PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Segurança da Informação

Gabriele Gonçalves de Azevedo

Gabriella de Oliveira Rodrigues

Gustavo Henrique Valeriano de Brito

Matheus Campos Madeira

**PROJETO: FUNDAMENTOS DE SISTEMAS – O Gaulês**

Belo Horizonte

2024

Gabriele Gonçalves de Azevedo

Gabriella de Oliveira Rodrigues

Gustavo Henrique Valeriano de Brito

Matheus Campos Madeira

**PROJETO: FUNDAMENTOS DE SISTEMAS – O Gaulês**

Projeto apresentado à disciplina de Fundamentos de Sistemas do curso de Segurança da Informação da Pontifícia Universidade Católica de Minas Gerais como parte do processo avaliativo.

Orientador: Fábio Leandro Rodrigues Cordeiro

Belo Horizonte

2024

Sumário

[ETAPA 1 4](#_Toc184594113)

[1 Equipe de trabalho 4](#_Toc184594114)

[2 Compreendendo a organização 4](#_Toc184594115)

[3 O negócio 5](#_Toc184594116)

[4 Os principais processos de negócios 5](#_Toc184594117)

[5 Leis e normas relacionadas a TI que impactam o negócio 7](#_Toc184594118)

[6 Matriz de relacionamento de processos organizacionais e leis. 9](#_Toc184594119)

[ETAPA 2 10](#_Toc184594120)

[7 Escolher 1 processo de negócio entre os que foram identificados na etapa 1 e detalhá-lo usando uma ferramenta de construção de fluxograma. 10](#_Toc184594121)

[8 Identificar os componentes suscetíveis a eventos de segurança da informação que fazem parte do processo de negócio escolhido vistos no MF de Fundamentos de Segurança. 11](#_Toc184594122)

[9 Mapear itens relacionados à TI invisível na organização. 11](#_Toc184594123)

[10 Identificar dispositivos pessoais utilizados na organização. 13](#_Toc184594124)

[11 Identificar riscos de segurança física e lógica discutidos no MF de Fundamentos de Segurança da Informação e encontrados no contexto organizacional estudado. 15](#_Toc184594125)

[ETAPA 3 15](#_Toc184594126)

[3.1 Construir um modelo de sistema de informação (no formato de um quadro) que atenda ao processo escolhido no item 1 da etapa 2 apresentando ameaças/vulnerabilidades e proposta de solução. 16](#_Toc184594127)

[3.2 Definir Hardware de servidor completo para atender ao modelo de sistema de informação construído no item 1, justificando cada escolha e mostrando o CAPEX e OPEX. 19](#_Toc184594128)

[3.3 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: (em anexo). 20](#_Toc184594129)

[3.4 Realizar uma análise de riscos/continuidade/contingência dos itens de segurança física e lógica encontrados no item 5 da etapa 2. 20](#_Toc184594130)

[Anexo dos Scripts e Protótipo navegável 27](#_Toc184594131)

[Referências Bibliográficas 31](#_Toc184594132)

[Anexo PSI e NORMAS 32](#_Toc184594133)

# ETAPA 1

Conhecimento da legislação de segurança da informação

# Equipe de trabalho

* Gabriele Gonçalves de Azevedo – 873248
* Gabriella de Oliveira Rodrigues- 873926
* Gustavo Henrique Valeriano de Brito – 870282
* Matheus Campos Madeira – 870263

# Compreendendo a organização

Menelick, o homem por trás do restaurante O Gaulês, é filho de um veterinário e de uma mãe dedicada ao lar. Ele viu sua vida desmoronar ainda na infância, quando seu pai abandonou a família por conta de um caso extraconjugal. Esse evento foi um divisor de águas e se tornou determinante na trajetória do empreendedor.

O restaurante“O Gaulês” foi fundado em 1999, em Belo Horizonte (BH), e reflete a trajetória e o espírito inovador do empresário. A ideia para o empreendimento surgiu após o sucesso de seu primeiro negócio, uma hamburgueria icônica da região chamada Druida. O projeto se consolidou em uma casa alugada e reformada que ficava em frente à própria hamburgueria. Os nomes da hamburgueria e do restaurante fazem referência à tribo gaulesa mencionada nos quadrinhos Asterix, unificando conceitualmente os dois negócios.

Especializado em comida brasileira à la carte, pizzas, porções e sobremesas, o restaurante tornou-se um ponto de referência em BH, destacando-se pela qualidade e pela experiência gastronômica oferecida aos clientes. Ao longo dos anos, O Gaulês recebeu chefs renomados e participou de eventos importantes, o que ajudou a consolidar sua reputação no cenário gastronômico local.

**Missão**

Nossa missão é criar experiências memoráveis que reúnem amigos e familiares ao redor da mesa, oferecendo pratos deliciosos, preparados com amor, que nutrem tanto o corpo quanto o espírito. Acreditamos que a comida é o elo que fortalece laços, celebra momentos especiais e traz calor e alegria a cada encontro  
**Visão**

Queremos ser o restaurante mais acolhedor do Brasil ao proporcionar para os nossos clientes a experiência de estarem em casa.

**Valores**

Fraternidade, Lealdade, Altruísmo.

# O negócio

* **O Gaulês** atua como restaurante especializado em comida brasileira à la carte, pizzas, porções e sobremesas. Receitas e molhos com fabricações próprias que se estendem a anos.
* Faz venda de comida brasileira, pizza, porções, drinks e sobremesas no próprio local, por delivery e pelo Ifood.

# Os principais processos de negócios

**Os processos podem ser agrupados em**:

* Processos Financeiros e Contábeis:
* Processos de Vendas e Marketing:
* Processos de Manufatura e Produção:
* Processos de Recursos Humanos:

Dentro destes grupos temos os seguintes detalhamentos:

* **Processos Financeiros e Contábeis:**
* contas a pagar:
* Insumos: R$200.000
* Funcionários: R$150.000
* Despesas eventuais: R$10.000
* gerenciamento e previsão de caixa: A previsão de fluxo de caixa permite que gestores enxerguem a saúde financeira futura da empresa, ajudando-os a tomar decisões informadas sobre investimentos, despesas, e gestão de recursos.
* contabilidade de custos de produto: Calcular o custo individual e cada produtos e serviços.
* contabilidade tributária: fazer o cálculo de imposto total do estabelecimento.
* gerenciamento relatórios financeiros: Detalha a situação financeira ao longo de um período, detalhando receitas, despesas e lucro ou prejuízo; entrada e saída de dinheiro, ajudando a entender a gestão do caixa
* Faturamento bruto: R$500.000
* **Processos de Vendas e Marketing:**
* processamento de pedidos, cotações e contratos
* configuração de produtos
* determinação de preço
* Faturamento, ticket médio de vendas no valor de R$150,00.
* gerenciamento de comissão, incentivos e planejamento de vendas.
* Atendimento ao cliente personalizado para melhor atendê-lo.
* Desenvolvimento de promoções:
* As terças-feiras com rodadas de chopp em dobro.
* Promoções dos pratos especiais no delivery.
* Sobremesa da casa para aniversariantes
* Desconto de 10% para reservas acima de 10 pessoas no almoço executivo, durante a semana.
* Divulgação, vídeos e fotos toda semana nas redes sociais dos pratos, saladas, bebidas e sobremesas.
* **Processos de Manufatura e Produção:**
* seleção de fornecedores: selecionar os melhores fornecedores de alimentos e bebidas.
* gestão de estoque: controle de armazenamento de insumos, levantamento do que entrou e saiu em produção, bebidas, pizzas, pratos e petiscos.
* Compras:
* Expedição: saída/vendas de pratos para delivery, sobremesas, drinks e sucos naturais.
* planejamento e programação de produção: feito semanalmente baseado no ticket médio de vendas; abrindo uma margem maior em determinadas datas de maior movimento.
* planejamento da necessidade de materiais: feito semanalmente baseado no ticket médio de vendas; abrindo uma margem maior em determinadas datas de maior movimento.
* controle de qualidade: controlar a qualidade dos pratos e drinks etc.
* controle de fornecedor: pesquisa de fornecedor com melhor qualidade e preço.
* Produção de insumos: produzir os demais alimentos que serão consumidos no restaurante.
* manutenção do delivery: atualizar todos os dias o aplicativo sobre os produtos de venda do dia para não gerar insatisfação aos clientes.
* fluxo de expedição: conferência de produtos embalados, despacho e entrega dos pedidos.
* **Processos de Recursos Humanos:**
* Todos os processos são feitos pelo dono: alocação de colaboradores, processos burocráticos, comunicação interna, folha de pagamento, demissões.
* Recrutamento e seleção: Encontrar os melhores perfis de pessoas, para cada cargo, com conhecimentos, habilidades e perfil de acordo com a empresa.
* Gestão de remuneração e benefícios: Gerir os salários e os benefícios dos funcionários.
* Planejamento: Prevenir erros, eliminar problemas e aproveitar o talento dos funcionários.

# Leis e normas relacionadas a TI que impactam o negócio

|  |  |
| --- | --- |
| **Leis e Normas** | **Impacto na organização** |
| Lei Geral de Proteção de Dados (LGPD) | Controle rigoroso para garantia da privacidade e tratamento dos dados sensíveis de pessoas físicas tanto de clientes pelo aplicativo próprio e de plataformas terceirizadas, quanto funcionários como informações de pagamentos, salários, atestados e etc. Acesso restrito a dados sensíveis, somente pela equipe responsável, e implementação de soluções para rastreamento, gestão e exclusão de dados pessoais conforme necessidade. |
| Marco Civil | O Marco Civil da Internet estabelece uma série de direitos e responsabilidades para o uso da rede, com ênfase na proteção da privacidade dos usuários e na neutralidade da rede. Para o restaurante Gaulês, isso significa adotar práticas transparentes na coleta, no armazenamento e no uso dos dados pessoais de seus clientes, assegurando que apenas as informações essenciais sejam obtidas e que isso ocorra conforme previamente informado. Também é crucial garantir a neutralidade e a responsabilidade no fornecimento de internet, como no caso do Wi-Fi oferecido aos clientes do restaurante, assim como no uso do aplicativo próprio do restaurante. Para utilizar esses serviços, é necessário que os clientes realizem um cadastro. |
| Lei de Crimes Cibernéticos (Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann" | Implementação de medidas de segurança para proteger o sistema de TI do restaurante contra invasões, ataques cibernéticos e uso não autorizado de dados. O Gaulês deve estar ciente de que qualquer violação da segurança que resulte em dano aos clientes pode resultar em penalidades criminais. |
| ISO 27001 | Implementação de um Sistema de Gestão de Segurança da Informação que assegura a confidencialidade, integridade e disponibilidade das informações. A adoção dessa norma ajuda a proteger as informações do restaurante contra ameaças, como ciberataques, vazamento de dados e garante a continuidade dos processos e negócio. |
| ISO 27002 | Aplicação de boas práticas para a implementação de controles de segurança da informação. A ISO 27002 fornece diretrizes para a seleção e implementação de controles, o que ajuda a reforçar a segurança da infraestrutura de TI do restaurante e a proteção dos dados dos clientes. |
| ISO 27005 | Foco no gerenciamento de riscos de segurança da informação. Sua implementação ajuda a identificar, analisar e mitigar os riscos relacionados aos dados e sistemas do Gaulês. O restaurante pode avaliar de forma proativa as ameaças e vulnerabilidades que podem impactar a confidencialidade, integridade e disponibilidade das informações. A norma apoia na criação de planos de mitigação, resposta e recuperação, garantindo a continuidade dos negócios e a proteção dos dados dos clientes e funcionários contra violações de segurança. |

# Matriz de relacionamento de processos organizacionais e leis.

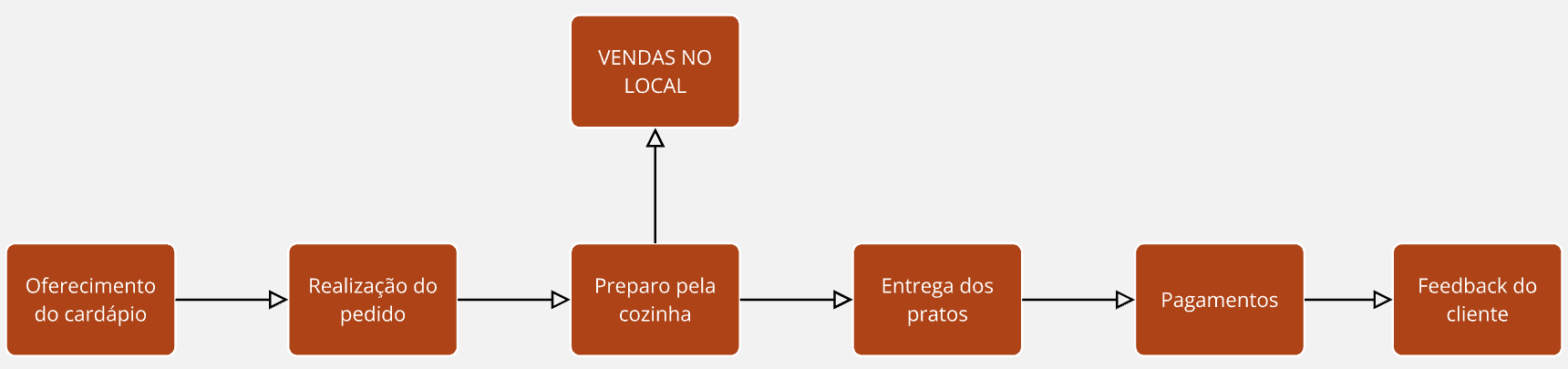
|  |  |
| --- | --- |
| **Processo** | **Leis e normas a serem observadas** |
| Processos de Vendas e Marketing | **Marco Civil da Internet, LGPD**: Observar o consentimento informado para o uso dos dados dos clientes em campanhas de marketing, evitando o envio de comunicação não solicitada via e-mail, WhatsApp e SMS, além de políticas de privacidade nas interações e controle de acessos e utilização do aplicativo próprio do Gaulês. |
| Processos Financeiros e Contábeis | **Lei de Crimes Cibernéticos, LGPD, ISO 27001, ISO 27002, ISO 27005**: Implementação de medidas de segurança para proteção dos dados financeiros dos clientes, fornecedores e funcionários, como transações de pagamento, salários, formas de pagamentos e outros tipos de dados financeiros. |
| Processos Manufatura e Produção | **ISO 27001, ISO 27002, ISO 27005**: Implementação de políticas de segurança e garantia da confidencialidade, integridade e disponibilidade dos dados de produção e manufatura do restaurante, categorizando somente como uso interno restrito ao Gaulês, além disso, implementação do gerenciamento de riscos de segurança da informação para identificar, analisar e mitigar os riscos relacionados aos dados dos processos de manufatura e produção do restaurante. |
| Recursos Humanos | **LGPD, ISO 27001, ISO 27002, ISO 27005**: Proteção de dados de funcionários como folha de pagamento, documentos, informações pessoais e avaliações de desempenho, garantindo que apenas pessoal autorizado tenha acesso. |

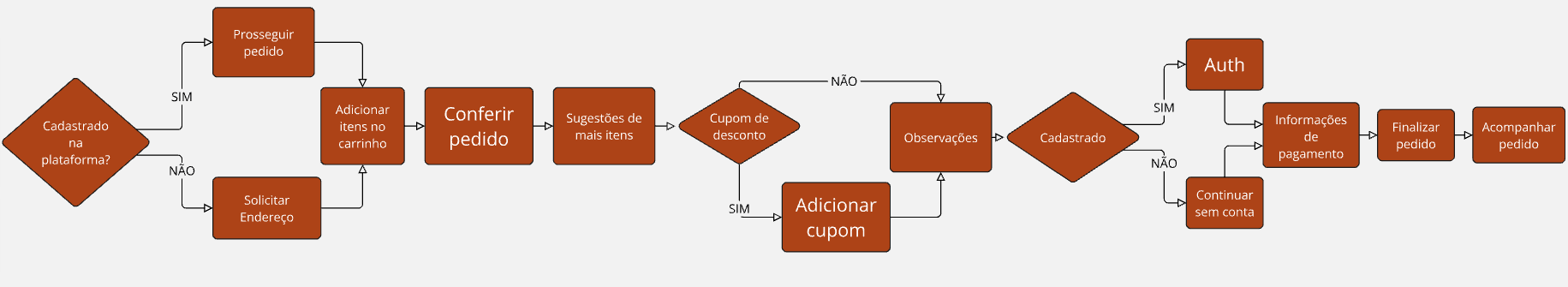
# ETAPA 2

Projeto fundamentos de sistemas

# Escolher 1 processo de negócio entre os que foram identificados na etapa 1 e detalhá-lo usando uma ferramenta de construção de fluxograma.

**Vendas**





Link para acesso ao fluxograma:

<https://miro.com/app/board/uXjVLY0PwDc=/?share_link_id=419408362836>

# Identificar os componentes suscetíveis a eventos de segurança da informação que fazem parte do processo de negócio escolhido vistos no MF de Fundamentos de Segurança.

No processo de vendas online por aplicativo, os componentes suscetíveis a eventos de segurança da informação incluem:

* **Dados do Cliente:** Informações pessoais e financeiras, como nome, endereço, e dados de cartão de crédito, que podem ser alvo de vazamentos ou roubo.
* **Plataforma de E-commerce:** Vulnerabilidades no software da loja virtual, incluindo plugins e temas desatualizados, que podem ser exploradas por hackers.
* **Conexões de Rede:** Redes Wi-Fi inseguras ou falta de criptografia durante a transmissão de dados podem permitir interceptação.
* **Processamento de Pagamentos:** Sistemas de pagamento que não estão devidamente protegidos, expondo transações a fraudes.
* **Armazenamento de Dados:** Bases de dados que não possuem segurança adequada, como criptografia e controle de acesso.
* **Autenticação de Usuários:** Falhas em sistemas de login e autenticação que podem permitir acesso não autorizado.
* **E-mails e Comunicação:** Phishing e outras técnicas que visam enganar usuários para obter informações sensíveis.
* **Atividades de Marketing:** Campanhas que envolvem coleta de dados podem ser vulneráveis a abusos e vazamentos.

Proteger esses componentes é essencial para garantir a segurança e a confiança dos clientes no processo de vendas online.

# Mapear itens relacionados à TI invisível na organização.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Setor** | **Item de TI não catalogado** | **Proprietário** | **Usuários** | **Risco** | **Obs.** |
| Vendas | WhatsApp (para comunicação com clientes) | Equipe de vendas | |  | | --- | | vendas | | Representantes comerciais | | Vazamento de dados de clientes; falta de controle de informação | Utilizado para agilizar respostas a pedidos e orçamentos |
| Marketing | Trello (gestão de campanhas) | Gerente de Marketing | Equipe de marketing | Perda de controle de dados; falha na integração com sistemas oficiais | Sem integração com CRM oficial da empresa |
| Produção | Planilhas do Google Sheets (controle de produção) | Supervisores de Produção | Equipe de chão de fábrica | Perda de dados críticos; falta de backup na rede corporativa | Dados armazenados na nuvem fora dos sistemas internos |
| Logística | |  | | --- | |  | | Google Maps (para planejamento de rotas) | | Coordenador de Logística | Motoristas e coordenadores de entrega | Inconsistência nas rotas; falta de monitoramento em tempo real | Usado para traçar rotas, mas sem integração com sistema de rastreamento oficial |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Risco** | **Probabilidade** | **Impacto** | **Classificação** | **Mitigação** | **Plano de Continuidade** | **Responsável** | **Prazo** |
| Falta de energia elétrica | Média | Alta | Crítico | Manutenção elétrica preventiva e gerador | Usar gerador para equipamentos essenciais | Gerente de Operações | Em 30 dias |
| Falta de ingredientes essenciais | Alta | Alta | Crítico | Fornecedores alternativos e estoque mínimo | Adaptação do menu com itens disponíveis | Chefe de Cozinha | Em 15 dias |
| Problemas de higiene e saúde | Baixa | Alta | Crítico | Treinamento em higiene e inspeções regulares | Correção imediata e comunicação aos clientes | Supervisor de Qualidade | Imediato |
| Greve ou falta de funcionários | Média | Alta | Crítico | Lista de freelancers e retenção de talentos | Reduzir horário ou menu temporariamente | Gerente de RH | Em 20 dias |
| Equipamentos quebrados | Alta | Média | Moderado | Manutenção preventiva e assistência técnica | Usar equipamentos reservas ou alugar temporariamente | Gerente de Operações | Em 7 dias |
| Reclamações de clientes (online) | Média | Média | Moderado | Monitoramento de redes e respostas rápidas | Implementar melhorias e comunicar clientes | Equipe de Marketing | Em 3 dias |
| Incêndio na cozinha | Baixa | Alta | Crítico | Extintores, treinamentos e inspeções frequentes | Evacuação, uso de extintores e inspeções | Gerente Geral | Imediato |

# Identificar dispositivos pessoais utilizados na organização.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Setor** | **Dispositivo** | **Proprietário** | **Usuários** | **Risco** | **Obs.** |
| Vendas | Smartphone pessoal | Analista de Vendas | Funcionário de Vendas | Vazamento de dados sensíveis de vendas para clientes | Aplicar política de criptografia de dados, autenticação de múltiplos fatores e restringir acesso a dados sensíveis pelo dispositivo |
| Financeiros e Contábeis | Notebook pessoal | Contador | Funcionário da Financeira e Contábil | Vazamento de dados financeiros, fraude ou roubo de informações | Aplicar política de criptografia de dados, autenticação de múltiplos fatores |
| Manufatura e Produção | Smartphone pessoal | Supervisor de Produção | Funcionário da Manufatura e Produção | Vazamento de dados operacionais e de produção | Aplicar política de criptografia de dados, autenticação de múltiplos fatores e restringir acesso a dados sensíveis pelo dispositivo |
| Recursos Humanos | Notebook pessoal | Analista de RH | Funcionário do RH | Vazamento de dados pessoais e confidenciais dos funcionários | Aplicar política de criptografia de dados, autenticação de múltiplos fatores |

# Identificar riscos de segurança física e lógica discutidos no MF de Fundamentos de Segurança da Informação e encontrados no contexto organizacional estudado.

|  |  |  |
| --- | --- | --- |
| **Ativo** | **Ameaça** | **Vulnerabilidade** |
| Lógico | Intrusão a Rede Wi-Fi | Senha fraca, falta de criptografia, e Firewall |
| Físico | Roubo / Furto | Falta de câmeras |
| Lógico | Vazamento de Dados | Falta de criptografia e configuração de Firewall |
| Físico | Incêndio | Falta de sistema de detecção de incêndio, portas sem vigilância |
| Físico | Vazamento de gás | Falta de manutenção no sistema de gás e verificação diária do mesmo |
| Físico | Equipamentos mal conservados | Falta de manutenção e verificação dos equipamentos de preparo e conservação de alimentos |
| Lógico | Invasão ao aplicativo de pedidos | Vulnerabilidade no software e em dispositivos físicos. |
| Lógico | Ransomware, Malware e furto de dados | Uso inseguro de computadores e celular no sistema/rede do restaurante, falta de segurança com os dados (físicos) |

# ETAPA 3

Projeto fundamentos de sistemas

# 3.1 Construir um modelo de sistema de informação (no formato de um quadro) que atenda ao processo escolhido no item 1 da etapa 2 apresentando ameaças/vulnerabilidades e proposta de solução.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Informação** | **Origem** | **Processamento /Transformação** | **Saída** | **Ameaças/ Vulnerabilidade** | **Proposta de solução** |
| Cadastro | Site/aplicativo | Registro no banco de dados | Avanço para captação de endereço | Senhas fracas, tentativa de Phising | Exigir um padrão de senha seguro, com caracteres especiais, números e letras maiúsculas |
| Carrinho de pedido | Site/aplicativo | Armazenamento da escolha do usuário | Confirmação do pedido | Duplicidade de pedido  Sair pedido errado para a cozinha. | Controle nas plataformas para não permitir que o mesmo pedido seja feito mais do que uma vez pelo mesmo cliente.  Conferência do papel de pedido sempre que for para a cozinha |
| Conferir pedido | Site/aplicativo | Conferição do pedido | Conferência | Falha no carregamento da página, não salvamento do pedido. | Criar sistema de armazenamento de carrinho por usuário, logado ou não na plataforma |
| Sugestões de mais itens | Site/aplicativo | Sugestão de pedidos mais vendidos pela plataforma | Sugestão | Não sugestão de itens mais pedidos, sugestão errada de itens | Criar padrão de itens mais vendidos pelo site/aplicativo e manter fixo |
| Cupom de desconto | Site/aplicativo | Verificação do cupom | Benefício ao usuário | Duplicidade de cupom, cupom não existente ou já usado | Criar cupons exclusivos, e de uso único do mesmo usuário |
| observações | Site/aplicativo | Anotar observações do pedido | Guia de informações do usuário referente ao pedido | Não ser impresso na comanda, sair observação errada de outro pedido. | Criar sistema de armazenamento de comanda por usuário, fazendo assim com que não seja possível a observação vá para outro pedido |
| Confirmação de cadastro | Site/aplicativo | Autenticação do usuário | Confirmação de conta e informações pessoais do cliente | Contas roubadas, falha no login, informações trocadas de outra conta | Orientar ao usuário a importância de estar com uma conta logada desde o início do processo, para que não haja perda de informações durante todo o processo, e sistema seguro de auth. |
| Informações de pagamento | Site/aplicativo | Confirmar meios de pagamentos | Recebimentos dos meios de pagamentos, pela própria plataforma ou na entrega | Cartões clonados, invasão e alteração da página de pagamento para roubo dos pagamentos, perda de dados de pagamento dos clientes | Criar página fixa de pagamento com plataforma segura, deixando bem claro todas as informações de cobrança do restaurante em uma guia própria de informações de cobrança de dados do restaurante, para que o usuário suspeite de qualquer alteração. |
| Finalizar pedido | Site/aplicativo | Finalização do pedido | Transferência do pedido para cozinha | Queda de internet e falha do processamento | Armazenamento de cookies do usuário para que não haja perda de informações casa tenha queda de internet do mesmo ou queda do site/aplicativo |
| Acompanhar pedido | Site/aplicativo | Rastreio do pedido | Localização ou informação do status do pedido | Localização errada ou de pedido errado, falta de comunicação da cozinha com a gestão de pedidos | Criar sistema de informação de qual motoboy irá levar o pedido e manter fixo, orientar a cozinha a atualizar todos os processos para que seja feita a gestão correta de qual etapa está o pedido na plataforma |

# **3.2 Definir Hardware de servidor completo para atender ao modelo de sistema de informação construído no item 1, justificando cada escolha e mostrando o CAPEX e OPEX.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Descrição** | **Justificativa** | **CAPEX** | **OPEX** |
| Servidor | Dell PowerEdge T30, Intel Core i5, 16GB RAM, 256GB SSD + 1TB HDD | Atende as necessidades de um restaurante de médio porte, incluindo gestão de reservas, cardápios e estoque. | R$ 15.000 | R$ 150,00 (manutenção) |
| Rede | Firewall: Fortinet FortiGate 60F | Assegura alta conectividade, segurança e gerenciamento de rede. | R$ 10.000 | R$ 200,00 (manutenção) |
| Hardware | Equipamentos de rede (switches, roteadores, pontos de acesso, cameras) | Conectividade entre os dispositivos da rede | R$ 3.000 | 100,00  (manutenção) |
| Software | MySQL, Docker, Backup, antivírus | Softwares que complementam a segurança física, como sistema operacional, banco de dados, antimalware | R$ 3.500 | 150,00 ~200,00  (manuten. E licenças) |
| Suporte Técnico |  | Manutenção e reparos nos servidores e equipamentos de rede | R$ 1.500/mês |  |

# 3.3 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: (em anexo).

* 1. Hardware
  2. Software
  3. Hardware e Software

# 3.4 Realizar uma análise de riscos/continuidade/contingência dos itens de segurança física e lógica encontrados no item 5 da etapa 2.

**1. Segurança Física**

A segurança física está relacionada à proteção do estabelecimento, das pessoas e dos ativos contra ameaças externas e internas.

**Ameaças:**

* Intrusão e Roubo: Invasões ao restaurante durante a noite ou enquanto está fechado, roubos de equipamentos, dinheiro e estoque.
* Violência ou Agressão: Atos de violência, como assaltos, brigas ou agressões dentro do restaurante.
* Incêndio e Desastres Naturais: Falhas no sistema de prevenção contra incêndios, inundações ou outros desastres naturais.
* Acessos não autorizados: Funcionários ou terceiros com acesso indevido a áreas restritas, como cozinha, estoque ou escritório.

**Medidas de Mitigação:**

* Controle de Acesso: Instalar sistemas de controle de entrada, como fechaduras digitais, catracas ou portões com identificação por biometria ou cartões. Limitar o acesso a áreas restritas (como a cozinha e o escritório financeiro).
* Monitoramento por Câmeras de Segurança (CFTV): Colocar câmeras em áreas chave, como entradas, corredores, estacionamento, e dentro do restaurante. Sistemas de CFTV ajudam a identificar e a registrar atividades suspeitas.
* Alarmes e Sensores: Instalar alarmes de intrusão e sensores de movimento para detectar acessos não autorizados ou movimentos inesperados durante a noite.
* Treinamento de Funcionários: Capacitar a equipe para identificar comportamentos suspeitos e como lidar com situações de risco, incluindo casos de agressões ou assaltos.
* Prevenção de Incêndios: Manter extintores de incêndio, sprinklers, detectores de fumaça e saídas de emergência adequadas. Realizar treinamentos periódicos de evacuação.
* Iluminação Adequada: Garantir boa iluminação nas áreas externas e de difícil acesso, como estacionamento e entradas, para dissuadir criminosos.
* Política de Segurança para Funcionários: Estabelecer procedimentos para o gerenciamento de dinheiro e equipamentos, evitando que um único colaborador tenha acesso irrestrito a recursos financeiros.

**2. Segurança Lógica**

A segurança lógica está relacionada à proteção de sistemas, dados e informações digitais do restaurante. Isso inclui informações sobre clientes, funcionários, operações financeiras e fornecedores.

**Ameaças:**

* Ataques Cibernéticos: Hackers, vírus ou malware podem comprometer sistemas de gestão de pedidos, dados financeiros ou informações pessoais de clientes.
* Acesso Indevido a Dados: Funcionários não autorizados podem acessar informações confidenciais, como senhas de sistemas, registros de pagamento ou dados bancários.
* Perda ou Roubo de Dados: Desastres como falhas de hardware, perda de dispositivos (como laptops ou tablets usados em mesas) podem levar à perda de dados críticos.
* Falhas em Sistemas de Pagamento: Problemas nos sistemas de pagamento (POS) podem gerar erros nas transações ou perda de dados financeiros.

**Medidas de Mitigação:**

* Firewall e Proteção de Rede: Implementar firewalls e sistemas de proteção para prevenir invasões externas em redes de dados e sistemas internos.
* Criptografia de Dados Sensíveis: Garantir que dados como informações de pagamento e dados pessoais dos clientes sejam criptografados tanto em trânsito quanto em repouso.
* Política de Senhas Fortes: Exigir o uso de senhas fortes e únicas para acessar sistemas críticos e garantir que as senhas sejam alteradas periodicamente.
* Controle de Acesso a Sistemas: Limitar o acesso a dados sensíveis e sistemas internos com base no cargo e responsabilidades de cada funcionário. Isso pode ser feito com sistemas de gerenciamento de identidade e autenticação.
* Backup Regular de Dados: Realizar backups periódicos dos dados e mantê-los em locais seguros (preferencialmente em servidores remotos ou na nuvem), para evitar perdas em caso de falhas.
* Treinamento de Funcionários sobre Segurança Cibernética: Capacitar a equipe para identificar ameaças, como phishing, e ensiná-los a adotar boas práticas de segurança.
* Monitoramento e Auditoria de Sistemas: Implantar sistemas de monitoramento para identificar acessos não autorizados ou atividades suspeitas e realizar auditorias regulares nos sistemas de gestão.
* Segurança em Transações de Pagamento: Implementar sistemas de pagamento seguros, como pagamentos por cartão EMV ou sistemas de pagamento via apps, que sejam resistentes a fraudes e clonagens.

**Integração entre Segurança Física e Lógica**

A combinação de segurança física e lógica é essencial para garantir uma proteção holística. Por exemplo, garantir que servidores ou sistemas de pagamento sejam armazenados em áreas seguras, com controle de acesso físico e protegidos por firewalls e criptografia.

Além disso, o uso de tecnologias como IoT (Internet das Coisas), que conecta dispositivos como câmeras de segurança, sensores de incêndio e sistemas de controle de entrada, pode permitir uma abordagem mais integrada e automatizada na gestão da segurança.

**Plano de Resposta a Incidentes**

Além de medidas preventivas, é importante ter um plano de resposta a incidentes. Isso envolve:

* Plano de Recuperação de Desastres: Definir como o restaurante irá reagir a falhas de segurança cibernética ou incidentes físicos, como incêndios.
* Treinamento em Situações de Crise: Instruir todos os colaboradores sobre o que fazer em caso de incêndio, intrusão ou falha de sistemas de pagamento.
* Análise Pós-Incidente: Após qualquer incidente, realizar uma análise para identificar as causas, ajustar procedimentos e melhorar a segurança.

Estabelecer um equilíbrio entre os custos de um incidente e os custos de uma medida de segurança envolve a análise de custo-benefício: ou seja, o valor que você gastaria para implementar uma medida de segurança em comparação com o impacto financeiro de um possível incidente.

**1. Classificação de Riscos e Incidentes Potenciais**

**Incidentes Físicos:**

* Roubo ou Furto (externo ou interno): Um incidente de roubo pode causar a perda de mercadorias, equipamentos, dinheiro ou até mesmo prejudicar a reputação do restaurante.
* Violência ou Assaltos: Além dos danos materiais, a agressão pode afetar gravemente a reputação e a segurança dos funcionários e clientes.
* Incêndio ou Acidente: Danos à estrutura, equipamentos e bens do restaurante, além de custos com interrupção das operações e multas de não conformidade com normas de segurança.
* Danos a Equipamentos: Roubo ou danos aos equipamentos, como sistemas de ponto de venda (POS) ou tecnologia de cozinha, pode paralisar as operações e gerar custos adicionais.

**Incidentes Lógicos (Cibernéticos):**

* Ataques Cibernéticos (phishing, malware, ransomware): O roubo de dados dos clientes ou o bloqueio dos sistemas pode afetar a confiança dos consumidores e resultar em custos com recuperação de dados, multas por vazamento de informações e possível perda de clientes.
* Fraude Financeira em Sistemas de Pagamento: Comprometimento de dados financeiros dos clientes ou do restaurante pode gerar processos judiciais e danos à reputação.
* **2. Custo das Medidas de Segurança**

**Segurança Física:**

* Câmeras de Segurança (CFTV): O custo para instalação de um sistema de câmeras de segurança de boa qualidade pode variar entre R$ 2.000 e R$ 10.000, dependendo da quantidade de câmeras e da tecnologia (com monitoramento remoto ou local).
* Controle de Acesso (fechaduras digitais, biometria, etc.): Um sistema de controle de acesso pode custar entre R$ 1.500 e R$ 5.000, dependendo da complexidade e do número de pontos de acesso.
* Alarmes e Sensores de Intrusão: Instalar alarmes e sensores de movimento pode custar entre R$ 1.000 e R$ 3.000, além da mensalidade do serviço de monitoramento.
* Treinamento de Funcionários em Segurança: O custo pode variar, mas geralmente fica entre R$ 500 e R$ 3.000 para treinamentos periódicos.

**Segurança Lógica:**

* Firewall e Proteção de Rede: Um bom firewall corporativo e serviços de proteção de rede podem custar entre R$ 2.000 e R$ 8.000, dependendo do porte da operação.
* Criptografia de Dados e Backup em Nuvem: O custo de software de criptografia e backup na nuvem pode variar entre R$ 500 e R$ 3.000 mensais, dependendo da quantidade de dados e do nível de segurança.
* Sistemas de Pagamento Seguros (POS): O custo de sistemas de pagamento seguros pode variar, mas geralmente fica entre R$ 3.000 e R$ 8.000, dependendo da complexidade dos sistemas.
* Treinamento em Segurança Cibernética: Treinamentos para os funcionários sobre práticas de segurança cibernética podem custar de R$ 1.000 a R$ 5.000, dependendo da profundidade do curso.

**3. Cálculo do Custo de um Incidente**

**Roubo ou Furto (Incidente Físico)**

**Custo do Incidente:**

* Perda de mercadorias e equipamentos: R$ 10.000 a R$ 30.000 (dependendo da gravidade do roubo).
* Custos com interrupção das operações (paralisação parcial ou total): R$ 5.000 a R$ 15.000 (por um dia ou mais).
* Custos legais, se necessário, ou danos à reputação: R$ 2.000 a R$ 10.000.
* Total do Incidente: Pode variar de R$ 17.000 a R$ 55.000.

**Custo das Medidas de Segurança:**

* Câmeras de segurança: R$ 2.000 a R$ 10.000.
* Alarmes e sensores: R$ 1.000 a R$ 3.000.
* Total das Medidas de Segurança: Entre R$ 3.000 e R$ 13.000 (uma vez, sem contar manutenção mensal).

**Ataque Cibernético (Incidente Lógico)**

**Custo do Incidente:**

* Vazamento de dados de clientes (multa, ações judiciais): R$ 20.000 a R$ 100.000.
* Interrupção do sistema (como um ataque de ransomware): R$ 10.000 a R$ 50.000 (dependendo do tempo de inatividade e custos de recuperação).
* Danos à reputação e perda de confiança do cliente: R$ 5.000 a R$ 30.000 (ou mais a longo prazo).
* Total do Incidente: Pode variar entre R$ 35.000 a R$ 180.000.
* **Custo das Medidas de Segurança:**
* Firewall e proteção de rede: R$ 2.000 a R$ 8.000.
* Criptografia de dados e backup: R$ 500 a R$ 3.000 mensais.
* Total das Medidas de Segurança: Entre R$ 2.500 e R$ 11.000 (inicialmente, mais custos mensais para manutenção e backup).

**Equilíbrio entre Custos de Medidas de Segurança e Custos de Incidentes**

A chave para encontrar um equilíbrio é considerar o retorno sobre o investimento (ROI) das medidas de segurança. A análise indica que o custo de uma medida de segurança (seja física ou lógica) é frequentemente muito menor do que os custos potenciais de um incidente. Portanto, implementar as medidas de segurança é geralmente uma escolha mais econômica, ao passo que prevenir é mais barato do que remediar.

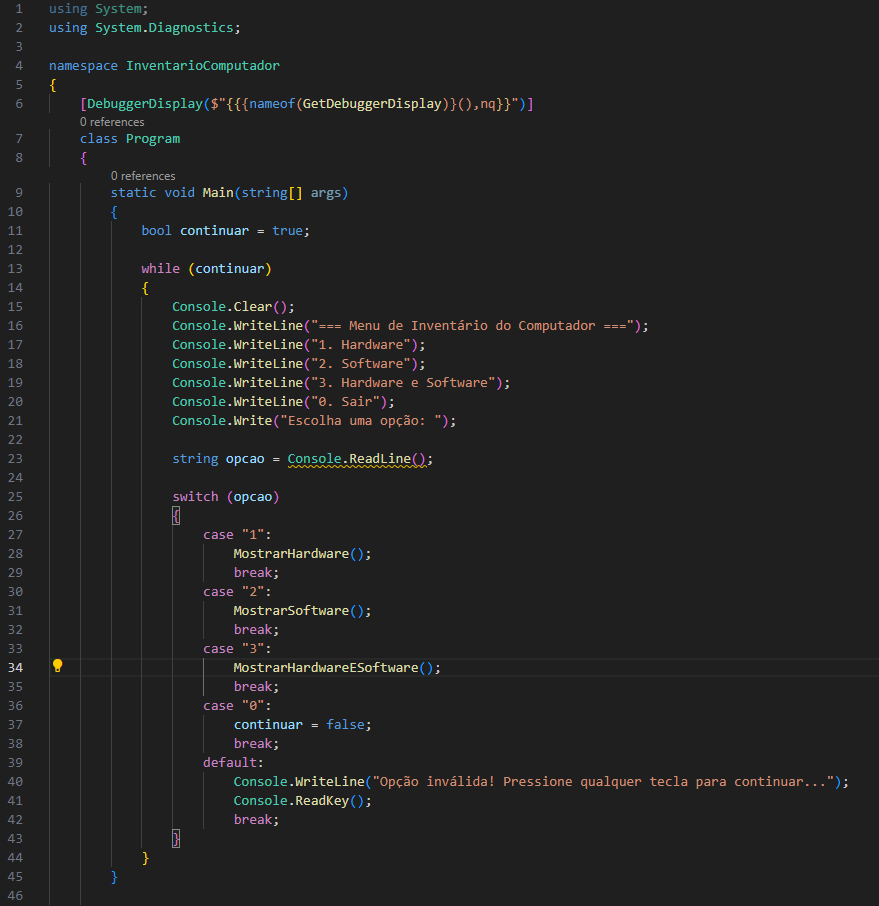
Custo das Medidas de Segurança: Geralmente, o valor investido nas medidas de segurança será 10 a 30 vezes menor do que o custo total de um incidente significativo, como um roubo ou um ataque cibernético.

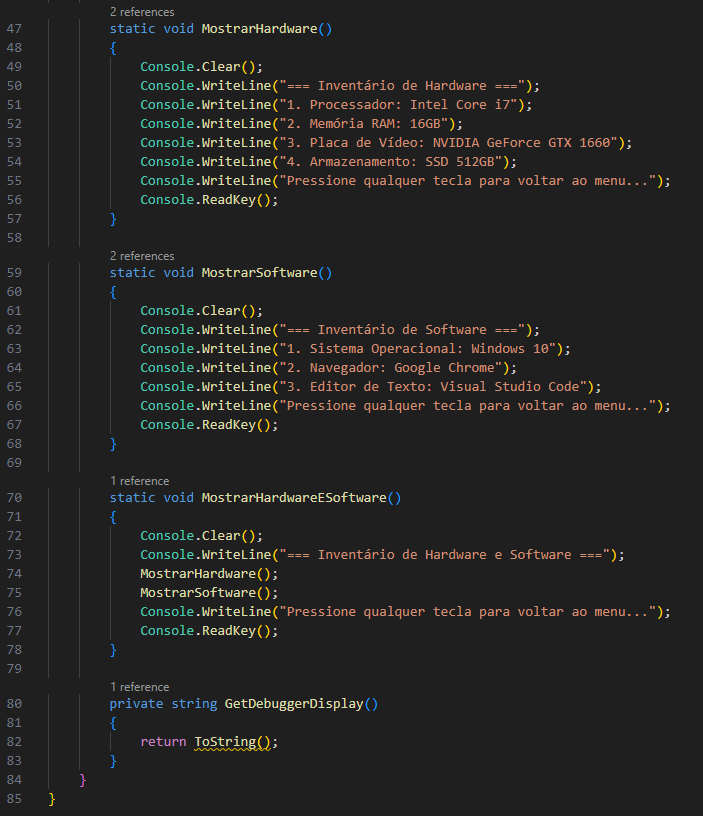
Prevenção é sempre mais barata: Investir em medidas de segurança (como câmeras, controles de acesso, firewalls e criptografia) ajuda a mitigar riscos e reduz as chances de um incidente sério, tornando-se mais vantajoso do ponto de vista financeiro.

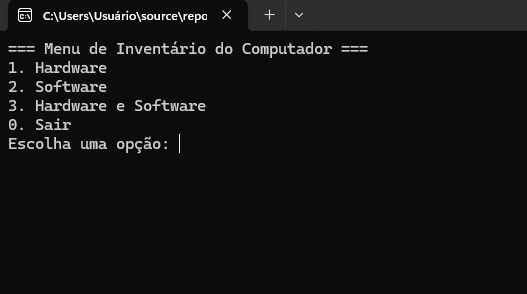
**Conclusão:**

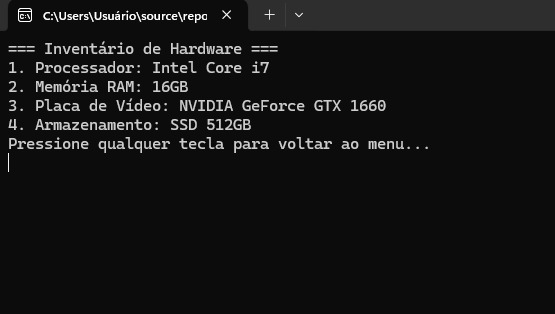
O equilíbrio entre os custos de medidas de segurança e os custos de um incidente depende da gravidade potencial dos riscos. Investir em segurança é sempre uma escolha mais vantajosa a longo prazo, pois reduz significativamente os custos financeiros e operacionais associados a incidentes. A segurança preventiva ajuda não só a evitar perdas imediatas, mas também protege a reputação do restaurante, mantendo a confiança dos clientes e evitando multas e danos financeiros a longo prazo.

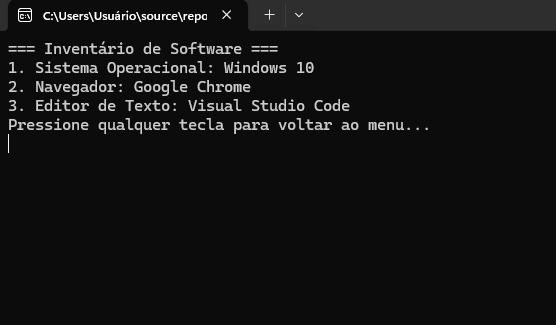
# Anexo dos Scripts e Protótipo navegável



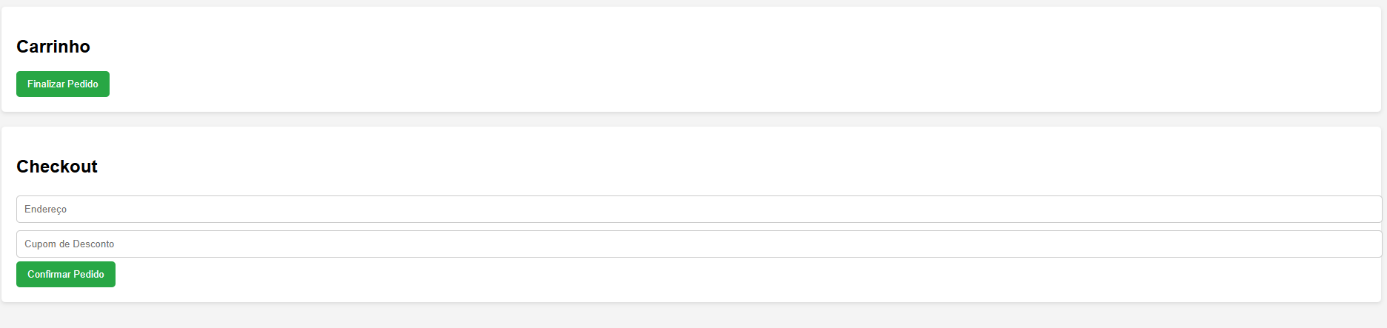








Interface [link interface](https://gustavohvb1.github.io/gaules-site/)



# Referências Bibliográficas

Livros

BONNEY, Bill; SHIPLEY, Greg. CISO Handbook: A Practical Guide to Security Leadership. Wiley, 2018.

KLEPPER, David L. Security Risk Management: Building an Information Security Risk Assessment Framework. Auerbach Publications, 2017.

STANISLAV, Mark; MITNICK, Kevin, et al. Information Security: Principles and Practice. Wiley, 2020.

STALLINGS, W. Segurança de Redes e Comunicações: Conceitos, Protocolos e Práticas. Pearson Education, 2017.

ISO/IEC 27001:2013. Sistema de Gestão da Segurança da Informação (SMSI). Disponível em: <https://www.iso.org>. Acesso em: 18 setembro. 2024.

BISHOP, Matt. Computer Security: Art and Science. Pearson Education, 2018.

PARKER, David. Cybersecurity: Understanding the Basics. CRC Press, 2020.

LANDFIELD, David. Introduction to Information Security: A Strategic-Based Approach. Auerbach Publications, 2019.

HADNAGY, C. Social Engineering: The Science of Human Hacking. Wiley, 2018.

Artigos e Documentos Técnicos

Framework for Risk Assessment in Information Security Projects. Disponível em: Google Scholar ou IEEE Xplore. Acesso em: 5 novembro. 2024.

Cybersecurity Risks in SMEs: Analysis and Frameworks for Security Implementation. Disponível em: SpringerLink ou ScienceDirect. Acesso em: 5 novembro. 2024.

NIST. Special Publication 800-30: Guide for Conducting Risk Assessments. Disponível em: <https://nvlpubs.nist.gov>. Acesso em: 30 outubro. 2024.

ZHANG, Y., & ZHOU, L. AI-based Behavioral Analysis for Threat Detection in Financial Transactions. Journal of Cybersecurity and Privacy, 2021.

TURKANOVIĆ, M., et al. AI and Machine Learning for Cybersecurity: Applications and Trends. 2020.

KROTOV, Alexei. Advances in Threat Intelligence and Security Management. Journal of Information Security, v. 12, n. 3, p. 101-115, 2022.

GHOSH, R.; BHADURI, A. Behavioral Analysis Using AI to Enhance Fraud Detection and Prevention. AI & Security Journal, 2019.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. Deep Learning. MIT Press, 2016.

PELTER, T. R. Information Security Policies, Procedures, and Standards: Guidelines for Management. Auerbach Publications, 2013.

**Normas e Padrões**

ISO/IEC 27005:2018. Information Security Risk Management. Internacional Organization for Standardization, 2018.

ISO/IEC 27001:2013. Information Security Management Systems (ISMS). Internacional Organization for Standardization, 2013.

PCI SECURITY STANDARDS COUNCIL. PCI DSS - Payment Card Industry Data Security Standard. 2021. Disponível em: <https://www.pcisecuritystandards.org/>. Acesso em: 15 outubro. 2024.

ISO/IEC 27001:2013. Sistema de Gestão da Segurança da Informação (SMSI). Disponível em: <https://www.iso.org>. Acesso em: 3 outubro. 2024.

NIST. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 2018.

ISO 22301:2019. Gestão da Continuidade do Negócio e Segurança Física. Disponível em: <https://www.iso.org>. Acesso em: 27 novembro. 2024.

Recursos Online

SANS Institute. Risk Management Resources. Disponível em: <https://www.sans.org>. Acesso em: 8 novembro. 2024.

Governo Federal (Gov.br). Diretrizes e documentos públicos sobre segurança digital. Disponível em: gov.br. Acesso em: 25 novembro. 2024.

BRASIL. Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018). Disponível em: <https://www.planalto.gov.br>. Acesso em: 14 outubro. 2024.

KUNER, Christopher; HILDEBRANDT, Mireille. The European Union and the Search for an International Data Protection Framework. 2019.

## Anexo PSI e NORMAS



ANEXO PSI- Dois cliques no arquivo para abrir o documento da PSI



ANEXO NORMAS – Dois cliques no arquivo para abrir as normas