PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

PUC Minas Virtual

Felipe da Silva Rosa

Vinicius de Almeida Pitondo

João lucas Farias Camilo

AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO E DIAGNÓSTICO ORGANIZACIONAL DA PADARIA PÃO NOSSO:

um estudo de caso sobre processos e tecnologias de segurança na panificação

Belo Horizonte

Sumario:

Referências

- Fontes consultadas e dados coletados

A **Padaria Pão Nosso**, estabelecida em Jundiaí desde 2010, é uma empresa de médio porte que se especializa na produção de pães artesanais, bolos, doces e lanches. Com um forte compromisso com a qualidade dos ingredientes e o atendimento ao cliente, a padaria conta com aproximadamente 30 colaboradores e registra um faturamento médio mensal de R$ 150.000, com aumentos sazonais durante datas comemorativas. Seu objetivo estratégico é consolidar-se como uma referência no segmento de panificação na região, pautando-se por valores como excelência, respeito ao cliente e práticas sustentáveis.

3. DIAGNÓSTICO ORGANIZACIONAL

3.1 Histórico da Organização

a) Apresentação do Empreendimento:

Segmento: A Padaria Pão Nosso é uma padaria de médio porte, que oferece uma variedade de produtos como pães artesanais, bolos, doces e lanches rápidos. Atende principalmente moradores e trabalhadores da região de Jundiaí.

Tamanho: A padaria conta com cerca de 30 funcionários e possui uma área para produção, atendimento ao público e um pequeno espaço para consumo local.

Faturamento: O faturamento mensal gira em torno de R$ 150.000, com aumentos durante datas especiais como festas e feriados.

Histórico: A padaria foi fundada em 2010 por uma família de padeiros, com o objetivo de produzir pães de alta qualidade de forma artesanal. Com o tempo, a padaria ampliou seus produtos e modernizou sua estrutura, mas manteve o toque familiar.

Missão: Oferecer produtos frescos e de alta qualidade, preparados com ingredientes naturais, para proporcionar uma experiência diferenciada aos clientes.

Visão: Ser uma das padarias mais reconhecidas em Jundiaí pela excelência dos produtos e pelo atendimento.

Valores:

- Qualidade e frescor dos produtos
- Satisfação do cliente como prioridade
- Ética e respeito nas relações com colaboradores e fornecedores
- Uso sustentável dos recursos

A Padaria Pão Nosso se preocupa com a segurança das informações e possui um contrato com uma empresa prestadora de serviços para auxiliá-la na manutenção dos níveis básicos de segurança da informação. Embora não tenha um departamento de TI próprio, o gestor administrativo supervisiona essa área com o suporte dessa empresa especializada. A prestadora de serviços ajuda a garantir que medidas essenciais de segurança, como backups, controle de acesso e proteção contra ameaças, sejam implementadas. Apenas o gestor e um auxiliar têm acesso aos sistemas financeiros e de estoque, assegurando o controle e a proteção dos dados.

---

b) Segurança da Informação:

Na Padaria Pão Nosso, proteger as informações da empresa é uma prioridade. Embora não haja um setor exclusivo de TI, algumas medidas básicas já foram adotadas para manter os dados seguros.

Responsável: O gestor administrativo cuida da segurança digital, supervisionando os sistemas e o controle de dados.

Acesso: Apenas o gestor e um auxiliar administrativo têm acesso completo aos sistemas financeiros e de controle de estoque.

Processos: A padaria usa um sistema integrado que controla o estoque, as finanças e emite notas fiscais eletrônicas.

---

c) Problemas de Segurança Relatados:

O gestor identificou os seguintes problemas de segurança:

- **Acesso Não Autorizado**: Tentativas de acesso ao sistema por meio de senhas fracas.
- **Phishing**: E-mails falsos que tentam roubar informações dos funcionários.
- **Backup Inadequado**: Falhas em cópias de segurança dos dados financeiros, causando risco de perda de dados importantes.

d) Medidas de Segurança Utilizadas:

Para resolver os problemas, a padaria implementou:

- **Firewall e Antivírus**: Protegem os computadores da rede contra ataques.
- **Backups Automáticos**: O sistema agora faz cópias de segurança dos dados na nuvem, para evitar perdas.
- **Treinamento**: Os funcionários foram orientados a usar e-mails e senhas com mais segurança, evitando riscos desnecessários.

---

e) Processos da Padaria:

A padaria segue processos claros para manter a qualidade dos produtos e a eficiência:

- **Produção**: O preparo dos pães é feito conforme uma programação diária, garantindo que estejam sempre frescos.
- **Atendimento**: A equipe de atendimento é treinada para ser cordial e eficiente com os clientes.

- **Gestão de Estoque**: O controle dos ingredientes é feito por um sistema que monitora o que entra e sai, evitando desperdícios.
- **Financeiro**: O faturamento diário é registrado e o sistema emite relatórios mensais para acompanhar o desempenho da padaria.

---

f) Segurança dos Dados (Disponibilidade, Integridade e Confidencialidade):

- **Disponibilidade**: O sistema da padaria funciona na maior parte do tempo, com poucas interrupções. Se houver problemas, a padaria conta com suporte técnico.
- **Integridade**: Os dados são mantidos precisos, com backups feitos regularmente, embora já tenham ocorrido falhas que precisam ser melhor monitoradas.
- **Confidencialidade**: Apenas o gestor administrativo tem acesso completo aos dados mais sensíveis da empresa, e o acesso dos outros funcionários é limitado conforme necessário.

Sistemas de Informação identificados na empresa

Software	Setor	Descrição
Sistema de Gestão Integrada (ERP)	Administração	Integra diversas áreas da padaria, como financeiro, estoque, vendas e recursos humanos, facilitando a gestão centralizada das operações.
Ponto de Venda (PDV)	Vendas	Sistema utilizado no atendimento ao cliente para

		registrar vendas, processar pagamentos e emitir recibos. Também gera relatórios de vendas diárias.
Controle de Estoque	Produção/Compras	Gerencia o estoque de insumos e produtos acabados, controlando entradas e saídas, prevenindo desperdícios e garantindo a disponibilidade de materiais.
Sistema Financeiro	Financeiro	Responsável pelo controle das finanças da padaria, incluindo contas a pagar e a receber, fluxo de caixa, e geração de relatórios financeiros mensais.
Backup em Nuvem	TI (terceirizado) Administração	Serviço de backup automático que armazena dados críticos da empresa na nuvem, garantindo a segurança e a recuperação rápida em caso de perda de dados.
Sistema de Gestão de Encomendas	Atendimento/Produção	Gerencia as encomendas feitas para festas e eventos, acompanhando o status de produção, prazos de entrega e personalizações solicitadas pelos clientes.
Sistema de Recursos Humanos (RH)	Recursos Humanos	Gerencia informações sobre os funcionários, como cadastro, folhas de

		pagamento, controle de ponto e benefícios, além de facilitar a comunicação interna.
Sistema de Marketing Digital	Marketing	Ferramenta utilizada para gerenciar campanhas de marketing online, redes sociais, e-mails promocionais e análise de desempenho das estratégias de marketing.
Sistema de Segurança (Firewall e Antivírus)	TI (terceirizado) Administração	Protege a infraestrutura de TI contra ameaças externas, como vírus, malware e tentativas de acesso não autorizado, garantindo a integridade e a confidencialidade dos dados.

Fonte: Gerente da Padaria Pão Nosso e Gestor Financeiro (2024)

MODELAGEM DO PROCESSO DE NEGÓCIO

Mapeamento dos processos atuais/existentes da empresa (foco em segurança da informação)

A Panificadora Pão Nosso trabalha com processos simples voltados para produção, vendas e gestão financeira. No entanto, a segurança dos dados não recebe muita atenção e há algumas fragilidades que precisam ser corrigidas.

Processos atuais:

- Pedidos: Os clientes fazem pedidos diretamente no balcão e o operador registra.
- Dados financeiros: São gerenciados em um sistema básico de computador (ERP).
- Dados de clientes: Apenas o nome e preferências são guardados, sem muitos detalhes.
- Backups: São feitos manualmente uma vez por semana, em discos externos.
- Equipamentos: Usam computadores antigos,programas simples de antivírus.

Relatórios e notas fiscais:

- Relatórios financeiros: São feitos periodicamente para controle.

- Notas fiscais: São impressas e entregues aos clientes na hora.

Segurança da informação:

- A padaria tem pouca proteção dos dados, usando apenas backups semanais e trocando senhas de vez em quando. Isso significa que há riscos de perder informações ou sofrer invasões.

A **Panificadora Pão Nosso** mantém seus processos de forma básica, focados nas atividades essenciais como produção, vendas e controle financeiro. No entanto, a segurança da informação é tratada de maneira limitada, apresentando pontos vulneráveis que precisam de melhorias.

Processos atuais identificados:

Entrada de informações:

- Pedidos: Realizados manualmente na padaria.
- Dados financeiros: Gerenciados por um sistema simples (ERP).
- Dados de clientes: Armazenados apenas com nome e algumas preferências, sem muitos detalhes.
- Backups: Feitos manualmente em HDs externos, uma vez por semana.
- Recursos: Uso de computadores antigos e internet pública, com softwares básicos de antivírus.

Saídas de informações:

Relatórios financeiros: Gerados regularmente para controle da padaria.

Comprovantes de venda e notas fiscais: Impressos diretamente no local após as compras.

Recursos utilizados:

- Hardwares: Computadores e impressoras simples conectados à rede.

- Softwares: Sistema ERP básico para gerenciar finanças e estoque, com pouca proteção para os dados.
- Pessoal: Um técnico de TI realiza a manutenção dos sistemas e backups, e os operadores de caixa cuidam das operações diárias.

Sequência de atividades:

- **Entrada dos pedidos:** Clientes fazem pedidos diretamente no balcão.
- **Processamento do pedido:** O operador registra o pedido e o pagamento no sistema.
- **Emissão da nota fiscal:** O sistema emite a nota que é entregue ao cliente.
- **Backup semanal:** Os dados são manualmente copiados para HDs externos.
- **Fechamento financeiro:** Relatórios são gerados no final de semana para controle financeiro.
- **Foco em segurança da informação:** Atualmente, as práticas de segurança são limitadas, como a troca ocasional de senhas e backups manuais. Não há uma proteção robusta para garantir a confidencialidade e integridade dos dados, expondo a empresa a riscos de perda ou vazamento de informações.

Mapeamento da proposta de processos da empresa (foco em segurança da informação)

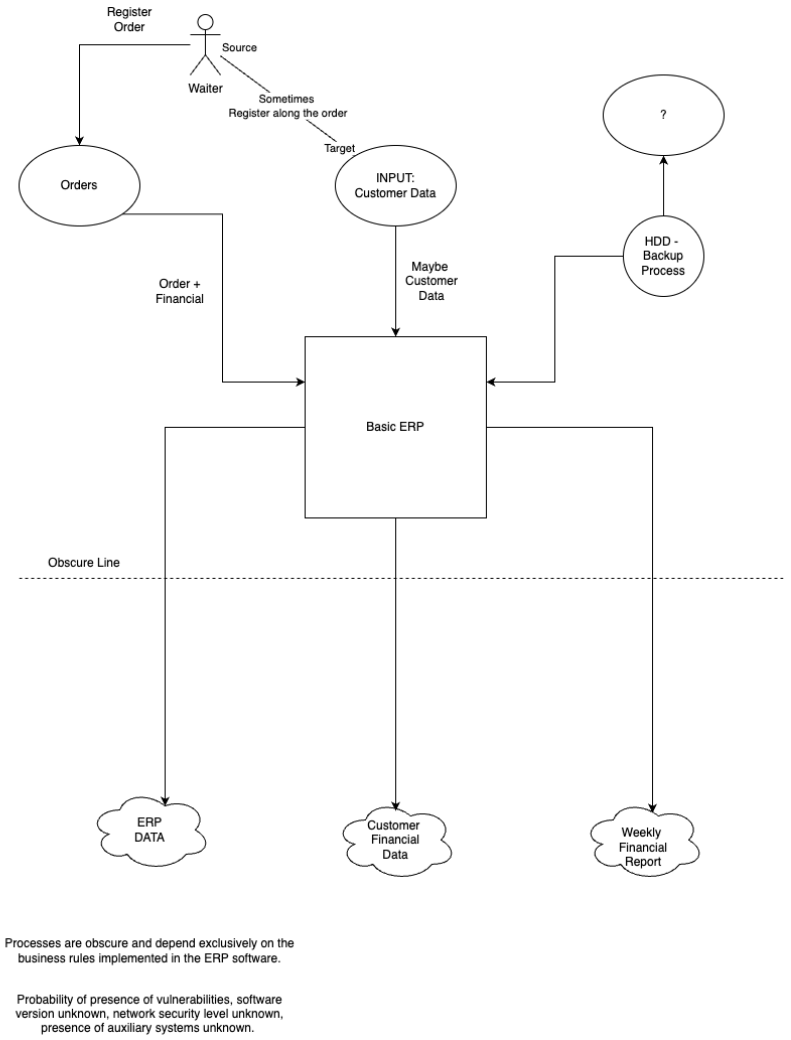
Proposta de otimização:

Para melhorar a segurança da informação, é necessário implementar um plano estratégico que aborde a gestão de dados de forma mais eficaz, introduzindo controles mais rigorosos e automações que garantam a integridade e proteção das informações da padaria.

Identificação de etapas redundantes e gargalos:

- **Gargalo: Backup manual** – O processo de backup feito manualmente em HDDs externos gera atraso e dependência humana, além de estar suscetível a falhas de execução.
- **Gargalo: Uso de rede pública** – A utilização de uma rede pública de internet para o gerenciamento das atividades internas é um ponto crítico que aumenta a vulnerabilidade.

- **Gargalo: Segurança de dados** – Não há controle adequado de acesso e proteção de dados financeiros e de clientes, o que deixa a empresa exposta a ataques.



Fonte: Elaborado pelos autores (2024)

Baseado na análise do contexto do negócio, identifica-se a necessidade urgente de um melhor entendimento de todos os processos internos, de auditoria nos softwares que são utilizados, de acompanhamento das rotinas de todos os processos envolvendo dados, afim de trazer transparência em relação as mesmo e eventualmente auxiliar no processo de identificação, prevenção, contenção e recuperação de acidentes.

Automatização de backups:

A padaria pode adotar um sistema de backup automático na nuvem. Isso significa que os dados importantes serão copiados para um local seguro na internet sem a necessidade de intervenção humana, garantindo que nada seja perdido em caso de falha.

Criação de uma rede dedicada:

Para aumentar a segurança, é recomendado instalar uma rede de internet exclusiva para os processos internos da padaria. Usar uma VPN (rede privada virtual) ajuda a proteger as informações que trafegam pela rede, impedindo que pessoas de fora acessem esses dados.

Implementação de firewall e antivírus avançados:

Em vez de utilizar um antivírus básico, a padaria deve adotar soluções de segurança mais robustas. Um firewall ajudará a bloquear acessos indesejados à rede, filtrando quem pode entrar ou sair dela, protegendo melhor o sistema.

Gerenciamento de acesso:

A padaria pode implementar um sistema onde apenas pessoas autorizadas possam acessar dados sensíveis, como informações financeiras. Isso significa que apenas o gerente e pessoas específicas poderão ver ou modificar esses dados, evitando que funcionários sem permissão tenham acesso.

Auditoria e monitoramento:

Monitorar constantemente quem acessa os sistemas e realizar auditorias periódicas para verificar se as regras de segurança estão sendo seguidas é essencial. Isso ajuda a detectar qualquer tentativa de acesso indevido e resolver o problema rapidamente.

Certificações e normas recomendadas:

- **ISO 27001:** Ajuda a padaria a organizar a segurança da informação, estabelecendo políticas e medidas para proteger todos os dados.
- **ISO 27002:** Reforça a padaria a seguir boas práticas de segurança, como controlar quem acessa as informações e monitorar os sistemas.
- **ISO 27005:** Ensina como identificar e gerenciar riscos, evitando problemas antes que aconteçam.
- **LGPD:** A padaria precisa proteger os dados pessoais dos clientes e funcionários, de acordo com a Lei Geral de Proteção de Dados.

Processos de auditoria:

Auditorias devem ser feitas periodicamente para garantir que as normas de segurança estão sendo seguidas. O monitoramento constante das redes e sistemas identifica falhas e corrige problemas antes que causem prejuízos.

Avaliação das normas de segurança da empresa:

A Panificadora Pão Nosso utiliza práticas básicas de segurança da informação para proteger seus dados físicos e digitais, especialmente os dados sensíveis dos clientes e as informações financeiras internas.

Normas de segurança identificadas:

- **LGPD (Lei Geral de Proteção de Dados):** A lei que protege os dados pessoais dos clientes e funcionários.

- **ISO 27001:** Sistema de Gestão de Segurança da Informação, garantindo que os dados estejam sempre seguros.
- **ISO 27002:** Boas práticas para proteger sistemas e dados de TI.
- **ISO 27005:** Normas para mapear e gerenciar os riscos de segurança da informação.

Detalhamento do mapeamento de riscos de segurança da informação:

A Panificadora Pão Nosso foca na segurança tanto física quanto digital para manter as operações funcionando com proteção contra falhas e ataques externos. A utilização de internet pública para algumas atividades internas requer maior atenção contra ameaças externas.

Segurança física da rede: Equipamentos de TI estão em locais restritos, protegidos por câmeras de vigilância e controles de acesso, impedindo que pessoas não autorizadas acessem áreas sensíveis.

Plano de contingência: O plano atual prevê o backup de dados e a duplicação de atividades críticas, como emissão de notas fiscais. No entanto, é preciso melhorar a capacidade de recuperação em caso de falha da internet pública.

Tipo de controle:

Tipo de controle	Descrição	Responsável
Softwares	Sistemas de gestão de vendas e financeiro baseados em planilhas e um sistema ERP simples, que gerencia a parte financeira e de estoque.	Técnico em informática responsável pelo TI.

	Softwares de proteção de dados são limitados a antivírus básico.	
Hardwares	Desktops antigos, roteadores comuns (domésticos) e impressoras conectadas à rede. Equipamentos de backup são HDDs externos que são atualizados semanalmente.	Equipe de TI e gerência.
Processos de operação de computador	Sistemas de controle de caixa e emissão de notas fiscais são operados em computadores locais. Os acessos a esses sistemas são controlados por senhas simples.	Técnico em informática e operadores de caixa.
Outros relatos	As senhas dos sistemas não seguem boas práticas de segurança (senhas fortes e únicas), sendo uma área a ser melhorada. O acesso à internet da padaria é feito via uma rede pública, o que aumenta a vulnerabilidade aos ataques.	Técnico de TI e gerente operacional.

Análise de risco:

Tipo de exposição	Probabilidade de ocorrência	Estimativa de prejuízo (mensa/anual)
Softwares	Média (uso de sistemas de ERP não atualizados e antivírus básico)	Prejuízo anual estimado em até R$ 10.000, considerando perda de dados de vendas e estoque.
Hardwares	Alta (uso de equipamentos antigos e falta de redundância em sistemas críticos)	Prejuízo anual estimado em até R$ 20.000, considerando falhas nos sistemas de gestão ou impressão de notas fiscais.
Processos de operação de computador	Média (uso de senhas fracas e práticas de segurança inadequadas)	Prejuízo mensal de até R$ 5.000, caso ocorra comprometimento de dados de clientes ou de sistemas internos.
Outros relatos	Alta (uso de rede pública e ausência de criptografia nos dados transmitidos)	Prejuízo potencial de até R$ 50.000, caso haja comprometimento de dados financeiros e de clientes.