

MAGALU

- Descrição do cenário

A Magazine Luiza, popularmente conhecida como Magalu, é uma das maiores empresas varejistas do Brasil, com forte atuação tanto no comércio eletrônico quanto em lojas físicas espalhadas por todo o território nacional. Fundada em 1957, a empresa evoluiu de uma rede de lojas regionais para um ecossistema digital completo, oferecendo produtos e serviços que vão além do varejo tradicional.

A Magalu também comercializa uma ampla variedade de produtos, incluindo:

- Eletrodomésticos
- Eletrônicos
- Móveis e decoração
- Moda e beleza
- Produtos de mercado
- Livros, brinquedos e papelaria;
- Serviços financeiros, como cartão de crédito Magalu e seguros;
- Marketplace com produtos de lojistas parceiros.

Recursos de TI

O Magalu investe fortemente em tecnologia, possuindo uma plataforma de e-commerce robusta, um aplicativo amplamente utilizado, serviços financeiros integrados e um marketplace que conecta lojistas parceiros. Toda essa infraestrutura depende fortemente da Tecnologia da Informação (TI), tornando a segurança da informação um fator estratégico essencial

Servidores e Infraestrutura

Servidores de aplicação (Web, ERP, CRM)

Servidores de banco de dados (MySQL, Oracle, PostgreSQL)

Servidores de backup e redundância

Infraestrutura em nuvem (ex: AWS, Google Cloud, Azure)

Equipamentos de rede: switches, roteadores, firewalls e balanceadores de carga

Data centers físicos e ambientes híbridos

Sistemas e Softwares

ERP (gestão integrada de estoque, vendas, financeiro)

CRM (gestão de relacionamento com o cliente)

Sistema de gestão logística (WMS e TMS)

Plataforma de e-commerce e marketplace

Sistemas antifraude e análise de risco

Softwares de monitoramento (Zabbix, Prometheus)

Antivírus corporativo e firewall de aplicação (WAF)

Dispositivos e Equipamentos

Estações de trabalho (computadores corporativos)

Notebooks para uso remoto ou de campo

Dispositivos móveis (tablets e smartphones)

Impressoras fiscais e não fiscais

PDVs (pontos de venda integrados)

Serviços de Rede e Conectividade

Redes Wi-Fi internas (com VLANs por setor)

VPN para acesso remoto seguro

Links de internet dedicados e redundantes

Servidores DNS e DHCP próprios

Recursos de Segurança da Informação

Autenticação multifator (MFA)

Sistema de gerenciamento de identidade (IAM)

Ferramentas de criptografia de dados

Políticas de controle de acesso (ACLs)

Sistemas de prevenção e detecção de intrusão (IDS/IPS)

Sistema de resposta a incidentes (SOC/NOC)

Armazenamento e Backup

Armazenamento em rede (NAS/SAN)

Soluções de backup automatizado e criptografado

Armazenamento em nuvem com redundância geográfica

Plataformas de Comunicação

E-mail corporativo com proteção contra spam e phishing

Ferramentas de videoconferência e chat (Microsoft Teams, Google Meet)

Central telefônica IP (VoIP)

Princípios de segurança aplicados (CID):

Confidencialidade: proteger dados de clientes (CPF, endereço, cartão).

Integridade: garantir que pedidos, estoques e pagamentos não sejam alterados maliciosamente.

Disponibilidade: site e app precisam estar sempre online, especialmente em promoções.

2. Mapeamento de possíveis ameaças e vulnerabilidades

Possíveis Ameaças para o Magalu:

Phishing: Tentativas de enganar clientes ou colaboradores via e-mail ou SMS.

Malware/Ransomware: Códigos maliciosos que podem afetar os sistemas de pagamento e logística.

Ataques DDoS: Podem derrubar a loja virtual em datas críticas (Black Friday, Natal).

Engenharia social: Funcionários podem ser manipulados para fornecer informações sigilosas.

Exposição de dados sensíveis: Vazamentos de dados de clientes ou cartões de crédito.

Ameaças internas: Ações maliciosas de funcionários ou ex-colaboradores.

Principais Vulnerabilidades no Ambiente da Magalu:

Sistemas desatualizados ou com falhas de configuração.

Falta de autenticação multifator em sistemas críticos.

Acesso excessivo a dados por usuários sem necessidade (privilégios elevados).

Treinamento insuficiente em segurança da informação para os colaboradores.

Integração com parceiros ou fornecedores inseguros.

Normas, leis e regulamentações pertinentes:

Para garantir a conformidade e segurança das operações, a Magalu deve seguir e adotar:

LGPD (Lei Geral de Proteção de Dados): regulamenta o tratamento de dados pessoais de clientes e colaboradores.

ISO/IEC 27001: norma internacional para gestão de segurança da informação.

PCI DSS: padrão de segurança aplicável para empresas que lidam com dados de cartão de crédito.

Marco Civil da Internet: regula o uso da internet no Brasil, garantindo direitos e deveres quanto à privacidade e proteção de dados.

Referências de Apoio

ABNT NBR ISO/IEC 27001:2022 – Sistemas de Gestão da Segurança da Informação.

Lei 13.709/2018 – LGPD

Lei 12.965/2014 – Marco Civil da Internet

Guia de Boas Práticas da ANPD

Cartilhas da CERT.br (boas práticas para usuários e empresas)

3. Boas Práticas e Gestão de

Risco

Essas práticas têm como objetivo prevenir incidentes de segurança e proteger dados sensíveis da empresa e dos clientes:

Boas práticas recomendadas:

Uso de senhas fortes: Senhas simples são facilmente quebradas. Por isso, recomenda-se o uso de senhas complexas, com letras, números e símbolos. Além disso, sempre que possível, é ideal implementar autenticação de dois fatores (2FA).

Política de backup: Ter cópias de segurança dos dados é essencial. Os backups devem ser feitos com frequência e armazenados de forma segura, preferencialmente criptografados e fora do ambiente principal.

Criptografia de dados: Tanto os dados em trânsito (enviados pela rede) quanto os que estão armazenados devem ser protegidos com criptografia, principalmente se forem dados sensíveis.

Antivírus e firewall: Softwares de proteção devem estar sempre atualizados e ativos para bloquear malwares, tentativas de invasão e tráfego malicioso.

Conscientização dos usuários: Muitas falhas de segurança acontecem por erro humano. Por isso, é importante que os colaboradores sejam treinados para reconhecer golpes como phishing, evitar clicar em links suspeitos e seguir boas práticas.

Controle de acesso: Nem todo mundo precisa ter acesso a tudo. O ideal é limitar os acessos com base nas funções de cada colaborador, aplicando o princípio do menor privilégio.

Gestão de risco

A gestão de risco serve para identificar o que pode dar errado, avaliar os impactos e definir o que fazer para evitar ou lidar com esses riscos.

Identificação de riscos: Primeiro passo é listar os ativos de TI (como servidores, sistemas e dados), possíveis ameaças e vulnerabilidades.

Análise e avaliação: Depois, é preciso avaliar quais riscos são mais críticos, considerando a probabilidade de acontecer e o impacto que causariam.

Tratamento dos riscos: Com base na análise, a empresa pode escolher aceitar, reduzir, transferir ou eliminar o risco. Isso pode envolver novas ferramentas, mudanças em processos, entre outros.

Monitoramento contínuo: A segurança não é algo fixo. É preciso acompanhar os riscos e atualizar as estratégias sempre que necessário.

Registro e documentação: Tudo deve ser documentado: riscos identificados, decisões tomadas, medidas aplicadas e resultados. Isso ajuda na gestão, auditorias e melhorias futuras.

4. SISTEMAS CRÍTICOS PRIORITÁRIOS

1. Plataforma de E-commerce e Marketplace
2. Sistemas de Logística e Estoque
3. Banco de Dados de Clientes e Parceiros

CENÁRIOS DE RISCO E AÇÕES DE CONTINGÊNCIA

1. Ataque Cibernético (Ransomware)

Impacto: Inviabiliza vendas, compromete dados e bloqueia sistemas críticos.

Ações Preventivas:

- * Backup diário automático, com cópias offline e em nuvem.
- * Autenticação multifator

Ações de Contingência:

- * Isolamento da rede e dos sistemas afetados.
- * Ativação do plano de resposta a incidentes com suporte forense.
- * Restauração imediata via backup mais recente testado.

2. Queda de Servidor ou Datacenter

Impacto: Interrupção do e-commerce, falhas no controle de estoque e transportes.

Ações Preventivas:

- * Arquitetura em nuvem híbrida com balanceamento de carga.
- * Replicação ativa dos dados em ambientes geograficamente distintos.

Ações de Contingência:

- * Ativação automática do site espelho e sistemas redundantes.
- * Redirecionamento de rotas logísticas para centros operacionais ativos.
- * Alerta interno para priorizar atendimento manual (caso necessário).