PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Segurança da Informação

PUC Minas

Apresentação
De
Soluções Seguras

Equipe:

Emanuel Mello de Oliveira.

Gustavo Henrique Siqueira Viana.

Lucas Domingos da Silva.

Marco Vinnycius Menezes Vieira.

Belo Horizonte
2024

SUMÁRIO

I – Introdução

História da Empresa

A "Sabor do Campo" foi fundada em 1990, em Belo Horizonte, Minas Gerais, pela Sra. Maria D.C.M. e seus filhos H. e H. Em 1991, a empresa transferiu suas operações para Contagem e, no ano seguinte, Vicente C., diretor comercial, tornou-se sócio da família, consolidando sua participação no negócio. Em 1995, os sócios adquiriram um laticínio em Conceição do Pará, focando na produção de queijos para aprimorar suas receitas, e inauguraram uma sede própria em Contagem. Em 1999, a empresa foi vendida para uma multinacional americana, mas, após dez anos, retornou às mãos de seus fundadores, retomando o mercado com foco em qualidade, sabor e tradição.

Atualmente, a "Sabor do Campo" é referência na produção de alimentos típicos de Minas Gerais, como pão de queijo, broinhas e palitos de queijo, além de diversificar seu portfólio com iguarias internacionais, como waffles, croissants, quiches, massas recheadas e empanadas. A empresa se destaca por investir continuamente em pesquisa e desenvolvimento para atender os mercados local, nacional e internacional, garantindo produtos de alta qualidade e sabor autêntico. Para isso, conta com uma equipe de profissionais qualificados, matérias-primas selecionadas e equipamentos de última geração.

A missão da empresa é proporcionar alimentos práticos e inovadores, com sabor e qualidade de receitas caseiras, enquanto sua visão é globalizar o pão de queijo e fazer parte do dia a dia das pessoas. Os valores da "Sabor do Campo" incluem tradição, qualidade, respeito, comprometimento, inovação e lucratividade, sendo pilares fundamentais para o crescimento sustentável do negócio e a satisfação de clientes e colaboradores. A empresa é especializada na produção e comercialização de alimentos congelados e atua em três frentes principais: fabricação de produtos típicos com tecnologia de congelamento, venda direta ao consumidor por plataformas digitais e redes de supermercados, e expansão para mercados internacionais. A base de seu sucesso está na produção própria de queijos, o que garante a essência e o sabor que conquistam consumidores no Brasil e no exterior.

Após passar por mudanças societárias, a Sabor do Campo retomou suas operações focadas em inovação e expansão. Atualmente, combina tradição e modernidade para atender mercados locais, enfrentando desafios de segurança da informação e modernização tecnológica, essenciais para seu crescimento sustentável.

Problema

Com a digitalização acelerada de suas operações e a dependência crescente de sistemas de TI, a Sabor do Campo enfrenta problemas críticos de segurança da informação. Entre os desafios mais urgentes estão:

Vazamento de dados sensíveis: Especialmente informações de clientes coletadas no processamento de pedidos online.

Ameaças cibernéticas: Como ataques de ransomware e phishing, que podem comprometer dados críticos e paralisar operações.

Conformidade legal: A necessidade de adequação à Lei Geral de Proteção de Dados (LGPD) e outras normas de proteção de dados, cuja não observância pode acarretar multas e danos à reputação.

Além disso, a ausência de uma política formal de segurança da informação antes do projeto aumentava o risco de uso inadequado de tecnologias e dados, expondo a organização a vulnerabilidades evitáveis.

Objetivo

O projeto foi concebido com os seguintes objetivos:

Identificar e compreender as principais vulnerabilidades nos sistemas de segurança da "Sabor do Campo".

Propor soluções específicas para ao menos um problema crítico, priorizando a mitigação de riscos e a proteção de dados.

Implementar ações práticas que fortaleçam a resiliência da empresa diante de ameaças cibernéticas e assegurem a conformidade com legislações aplicáveis.

Esses objetivos estão alinhados ao compromisso estratégico da empresa de operar de forma segura, eficiente e sustentável, promovendo a confiança dos clientes e o crescimento contínuo.

Justificativa

A segurança da informação é um pilar essencial para empresas modernas, especialmente aquelas que, como a "Sabor do Campo", dependem de sistemas digitais para suas operações. A resolução dos problemas identificados trará benefícios como:

Mitigação de riscos cibernéticos: Reduzindo a probabilidade de vazamentos de dados, ataques cibernéticos e falhas operacionais.

Conformidade regulatória: Garantindo que a empresa atenda às exigências da LGPD e outras legislações relevantes, evitando penalidades legais.

Fortalecimento da reputação: A confiança dos consumidores em uma marca é diretamente afetada pela forma como seus dados são tratados.

Eficiência operacional: A implementação de medidas de segurança aprimora os processos internos, tornando a organização mais ágil e preparada para desafios futuros.

II - Metodologia

O projeto foi desenvolvido em três etapas interdependentes, cada uma com objetivos claros e resultados significativos.

Etapa 1: Levantamento Inicial

Objetivo: Mapear os principais processos de negócio, identificar riscos preliminares e compreender o impacto das legislações sobre as operações.

Atividades:

Levantamento dos processos principais, como vendas, manufatura e recursos humanos.

Identificação das legislações aplicáveis, incluindo LGPD, Código de Defesa do Consumidor e normas ISO.

Resultados: A análise inicial destacou o processamento de pedidos online como o processo mais vulnerável, com riscos significativos relacionados à coleta e armazenamento de dados sensíveis. Identificou-se também uma lacuna na integração entre sistemas de TI, o que aumentava a exposição a vulnerabilidades.

Construção de uma matriz de relacionamento entre processos e leis, conforme detalhado a seguir:

A tabela detalha leis e normas que impactam a organização, destacando a necessidade de conformidade com privacidade (LGPD, Marco Civil), direitos do consumidor (Lei do E-commerce, CDC) e segurança da informação (ISO 17799, 27002). Abrange ainda proteção fiscal, trabalhista e propriedade intelectual.

Lei	Impacto na Organização
LGPD	Controle de acesso aos dados sensíveis dos clientes, armazenados com segurança e acessados apenas por pessoal autorizado. Implementação de mecanismos de rastreamento e exclusão de dados pessoais conforme solicitado pelos clientes.
Marco Civil	Estabelecimento de regras claras para o uso da internet, garantindo a privacidade dos dados dos usuários e a transparência nas práticas de coleta e uso de informações.

Lei do E-commerce	Conformidade com os direitos do consumidor em vendas online, incluindo informações claras sobre produtos, preços, condições de venda, políticas de devolução e segurança no processamento de pagamentos.
Código Civil	Regulação de obrigações contratuais e responsabilidades civis em transações comerciais. Garantia de conformidade legal em operações e contratos, evitando problemas jurídicos.
Código de Defesa do Consumidor	Proteção dos direitos dos consumidores, como informações claras sobre produtos e serviços, direito à privacidade e garantia da qualidade dos produtos. A empresa assegura conformidade com os direitos do consumidor em suas operações de venda.
Código Penal	Prevenção de crimes relacionados à violação de privacidade, fraudes e crimes cibernéticos. A empresa alinha suas práticas de segurança da informação para evitar crimes digitais e outros ilícitos.
Código Tributário Nacional	Implementação de sistemas de TI para gerenciar registros fiscais com segurança e eficiência, garantindo conformidade tributária e evitando erros humanos ou fraudes fiscais. Colaboração com contabilidade para atender exigências legais.
Constituição Federal	Observância dos direitos fundamentais, incluindo a proteção de dados pessoais e privacidade, bem como respeito à dignidade e aos direitos do consumidor.
Consolidação das Leis do Trabalho (CLT)	Conformidade com as normas trabalhistas em processos de contratação, demissão e gestão de dados de funcionários, garantindo direitos e regulando relações de trabalho.
Lei de Propriedade Industrial	Proteção de marcas, patentes e inovações, assegurando os direitos de propriedade intelectual, especialmente sobre produtos exclusivos como o pão de queijo.
Lei de Direitos Autorais	Proteção de materiais criativos, como imagens, textos e receitas, evitando violação de direitos autorais em marketing, embalagens e comunicações.
ISO 17799	Implementação de melhores práticas de segurança da informação, com foco na proteção de ativos, controle de acesso, gestão de incidentes e segurança física.
ISO 27002	Aplicação de controles para garantir a confidencialidade, integridade e disponibilidade dos dados, protegendo

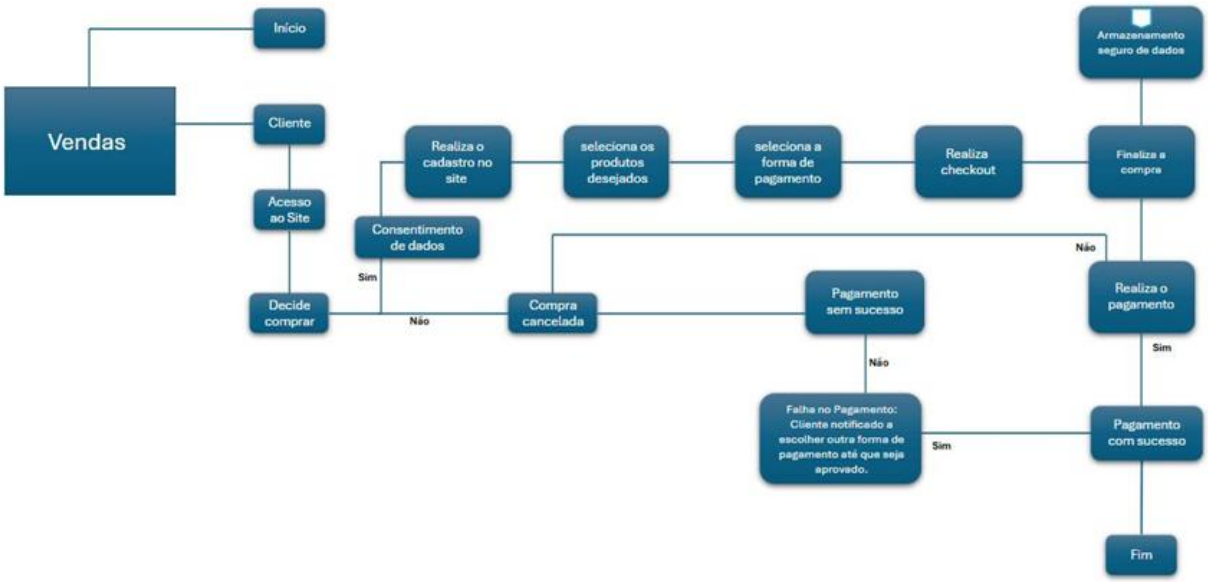
	informações sensíveis e assegurando conformidade com legislações como a LGPD.

Etapa 2: Diagnóstico Detalhado

Objetivo: Realizar uma análise aprofundada dos riscos e propor diretrizes para mitigá-los.

Atividades:

Detalhamento do processo de processamento de pedidos por meio de fluxogramas, mapeando etapas críticas como cadastro, pagamento e finalização da compra.



Levantamento de itens de TI invisíveis, como softwares pessoais não catalogados em vendas e marketing, que representavam risco de perda de dados e falta de integração.

A tabela lista itens de TI não catalogados em setores organizacionais, identificando proprietários, usuários, riscos e observações. Destacam-se ferramentas usadas individualmente, como CRM e softwares de gestão, que apresentam riscos como perda de dados, vulnerabilidades sensíveis e falta de integração com sistemas oficiais. Ferramentas de design, controle remoto e rastreamento também trazem desafios relacionados à segurança e conformidade, enquanto planilhas de RH e análises financeiras exigem proteção rigorosa de dados críticos.

Setor	Item de TI Não Catalogado	Proprietário	Usuários	Risco	Observações
Vendas	Software de CRM pessoal	Representante de vendas	Equipe de vendas	Risco de perda de dados e falta de integração com sistemas oficiais	Utilizado para rastreamento de clientes individualmente
Marketing	Ferramentas de design online	Equipe de marketing	Designers e equipe de marketing	Risco de segurança e conformidade com dados pessoais	Ferramentas usadas para criar materiais rapidamente
RH	Planilhas de RH	Gerente de RH	Equipe de RH	Vulnerabilidade de dados sensíveis	Utilizado para acompanhamento de dados de colaboradores
Operações	Software de gestão de tarefas	Líder de operações	Equipe de operações	Falta de integração com sistemas de produtividade	Ferramenta pessoal usada para gestão de tarefas
Finanças	Ferramentas de análise de dados	Analista financeiro	Equipe financeira	Vazamento de dados financeiros	Utilizado para análises financeiras e projeções
Suporte Técnico	Ferramenta de controle remoto	Técnico de suporte	Equipe de suporte	Risco de acesso não autorizado	Utilizado para suporte rápido sem supervisão
Logística	Aplicativos de rastreamento	Coordenador de logística	Equipe de logística	Exposição de dados de localização e uso de redes não seguras	Usado para rastreamento de entregas por apps externos

Identificação de riscos físicos (acesso não autorizado, falhas ambientais) e lógicos (credenciais fracas, redes inseguras).

A tabela mapeia ativos de TI, destacando ameaças, como ataques DDoS, phishing e fuga de dados, e vulnerabilidades associadas, como configurações inadequadas, falta de atualizações e autenticação fraca. Aponta riscos em servidores, computadores, redes, serviços na nuvem, softwares e sistemas de controle de acesso. O objetivo é identificar falhas como credenciais fracas, protocolos obsoletos e ausência de segmentação de rede, além de propor melhorias para fortalecer a segurança e minimizar riscos cibernéticos.

Ativo	Ameaça	Vulnerabilidade
Servidores	Ataques de DDoS: Sobrecarga de servidores com tráfego, tornando-os indisponíveis. Malware/Ransomware: Software malicioso que pode comprometer dados e funcionalidades. Acesso não autorizado: Hackers podem explorar vulnerabilidades para obter acesso a dados sensíveis.	Configurações inadequadas: Configurações padrão ou mal configuradas podem ser exploradas. Falta de atualizações: Servidores desatualizados são vulneráveis a exploits conhecidos. Credenciais fracas: Senhas fracas ou não alteradas regularmente.
Computadores e Notebooks	Phishing: Obtém informações sensíveis por e-mails ou sites fraudulentos.	Falta de criptografia: Dados não criptografados são acessíveis se comprometidos.
	Spyware e Adware: Software coleta dados sem consentimento do usuário.	Software desatualizado: Sistemas e aplicativos antigos são vulneráveis.
	Roubo físico: Exposição de dados armazenados no dispositivo roubado.	Uso de redes inseguras: Conexões Wi-Fi públicas sem proteção adequada.
Infraestrutura de Rede	Intercepção de dados: Ataques MitM capturam dados em trânsito.	Configurações de firewall inadequadas: Permitem acessos não autorizados.
	Injeção de pacotes maliciosos: Explora a rede.	Falta de segmentação: Redes não segmentadas facilitam a propagação de ataques.
	Ataques de redirecionamento: Desvio de tráfego para servidores maliciosos.	Protocolos inseguros: Uso de protocolos obsoletos e inseguros.
Serviços de Nuvem	Fuga de dados: Acesso não autorizado a dados armazenados na nuvem.	Gerenciamento inadequado de credenciais: Senhas fracas ou compartilhadas.
	Configurações inadequadas: Exposição de dados devido a erros.	Controle inadequado de acesso: Falta de políticas rigorosas.
	Dependência de terceiros: Risco associado ao provedor de serviços.	Falta de criptografia: Dados não criptografados em trânsito ou armazenados.

Softwares	Exploração de vulnerabilidades: Falhas usadas para comprometer sistemas.	Código mal escrito: Bugs e falhas exploráveis.
	Backdoors: Acessos escondidos para entrada não autorizada.	Falta de atualizações: Software desatualizado é suscetível a exploits conhecidos.
	Trojan Horses: Software legítimo executando ações maliciosas.	Permissões excessivas: Aplicativos com permissões além do necessário.
Sistemas de Controle de Acesso	Bypassing: Técnicas para contornar sistemas de controle de acesso.	Autenticação fraca: Métodos de autenticação não robustos.
	Social Engineering: Manipulação de pessoas para obter acesso não autorizado.	Gestão inadequada de privilégios: Usuários com mais acesso do que o necessário.
	Credential Stuffing: Uso de credenciais roubadas.	Falta de monitoramento: Ausência de auditoria e monitoramento de acessos.

Desenvolvimento de uma política de segurança da informação com orientações para controle de acesso, confidencialidade e treinamento de colaboradores.

A política da Sabor do Campo tem como objetivo principal estabelecer diretrizes que assegurem a proteção e gestão de informações e ativos digitais. Por meio de requisitos e práticas abrangentes, a empresa busca criar um ambiente seguro e confiável para dados, sistemas e operações, alinhando-se a normas e padrões de segurança da informação.

Essa política é aplicável a todos os funcionários, prestadores de serviços, fornecedores e parceiros da Sabor do Campo, cobrindo todas as interações com informações e sistemas corporativos. O escopo abrange desde o uso adequado de dados pessoais e corporativos até a proteção de ativos digitais essenciais, atendendo às exigências de conformidade e proteção de dados.

Diretrizes Fundamentais de Segurança

A Sabor do Campo adota medidas rigorosas para garantir a confidencialidade, integridade e disponibilidade das informações. A confidencialidade é assegurada por criptografia, segregação de funções e monitoramento de acessos. A integridade é mantida por auditorias e controles que evitam alterações não autorizadas. A

disponibilidade é garantida por políticas de backup, redundância e recuperação de desastres, assegurando continuidade operacional mesmo em casos de falhas.

Gerenciamento e Controle de Acesso

O acesso a dados e sistemas é baseado nas funções de cada colaborador por meio do Controle de Acesso Baseado em Funções (RBAC), que é revisado periodicamente. Os sistemas contam com autenticação multifatorial (MFA), combinando senhas, tokens e biometria para reforçar a segurança. Além disso, permissões são concedidas apenas conforme a necessidade, e acessos são monitorados para evitar abusos.

Segurança Física e Proteção Ambiental

As instalações da Sabor do Campo possuem câmeras, controles de acesso e segurança 24/7, com restrições em áreas críticas como data centers. Sistemas de controle ambiental, como sensores de fumaça e procedimentos de emergência, mitigam riscos como incêndios e inundações, garantindo a proteção da infraestrutura e a continuidade das operações.

Segurança de Redes e Comunicações

A empresa utiliza firewalls, sistemas de prevenção de intrusão e segmentação de rede para proteger contra ameaças externas e internas. As redes são monitoradas continuamente para detectar padrões incomuns e responder a ameaças em tempo real, garantindo um ambiente digital seguro.

Gerenciamento e Resposta a Incidentes de Segurança

A equipe de segurança segue um plano estruturado de resposta a incidentes, cobrindo identificação, contenção e recuperação. Todos os incidentes são documentados e relatados para análise e melhoria contínua, com medidas preventivas implementadas para evitar recorrências.

Conscientização e Treinamento em Segurança

A Sabor do Campo promove campanhas educativas e treinamentos regulares para conscientizar os colaboradores sobre riscos e boas práticas de segurança. Os treinamentos são adaptados às funções de cada funcionário, incluindo prevenção de phishing, gestão de senhas e segurança digital.

Avaliação e Melhoria Contínua

Auditorias internas e externas avaliam a conformidade com as políticas de segurança. Políticas e procedimentos são revisados regularmente para alinhamento com as melhores práticas. Análises de risco identificam vulnerabilidades e guiam ações preventivas e corretivas, enquanto KPIs monitoram o desempenho das medidas de segurança.

Conformidade Legal e Regulatória

A Sabor do Campo cumpre rigorosamente a LGPD e normas internacionais, garantindo conformidade com regulamentações de privacidade e proteção de dados. Vulnerabilidades são gerenciadas e corrigidas por meio de atualizações regulares nos sistemas.

Política de Proibição de Dispositivos Pessoais para Atividades Corporativas

O uso de dispositivos pessoais (BYOD) para atividades corporativas é proibido devido aos riscos de segurança. Apenas dispositivos fornecidos pela empresa, configurados e monitorados pela equipe de TI, podem ser usados para acessar sistemas e dados. Exceções precisam de autorização formal e são revisadas periodicamente.

Papéis e Responsabilidades

A direção apoia e supervisiona as iniciativas de segurança, enquanto a equipe de segurança planeja, monitora e responde a incidentes. Todos os colaboradores têm o compromisso de seguir as políticas e relatar irregularidades para garantir a proteção dos dados e a segurança organizacional.

Conclusão

A implementação desta política reforça o compromisso da Sabor do Campo com a segurança da informação. O cumprimento das diretrizes e a colaboração de todos os envolvidos são fundamentais para proteger os dados e assegurar um ambiente corporativo confiável e seguro.

Resultados: Detectou-se que configurações inadequadas de servidores e ausência de segmentação de redes eram pontos críticos de falha. A política de segurança elaborada abordou essas questões, introduzindo práticas como o uso de autenticação multifatorial e proibição de dispositivos pessoais.

Etapa 3: Proposta de Soluções

Objetivo: Implementar soluções práticas para os problemas diagnosticados.

Atividades:

Proposta de uma nova arquitetura de segurança, com firewalls, VPNs e segmentação de redes.

A tabela mapeia o ciclo de vida dos dados de clientes e medidas de proteção. Dados são coletados via cadastro no site e processados (nome, e-mail, endereço e CPF validados no banco de dados). A saída é a criação de uma conta cadastrada. Identifica ameaças como vazamento de dados pessoais e uso de bots. Propõe soluções como criptografia (SSL) para proteger dados, CAPTCHA para evitar cadastros automáticos e autenticação multifator (MFA) para reforçar a segurança no acesso.

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).

Análise de custos, separando investimentos fixos (CAPEX) e despesas operacionais (OPEX).
As tabelas apresentam os custos relacionados à infraestrutura de TI, divididos em CAPEX (gastos de capital) e OPEX (gastos operacionais anuais).

CAP/EX

Inclui os investimentos iniciais em hardware, como um servidor Dell PowerEdge R360 (R$ 17.499), dois storages NAS Synology 6TB (R$ 6.600), um switch/roteador Ubiquiti UniFi (R$ 4.900) e um firewall Fortigate FG-40F (R$ 5.400). O total desses investimentos soma R$ 34.399.

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

Abrange despesas anuais como manutenção de hardware (R$ 15.000), energia elétrica (R$ 25.000), suporte técnico (R$ 17.000), atualizações de software (R$ 9.000) e armazenamento em nuvem AWS S3 10TB (R$ 16.383,57), totalizando R$ 82.383,57.

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				

Esses custos equilibram a infraestrutura física com serviços em nuvem para assegurar eficiência e segurança.

Criação de um plano de continuidade para garantir resiliência em caso de incidentes.

Resultados: A arquitetura implementada fortaleceu a proteção contra ataques cibernéticos, enquanto os backups regulares e os treinamentos de equipe aumentaram a resiliência da empresa.

III - Execução

Etapa 1: Levantamento Inicial

Entrevistas com equipes internas para identificar pontos de vulnerabilidade.

Análise das práticas atuais de proteção de dados.

Resultados: Foi mapeado que o processamento de pedidos online carecia de controles adequados, expondo a empresa a vazamentos de dados e ataques.

Etapa 2: Diagnóstico Detalhado

Desenvolvimento de fluxogramas detalhados para o processamento de pedidos.

Auditoria interna para catalogar itens de TI não controlados.

Proposta de treinamento para colaboradores.

Resultados: Identificou-se que 60% dos dispositivos utilizados não estavam configurados para segurança. A política de segurança começou a ser implementada nesta etapa.

Etapa 3: Proposta de Soluções

Configuração de firewalls Fortigate.

Implementação de backups em nuvem usando AWS.

Realização de workshops para conscientização sobre phishing.

Resultados: Mitigação de riscos como vazamento de dados e ataques de engenharia social.

IV - Conclusão

Este projeto representou um marco na segurança da informação da "Sabor do Campo", permitindo a identificação de vulnerabilidades críticas e a implementação de soluções eficazes para mitigar riscos. A elaboração de uma Política de Segurança da Informação, aliada à modernização da infraestrutura tecnológica e ao treinamento dos colaboradores, garantiu maior proteção dos dados, conformidade com legislações como a LGPD e resiliência operacional.

As melhorias realizadas fortaleceram a defesa contra ameaças cibernéticas, reduziram a exposição a incidentes de segurança e promoveram uma cultura organizacional voltada para a proteção de informações. Como resultado, a empresa está mais preparada

para atender às demandas do mercado, com operações mais seguras, confiáveis e alinhadas às melhores práticas.

A "Sabor do Campo" conclui este projeto mais segura e competitiva, com uma estrutura que não apenas resolve problemas imediatos, mas também sustenta seu crescimento futuro no ambiente digital. A segurança da informação, consolidada como prioridade estratégica, torna-se agora um diferencial que reforça a confiança de clientes e parceiros.

V – Anexos

Abaixo está o script desenvolvido em C#, para atender os requisitos da terceira etapa, item 4, onde foi solicitado a elaboração de um programa de inventário, listando hardware e softwares instalados em uma estação.

```
using System;
using System.Diagnostics;
using System.IO;

namespace InventarioComputador
{
    class Program
    {
        static void Main(string[] args)
        {
            while (true)
            {
                Console.Clear();
                Console.WriteLine("Escolha uma opção de inventário:");
                Console.WriteLine("1. Hardware");
                Console.WriteLine("2. Software");
                Console.WriteLine("3. Hardware e Software");
```

```
        Console.WriteLine("4. Sair");
        Console.Write("Digite o número da opção desejada: ");

        string opcao = Console.ReadLine();

        switch (opcao)
        {
            case "1":
                SalvarInventario("Hardware");
                break;
            case "2":
                SalvarInventario("Software");
                break;
            case "3":
                SalvarInventario("HardwareSoftware");
                break;
            case "4":
                Console.WriteLine("Saindo...");
                return;
            default:
                Console.WriteLine("Opção inválida. Tente novamente.");
                break;
        }

        Console.WriteLine("Pressione qualquer tecla para voltar ao menu...");
        Console.ReadKey();
    }
}
```

```
    static void SalvarInventario(string tipo)
    {
        string arquivo = "InventarioComputador.dat";
        string conteudoInventario = "";

        if (tipo == "Hardware" || tipo == "HardwareSoftware")
        {
            conteudoInventario += "=== Inventário de Hardware ===\n";
            conteudoInventario += ExecutarComandoPowerShell("Get-ComputerInfo");
            conteudoInventario += "\n";
        }

        if (tipo == "Software" || tipo == "HardwareSoftware")
        {
            conteudoInventario += "=== Inventário de Software ===\n";
            conteudoInventario += ExecutarComandoPowerShell("Get-WmiObject -
Class Win32_Product | Select-Object -Property Name,Version");
            conteudoInventario += "\n";
        }

        File.WriteAllText(arquivo, conteudoInventario);
        Console.WriteLine($"Inventário salvo em: {arquivo}");
    }

    static string ExecutarComandoPowerShell(string comando)
    {
        ProcessStartInfo psi = new ProcessStartInfo
        {
            FileName = "powershell.exe",
```

```
            Arguments = $"-Command \"{comando}\"",
            RedirectStandardOutput = true,
            UseShellExecute = false,
            CreateNoWindow = true
        };

        using (Process process = Process.Start(psi))
        {
            using (StreamReader reader = process.StandardOutput)
            {
                return reader.ReadToEnd();
            }
        }
    }
}
```