento:** Realização de treinamentos periódicos sobre segurança da informação para todos os colaboradores, abordando temas como phishing, engenharia social e uso seguro de dispositivos.
    - **Segregação de Redes:** Redes Wi-Fi separadas para funcionários e clientes; rede cabeada isolada para PDVs e câmeras.
    - **Monitoramento:** Monitoramento proativo de logs de acesso, eventos de segurança e performance dos sistemas (servidores, redes).
    - **Segurança Física:** Controle de acesso físico à loja e escritório, monitoramento por câmeras e sistemas de alarme.
- **Aceitação:** Decisão de aceitar o risco devido ao baixo impacto ou custo elevado de mitigação.
- **Transferência:** Transferir o risco para terceiros (ex: seguros, terceirização de serviços com SLAs robustos).

- **Evitar:** Modificar ou descontinuar a atividade que gera o risco.

3.5. Monitoramento e Revisão de Riscos

Acompanhar a eficácia das ações de tratamento e identificar novos riscos.

- **Frequência:** Revisões trimestrais dos riscos e da eficácia dos controles.
- **Indicadores:** Número de incidentes, tempo de resposta a incidentes, resultados de auditorias internas e externas.
- **Responsáveis:** A gestão de riscos será coordenada pelo [Gerente de TI ou Comitê de Segurança da Informação], com a colaboração de todos os departamentos.

4. Responsabilidades

- **Diretoria:** Aprovar a Política de Boas Práticas de Gestão de Riscos e garantir os recursos necessários para sua implementação.
- **Gerência de TI:** Coordenar a implementação das ações de segurança técnica, monitoramento de sistemas e gestão de incidentes.
- **Analista de Boas Práticas e Gestão de Risco:** Elaborar e manter atualizado o registro de riscos, propor e acompanhar a implementação do plano de mitigação de riscos.
- **Todos os Colaboradores:** Cumprir as diretrizes e boas práticas de segurança, reportar incidentes e preocupações de segurança.

5. Documentação e Comunicação

Todas as informações relacionadas à gestão de riscos, incluindo o registro de riscos, planos de tratamento e resultados de monitoramento, serão devidamente documentadas e comunicadas aos stakeholders relevantes.

6. Conformidade Legal e Normativa

Esta política está alinhada com as normas e regulamentações pertinentes, como a LGPD (Lei Geral de Proteção de Dados) e as boas práticas de segurança da informação (ex: ISO 27001), garantindo a proteção dos dados pessoais dos clientes e colaboradores.

Etapa 4: Gestão de Continuidade do Negócio

Gestão de Continuidade de Negócio (GCN) - Midnight Sky

A Gestão de Continuidade de Negócio (GCN) da Midnight Sky tem como objetivo principal garantir que as operações essenciais da empresa possam ser mantidas ou rapidamente restabelecidas em caso de interrupções significativas causadas por desastres, falhas de sistemas, ataques cibernéticos ou outros eventos inesperados. Este plano visa minimizar o tempo de inatividade, proteger a reputação da empresa e

garantir a entrega contínua de produtos e serviços aos clientes.

1. Identificação de Processos Críticos do Negócio

Para a Midnight Sky, os processos críticos são aqueles cuja interrupção impactaria diretamente a receita, a satisfação do cliente, a conformidade legal ou a reputação da marca.

- **Processo de Vendas (Loja Física):** Realização de transações, processamento de pagamentos via PDV e emissão de notas fiscais.
  - **Impacto:** Perda de receita imediata, insatisfação do cliente.
- **Processo de Vendas (E-commerce):** Disponibilidade da plataforma online, processamento de pedidos e pagamentos.
  - **Impacto:** Perda de receita online, danos à reputação, interrupção das vendas nacionais.
- **Gestão de Estoque:** Controle de entrada e saída de joias, atualização de inventário.
  - **Impacto:** Vendas de produtos indisponíveis, atrasos na entrega, falha na reposição.
- **Gestão Financeira:** Processamento de pagamentos de fornecedores, recebimento de clientes, controle de fluxo de caixa.
  - **Impacto:** Problemas de fluxo de caixa, multas por atraso de pagamento, interrupção de serviços essenciais.
- **Comunicação com Clientes:** Atendimento a dúvidas, suporte pós-venda, gestão de reclamações.
  - **Impacto:** Perda de confiança, danos à reputação, insatisfação do cliente.
- **Gestão de Dados Sensíveis:** Proteção e processamento de informações de clientes (nome, CPF, endereço, histórico de compras) e dados financeiros.
  - **Impacto:** Violação da LGPD, multas, perda de confiança, danos reputacionais.

2. Estratégias de Recuperação

Para cada processo crítico, são definidas estratégias de recuperação para minimizar o tempo de inatividade e os impactos.

- **Para o E-commerce:**
  - **Infraestrutura em Nuvem:** Utilização de provedor de nuvem com alta disponibilidade (SLA robusto) e redundância geográfica para a plataforma de e-commerce e banco de dados.
  - **Backup e Restauração:** Backups automáticos diários do banco de dados e arquivos do site, com testes regulares de restauração para garantir a integridade dos dados.
  - **Plano de Contratação de Emergência:** Acordo pré-estabelecido com provedor de serviços de hospedagem alternativo (ou planos de contingência do

provedor atual) em caso de falha sistêmica do principal.
    - **Cache e CDN:** Uso de Content Delivery Network (CDN) para otimizar o carregamento do site e oferecer redundância de conteúdo.
- **Para a Loja Física e Operações Internas:**
    - **Servidor Local (Opcional):** Se houver um servidor local para backups e arquivos internos, garantir redundância de hardware (RAID), no-break e um plano de substituição rápida em caso de falha.
    - **Backup Offsite/Nuvem:** Backups regulares dos dados dos PDVs, ERP e arquivos internos para um local offsite (nuvem) para proteção contra desastres locais (incêndio, roubo).
    - **Hardware de Contingência:** Manter um computador e impressora sobressalentes para uso emergencial.
    - **Acesso Remoto Seguro:** Utilização de VPN para acesso seguro a sistemas essenciais a partir de locais alternativos, se necessário.
- **Para Conectividade de Rede:**
    - **Internet Redundante:** Contratação de dois provedores de internet diferentes na loja física para garantir conectividade contínua em caso de falha de um deles.
    - **Rede Móvel 4G/5G:** Dispositivos com capacidade de tethering (smartphones corporativos) como backup temporário para acesso à internet em caso de falha total da rede fixa.
- **Para Dados Sensíveis:**
    - **Criptografia:** Implementação de criptografia forte para dados em repouso e em trânsito.
    - **Controles de Acesso:** Manutenção rigorosa dos controles de acesso baseados em privilégios mínimos.
    - **Gateways de Pagamento Externos:** Utilização de gateways de pagamento PCI-DSS compliant para minimizar o armazenamento de dados financeiros sensíveis localmente.

3. Plano de Contingência Básico

O Plano de Contingência define os procedimentos de emergência, os responsáveis e as estratégias de comunicação em caso de incidentes.

3.1. Procedimentos de Emergência

- **Incidente de Segurança Cibernética (Ex: Ataque de Ransomware no ERP):**
    - Detecção, Isolamento dos sistemas infectados, Análise da extensão do dano (TI/consultoria), Recuperação (restauração de backup íntegro) e Investigação Pós-Incidente.
- **Falha no Servidor de E-commerce:**
    - Notificação, Ativação das estratégias de recuperação em nuvem

(failover/backup), Monitoramento de estabilidade e desempenho.
- **Interrupção de Energia Elétrica na Loja Física:**
  - Uso de no-breaks, Operação em modo manual (registros em papel, pagamentos em dinheiro), Comunicação com clientes.
- **Roubo/Furto de Equipamentos na Loja:**
  - Registro do incidente e acionamento das autoridades, Ativação de hardware de contingência, Restauração de dados de backups.

3.2. Responsáveis

A GCN exige responsabilidades claras:

- **Comitê de Continuidade (ou Gerência de TI):** Aprovar e coordenar o PCN, conduzir testes.
- **Equipe de TI:** Executar recuperações técnicas, monitorar infraestrutura.
- **Gerência de Vendas e Operações:** Implementar procedimentos manuais, gerenciar comunicação com clientes/equipe.
- **Gerência Financeira:** Garantir fluxo de caixa e pagamentos.
- **Colaboradores:** Cientes dos procedimentos e reportar incidentes.

3.3. Comunicação

Uma comunicação eficaz é vital:

- **Interna:** Usar canais de emergência (WhatsApp, e-mail alternativo); atualizações regulares para a equipe.
- **Externa (Clientes e Parceiros):** Utilizar canais primários (e-mail, redes sociais, site); definir porta-voz oficial; usar modelos de mensagens pré-aprovadas; informar sobre medidas e tempo de retorno.
- **Autoridades e Órgãos Reguladores:** Notificar a ANPD em caso de vazamento de dados pessoais (LGPD).

Referências Bibliográficas

- BRASIL. Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
- BRASIL. Marco Civil da Internet (Lei nº 12.965/2014). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
- PCI DSS – Payment Card Industry Data Security Standard. Council Standards. Disponível em: https://www.pcisecuritystandards.org/
- ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.
- CABRAL, Fernando; CAPRINO, Fabio. Segurança da Informação: uma abordagem gerencial. Rio de Janeiro: Ciência Moderna, 2017.

- STALLINGS, William. Segurança em Redes de Computadores: princípios e práticas. São Paulo: Pearson, 2018.
- HINTZBERGEN, Jan et al. Fundamentos de Segurança da Informação. São Paulo: Novatec, 2016.
- CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: https://www.cert.br/
- Instituto Nacional de Tecnologia da Informação – ITI. Diretrizes sobre certificados digitais e segurança. Disponível em: https://www.iti.gov.br/