Proposta
De
Soluções Seguras

Equipe:
Emanuel Mello de Oliveira.
Gustavo Henrique Siqueira Viana.
Lucas Domingos da Silva.
Marco Vinnycius Menezes Vieira.

Belo Horizonte, 17 de novembro de 2024

Sumário

Etapa 3 – Projeto Fundamentos de Sistemas.

1. Introdução

1.1 Contexto

A empresa "Sabor do Campo", dedicada à produção de produtos artesanais, foi concebida do ponto zero, exigindo a implementação de uma infraestrutura de TI robusta e segura para sustentar suas operações. Diante de um cenário tecnológico desafiador, a proteção de dados e a continuidade dos processos empresariais tornaram-se prioridades essenciais.

1.2 Descrição do Problema

A crescente dependência de sistemas digitais expõe a empresa a vulnerabilidades como vazamento de dados pessoais, ataques cibernéticos e inconsistências operacionais. Além disso, a adequação às exigências da Lei Geral de Proteção de Dados (LGPD) é indispensável para assegurar a conformidade regulatória e a confiança dos clientes.

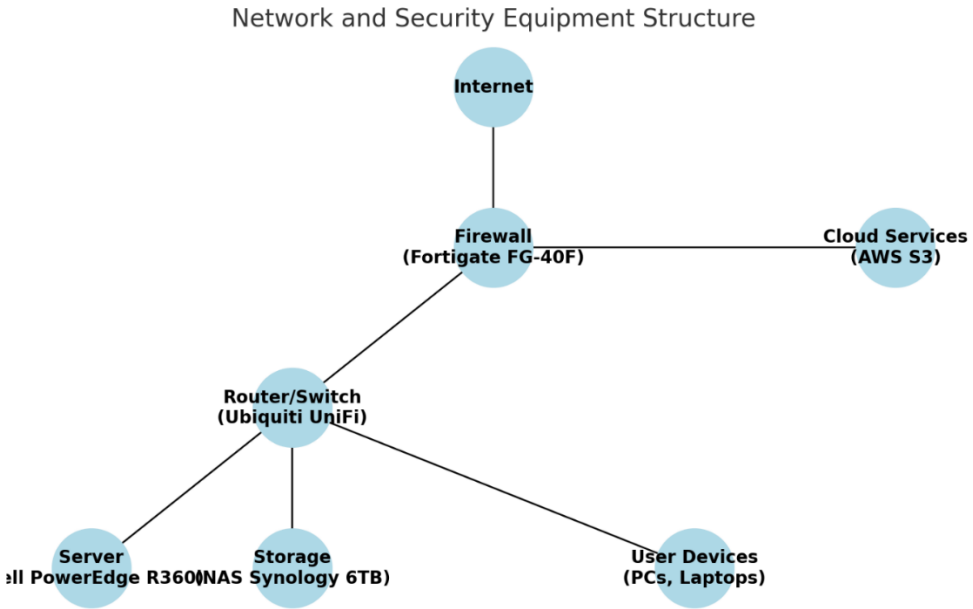
1.3 Objetivo

Identificar e mitigar problemas de segurança digital e física, com foco em proteger dados sensíveis, garantir a continuidade operacional e atender às exigências legais.

1.4 Objetivo Específico

Identificar e solucionar problemas relacionados à conformidade com a LGPD.
Justificativa
A resolução dos problemas identificados resultará em uma operação mais segura, com redução significativa de riscos e impactos de incidentes cibernéticos. Além disso, a conformidade com a LGPD fortalecerá a reputação da empresa e a confiança dos clientes, garantindo um ambiente digital confiável para sustentar o crescimento do negócio.

1.5 Diagrama da arquitetura:



O diagrama apresentado ilustra a arquitetura de rede e segurança projetada para a empresa "Sabor do Campo", destacando os principais componentes tecnológicos necessários para garantir conectividade, desempenho e proteção de dados.

2 Modelo de sistema de informação e proposta de solução.

Informação	**Origem**	**Processamento/ Transformação**	**Saída**	**Ameaças/ Vulnerabilidades**	**Proposta de solução**
Dados do cliente	Cadastro no site	Nome, e-mail, endereço, CPF, validado no banco de dados	Conta cadastrada	Vazamento de dados pessoais; cadastros automáticos (bots).	Uso de criptografia (SSL), CAPTCHA para validação humana e autenticação multifator (MFA).

3 Investimentos CAPEX e OPEX.

CAP/EX				
Categoria	Descrição	Quantidade	Valor	Valor Total
Servidores	Servidor Dell PowerEdge R360	1	R$ 17.499	R$ 17.499
Storage	NAS Synology 6TB	2	R$ 3.300	R$ 6.600
Switch / Roteador	Ubiquiti UniFi (UDM - Pro)	1	R$ 4.900	R$ 4.900
Firewall	Fortigate - FG-40F	1	R$ 5.400	R$ 5.400
Total: R$ 34.399				

OP/EX (Anual)				
Categoria	Descrição	Quantidade	Valor	Valor Total
Manutenção de Hardware	Contratos de manutenção	1	R$ 15.000	R$ 15.000
Consumo de Energia	Energia elétrica	N/A	R$ 2.083	R$ 25.000
Suporte Técnico	Contrato de suporte	1	R$ 17.000	R$ 17.000
Atualizações de Software	Licenças e atualizações	3	R$ 9.000	R$ 9.000
Cloud Storage	AWS S3 10TB	1	R$ 1.362,28	R$ 16.383,57
Total: R$ 82.383,57				

4 C# Script

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:

- Hardware
- Software
- Hardware e Software

5 Análise de riscos/continuidade/contingência dos itens de segurança física e lógica.

5.1 Identificação de ativos e seus valores:

Servidores: Críticos para o funcionamento de sistemas e armazenamento de dados sensíveis.
Computadores e notebooks: Usados para tarefas diárias e armazenamento de informações.
Infraestrutura de Rede: Base para conectividade e transmissão de dados.
Serviços de Nuvem: Armazenamento remoto e serviços de alta disponibilidade.
Softwares: Ferramentas e sistemas que suportam os processos organizacionais.
Sistemas de Controle de Acesso: Responsáveis por manter a segurança de áreas e informações críticas.

5.2 Determinar as vulnerabilidades e ameaças:

Servidores:
Vulnerabilidades: Configurações inadequadas, falta de atualizações, credenciais fracas.
Ameaças: DDoS, malware/ransomware, acesso não autorizado.

Computadores e notebooks:
Vulnerabilidades: Falta de criptografia, software desatualizado, uso de redes inseguras.
Ameaças: Phishing, spyware/adware, roubo físico.

Infraestrutura de Rede:
Vulnerabilidades: Configurações de firewall inadequadas, falta de segmentação, protocolos inseguros.
Ameaças: Interceptação de dados, injeção de pacotes, ataques de redirecionamento.

Serviços de Nuvem:
Vulnerabilidades: Configurações inadequadas, gestão de credenciais, controle de acesso ineficaz.
Ameaças: Fuga de dados, dependência de terceiros.

Softwares:
Vulnerabilidades: Falta de atualizações, permissões excessivas, bugs/código mal escrito.
Ameaças: Exploração de vulnerabilidades, backdoors, trojans.

Sistemas de Controle de Acesso:
Vulnerabilidades: Autenticação fraca, gestão de privilégios inadequada, falta de monitoramento.
Ameaças: Bypassing, engenharia social, credential stuffing.

5.3 Risco potencial de ameaças:

- Alta probabilidade e alto impacto: Ransomware em servidores ou fuga de dados na nuvem pode interromper operações críticas.

Alta probabilidade e impacto moderado: Uso de redes inseguras ou software desatualizado pode levar a ataques pontuais.

Baixa probabilidade e alto impacto: Ataques de redirecionamento na rede ou roubo físico de notebooks com informações sensíveis.

Baixa probabilidade e impacto moderado: Engenharia social ou ataques de phishing que comprometam dados individuais.

5.4 Custos: Incidentes X Medidas de Segurança

Servidores:
Medidas Prioritárias:
Regras de acesso e permissões restritas (RBAC), implementação de auditorias periódicas (custo zero).
Solução de armazenamento de backups em nuvem, como o AWS S3 (R$16.000 anuais).
Atualizações de sistemas operacionais e software de servidores periodicamente (custo zero).
Justificativa: As configurações básicas de segurança e os backups regulares protegem contra os riscos de indisponibilidade (DDoS, ransomware) e minimizam o impacto em caso de incidentes.
Total para servidores: R$16.000.

Computadores e notebooks:
Medidas Prioritárias:
Uso de criptografia de discos com ferramentas gratuitas como o BitLocker, para proteção de dados em caso de perda ou roubo (custo zero).
Contratar antivírus corporativo básico, como ESET ou Avast Business (R$5K anuais).
Promover treinamentos anuais de conscientização sobre phishing e segurança digital, utilizando soluções EAD ou workshops econômicos (R$3K).

Justificativa: Essas medidas são cruciais para proteger dados sensíveis armazenados localmente e reduzir a probabilidade de sucesso de ataques de engenharia social.
Total para computadores e notebooks: R$8K.

Infraestrutura de Rede:
Configuração adequada do firewall, oferecendo proteção robusta contra ameaças. (custo zero)
Configurar segmentação de rede para separar ativos críticos de dispositivos gerais (custo zero).
Utilizar a funcionalidade de VPN do FortiGate para garantir conexões seguras e proteger dados em trânsito (custo incluído na licença + R$ 1.500, custo aproximado anual do ip fixo).

Justificativa: Essas ações protegem contra ameaças como interceptação de dados e redirecionamento de tráfego malicioso, limitando a propagação de ataques.
Total para infraestrutura de rede: R$ 1.500.

Serviços de Nuvem:
Medidas Prioritárias:
Uso de soluções em nuvem econômicas com segurança integrada, como o Microsoft 365 Business Basic, incluindo autenticação multifator e backup (R$ 8.000 / Ano).
Garantir a criptografia de dados em trânsito e armazenamento, já incluída na maioria dos serviços de nuvem (custo zero).

Justificativa: Esses serviços oferecem segurança integrada, escalabilidade e proteção contrafuga de dados, atendendo as necessidades de uma pequena empresa sem grandes investimentos.
Total para serviços de nuvem: R$8.000.

Softwares:
Medidas Prioritárias:
Automatizar atualizações de sistemas operacionais e aplicativos com ferramentas nativas. Ex: WSUS (custo zero).
Revisar regularmente as permissões e logs de acessos nos sistemas, com apoio de ferramentas gratuitas ou já existentes (custo zero).

Justificativa: Atualizações e gestão de permissões são medidas simples e de baixo custo que mitigam riscos associados a exploração de vulnerabilidades.
Total para softwares: R$0 (tempo interno da equipe).

6 Referências bibliográficas

- Referência: STALLINGS, William. Redes de Computadores e a Internet: Uma Abordagem Top-Down. 6ª Edição. Pearson, 2013.
  Link: Redes de Computadores - William Stallings
  Modelo de Sistema de Informação e Proposta de Solução
- Referência: TURBAN, Efraim; VOLONINO, Linda. Tecnologia da Informação para Gestão: Transformando as Organizações na Economia Digital. Tradução. Bookman, 2010.
  Link: Tecnologia da Informação para Gestão - Efraim Turban
  Investimentos CAPEX e OPEX
- Referência: FITZSIMMONS, James A.; FITZSIMMONS, Mona J. Administração de Serviços: Operações, Estratégia e Tecnologia da Informação. 5ª Edição. McGraw-Hill, 2007.
  Link: Administração de Serviços - James A. Fitzsimmons
  C# Script
- Referência: TROELSEN, Andrew; JAPIKSE, Philip. Dominando C#: Introdução e Prática com C# e .NET. Tradução. Apress, 2021.
  Link: Dominando C# - Andrew Troelsen
  Análise de Riscos/Continuidade/Contingência dos Itens de Segurança Física e Lógica
- Referência: TIPTON, Harold F.; KRAUSE, Micki. Gestão de Segurança da Informação: Guia Completo. Tradução. LTC, 2007.
  Link: Gestão de Segurança da Informação - Harold F. Tipton
  Identificação de Ativos e Seus Valores
- Referência: NIST. Guia para Realização de Avaliações de Risco (SP 800-30 Revisão 1). Tradução oficial. Instituto Nacional de Padrões e Tecnologia, 2012.
  Link: Guia para Avaliações de Risco - NIST

Determinar as Vulnerabilidades e Ameaças

- Referência: OWASP. OWASP Top Ten: Os Dez Principais Riscos de Segurança em Aplicações Web. OWASP, 2021.
  Link: OWASP Top Ten - Tradução para Português
  Risco Potencial de Ameaças
- Referência: ISO/IEC 27005:2018. Gestão de Riscos de Segurança da Informação. Organização Internacional de Normalização, 2018.
  Link: ISO/IEC 27005:2018
  Custos: Incidentes X Medidas de Segurança
- Referência: GORDON, Lawrence A.; LOEB, Martin P. Gestão de Recursos de Cibersegurança: Uma Análise de Custo-Benefício. Tradução. McGraw-Hill, 2006.
  Link: Gestão de Recursos de Cibersegurança - Gordon