

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

SUMÁRIO

1. EQUIPE DE TRABALHO	1
2. COMPREENDENDO A ORGANIZAÇÃO (CODE SECURITY).....	1
2.1. O negócio.....	3
3. OS PRINCIPAIS PROCESSOS DE NEGÓCIOS	4
3.1 Processos principais (Fluxograma).....	5
4. ESCOLHER 1 PROCESSO DE NEGÓCIO ENTRE OS QUE FORAM IDENTIFICADOS NA ETAPA 1 E DETALHÁ-LO USANDO UMA FERRAMENTA DE CONSTRUÇÃO DE FLUXOGRAMA.	7
5. 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.	8
6. MAPEAR ITENS RELACIONADOS À TI INVISÍVEL NA ORGANIZAÇÃO.	12
7. IDENTIFICAR DISPOSITIVOS PESSOAIS UTILIZADOS NA ORGANIZAÇÃO.	14
8. IDENTIFICAR RISCOS DE SEGURANÇA FÍSICA E LÓGICA DISCUTIDOS NO MF DE FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO E ENCONTRADOS NO CONTEXTO ORGANIZACIONAL ESTUDADO.	15
8.1. Mapas de Riscos	17
9. 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.	19
10. 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.	20

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.		PFS-003-2025
			Versão: 1.0
	Classificação: interna		Última revisão: 23/05/2025

11. 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:	21
12. REALIZAR UMA ANÁLISE DE RISCOS/CONTINUIDADE/CONTINGÊNCIA DOS ITENS DE SEGURANÇA FÍSICA E LÓGICA ENCONTRADOS NO ITEM 5 DA ETAPA 2.	29
GLOSSÁRIO.....	31

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.		PFS-003-2025
			Versão: 1.0
	Classificação: interna		Última revisão: 23/05/2025

1. EQUIPE DE TRABALHO


- Douglas Lee de Freitas - 897172
- Gustavo Felipe Magalhães - 883903
- Herrison Teles da Silva – 1578558
- Judá Benhur de Goes Cabral - 882292
- Marcos Silas Mamede Câmara - 1578219
- Pedro Henrique de Oliveira Dornelas – 1593852

2. COMPREENDENDO A ORGANIZAÇÃO (CODE SECURITY)

A Code Security, criada em 28 de fevereiro de 1975, é integrante da administração indireta do Poder Executivo do Estado do Amazonas, está vinculada à Secretaria de Estado da Agricultura. Tem por finalidade a execução das políticas públicas de recursos hídricos e irrigação do Estado, como o aproveitamento múltiplo da água, saneamento básico para comunidades rurais, estudos, pesquisas, ações de desenvolvimento social e econômico a partir do uso racional de águas subterrâneas, fluviais, reservamento de águas pluviais e irrigação no estado.

O ente público, caracterizado como uma sociedade de economia mista de capital autorizado, em que o Governo do Estado do Amazonas detém o controle acionário, se tornou ao longo de 39 anos de existência a empresa pública de maior atuação em irrigação e captação de águas subterrâneas no estado, tendo perfurado mais de 3.860 poços tubulares e disponibilizando infraestrutura que tornam irrigáveis 11.516 hectares de terra agricultável, beneficiando continuamente mais de 66 mil pessoas no campo.

Metade desta infraestrutura de irrigação instalada pelo Governo do Estado, a Code Security mesmo administra em seis perímetros irrigados responsáveis pela produção média anual de 100 mil toneladas de alimentos variados, como: batata-doce, quiabo, milho verde, cana-de-açúcar, inhame, macaxeira, maracujá, goiaba, tomate, pimentão, alface, coentro, cebolinha. Nos perímetros, a água captada em reservatórios fluviais abastece 1.450 lotes da agricultura familiar e 31 empresariais. Somando a terra agricultável, as áreas de proteção permanente (APPs) e os setores operacionais para o abastecimento de água irrigação, esses perímetros ocupam uma área total de 10.158 hectares,

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025


abrangendo setores dos municípios de Manaus, Itacoatiara, Manacapuru, Coari, Humaitá e Malhador e Hamilt.

Ao mesmo tempo, a companhia atualmente é responsável por administrar os contratos de concessão do Distrito de Irrigação do Platô de Anamã. Neste, são 10.312 hectares ocupados por 41 lotes empresariais, infraestrutura para fornecer irrigação e APPs, abrangendo os municípios de Anamã e Alvarães. Lá são produzidas frutícolas destinadas ao mercado nacional e de exportação; matéria prima para indústria sucroalcooleira, de cerâmicas, de ração animal e também ao mercado de jardinagem.

No tocante à exploração racional dos recursos hídricos para o abastecimento humano e dessedentação animal, a empresa detém no estado do Amazonas o know-how para perfurar uma média aproximada de 100 novos poços tubulares todo ano, a partir de suas sete equipes de perfuração e teste de vazão. Quando lhe compete, instala sistemas de bombeamento, armazenamento e distribuição de água a partir destes poços, dispondo de duas equipes de instalação e manutenção de poços. Corpo técnico que também opera em todo estado em demandas que vão desde a recuperação de sistemas de abastecimento desativados, reparos por falhas técnicas e manutenções preventivas, originando mais de 230 atendimentos anuais. Quanto ao reservamento de águas fluviais, ao longo dos seus 39 anos de existência a Code Security atuou também construindo ou recuperando mais de 3.000 barragens e cerca de 5.000 cisternas.

Possui a missão de promover o desenvolvimento sustentável do meio rural amazonense, com aproveitamento múltiplo dos recursos hídricos do estado, através da implantação e operação de sistemas de abastecimento de água e irrigação, da infraestrutura hídrica para aproveitamento de águas subterrâneas e da prestação de serviços de assistência técnica aos irrigantes familiares.

A Code Security tem como visão ser reconhecida pela sociedade como referência nas atividades fomentadoras do desenvolvimento sustentável no meio rural e programar projetos públicos de irrigação, aproveitamento de águas pluviais e subterrâneas, tendo em vista a inclusão social e econômica.

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025


2.1. O negócio

A Code Security com sede em Manaus, capital do estado do Amazonas e jurisdição em todo o território estadual de acordo com o estatuto social da empresa tem como objetivos:

- ❖ Aproveitamento múltiplo dos recursos hídricos do estado visando:
 - Abastecimento d'água às populações rurais;
 - Implantação e operação de sistemas de irrigação.
 - Prestação de serviços de assistência técnica aos agricultores e assentados nos perímetros irrigados administrados pela Code Security.
 - Apoio ao desenvolvimento da piscicultura.
 - Implantação de esgotos sanitários para comunidades rurais.

- ❖ Otimização da capacidade dos recursos hídricos do estado:
 - Construção de barragens, açudes e cisternas;
 - Perenização de cursos d'água;
 - Perfuração de poços tubulares profundos;
 - Desenvolvimento de estudos com vistas à concepção de formas alternativas de abastecimento d'água às populações rurais.


- ❖ Prestação de serviços agrícolas mecanizados, em função de prioridades estabelecidas.
- ❖ Promoção e execução de outras atribuições ou atividades correlatas, ou aquelas outras inerentes à sua finalidade ou ao desenvolvimento de recursos hídricos e irrigação.
- ❖ Colonização e assentamento de produtores rurais em perímetros irrigados.

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

3. OS PRINCIPAIS PROCESSOS DE NEGÓCIOS

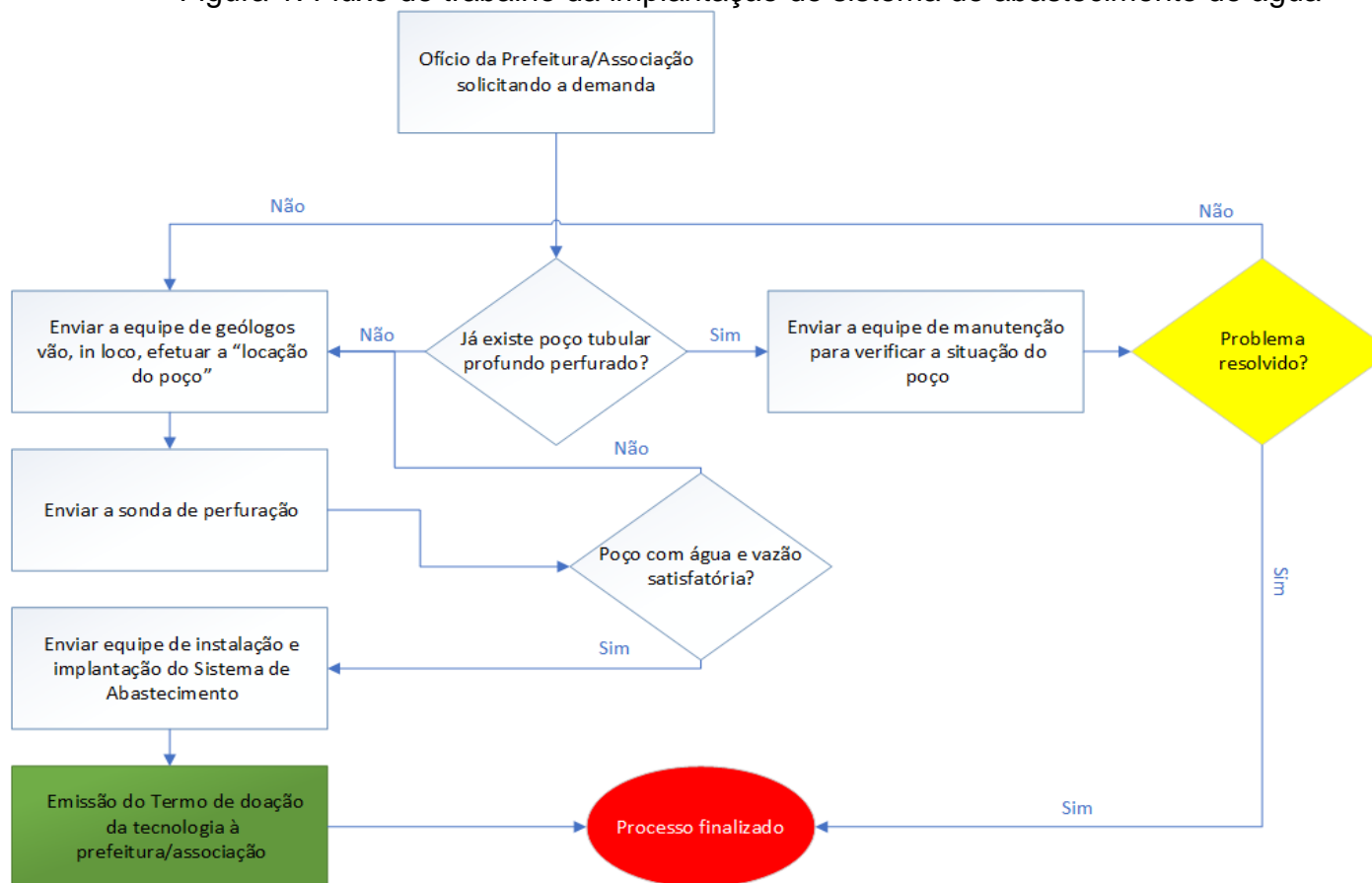
No caso da Code Security, os principais processos de negócio são:

- Definição de fornecedores de insumos;
- Recebimento de insumos para perfuração de poços tubulares profundos;
- Recebimento de insumos para instalação e implantação de poços tubulares profundos;
- Recebimento de materiais e/ou equipamentos para manutenção dos perímetros irrigados;
- Faturamento e pagamento de insumos;
- Faturamento e cobrança da tarifa d'água dos irrigantes;
- Ordem de serviço;
- Autorização de execução de obras de infraestrutura;
- Controle de estoque;
- Faturamento;
- Gerenciamento de logística;
- Gerenciamento de relacionamento a população;

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.		PFS-003-2025
			Versão: 1.0
	Classificação: interna		Última revisão: 23/05/2025

3.1 Processos principais (*Fluxograma*)

Figura 1. Fluxo de trabalho da implantação de sistema de abastecimento de água



FONTE: Elaborado pelos próprios autores (2025)


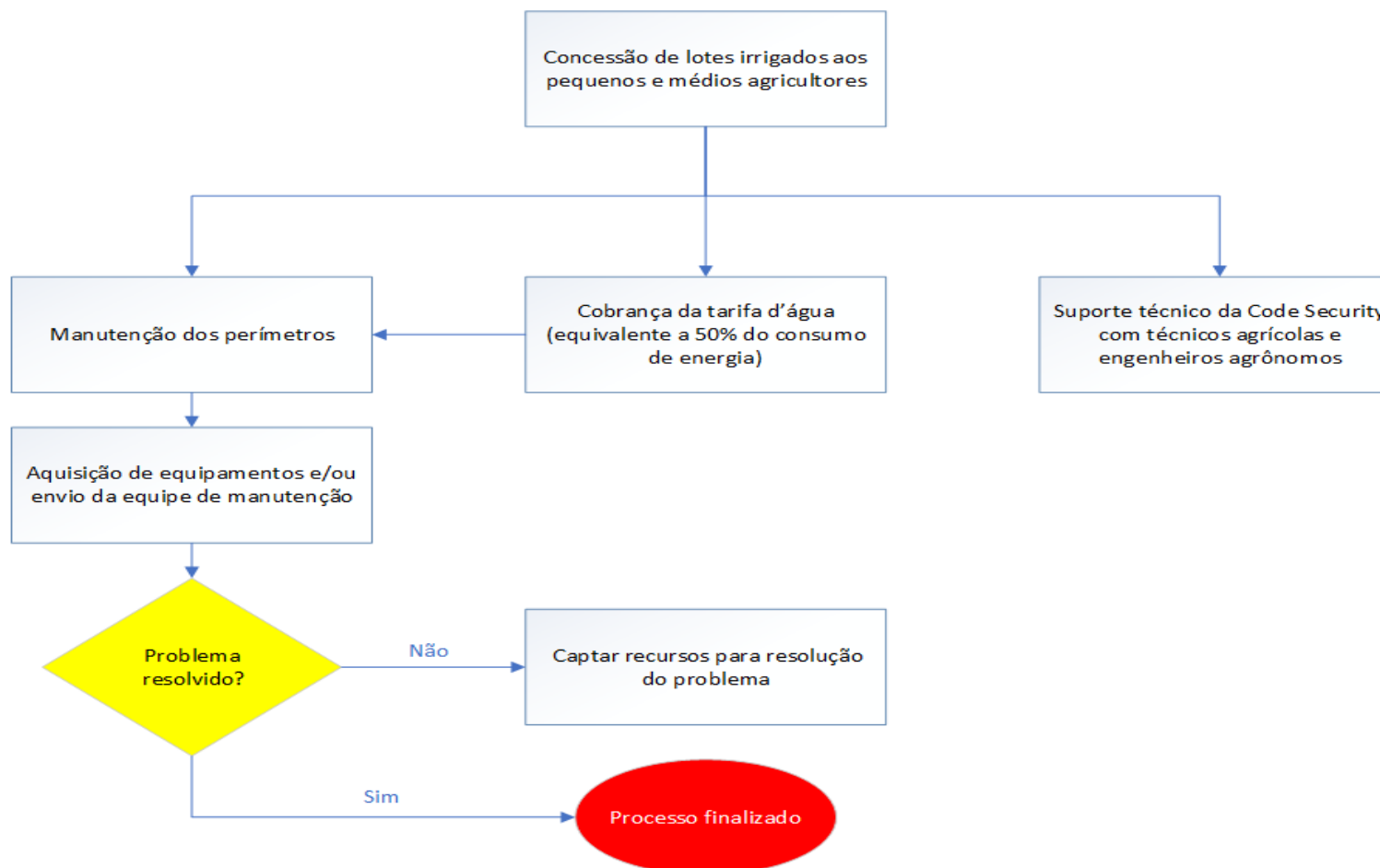

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

Figura2. Fluxo de trabalho dos perímetros irrigados administrados pela Code Security

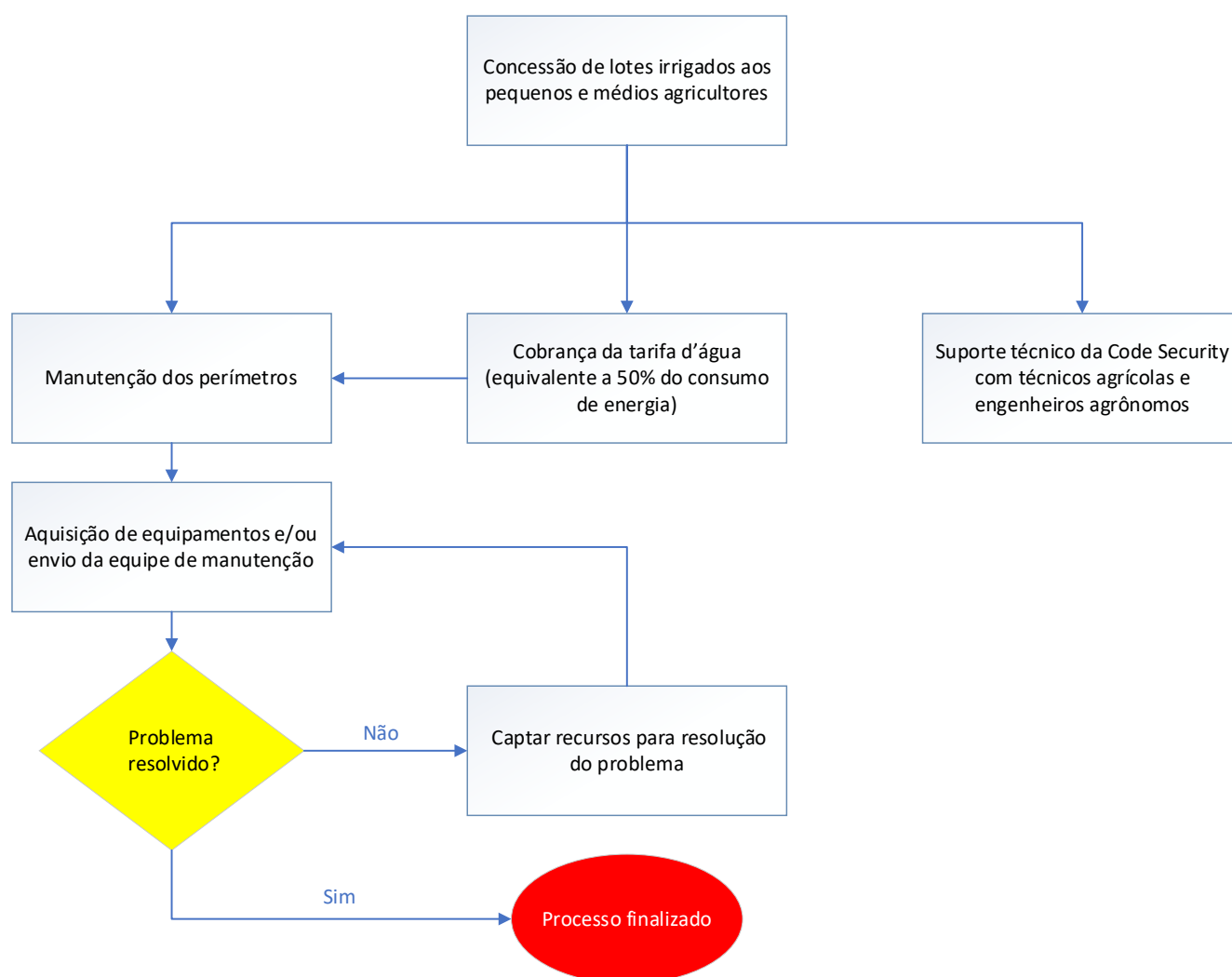


FONTE: Elaborado pelos próprios autores (2025)

	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025


4. ESCOLHER 1 PROCESSO DE NEGÓCIO ENTRE OS QUE FORAM IDENTIFICADOS NA ETAPA 1 E DETALHÁ-LO USANDO UMA FERRAMENTA DE CONSTRUÇÃO DE FLUXOGRAMA.

Figura 3. Fluxo de trabalho dos perímetros irrigados administrados pela Code Security




FONTE: Elaborado pelos próprios autores (2025)

Na Figura 1 é demonstrado o mapeamento do processo escolhido que serviu de base para dar seguimento aos tópicos posteriores. Os quais são referentes à Tarefa 2 do Projeto: Fundamentos de Sistemas do Eixo 1 do curso de Segurança da Informação.


	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

5. 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.


Classes de Segurança Informação	Eventos Suscetíveis	Setores Vulneráveis	Análise de Riscos	Solução
Sinistros	Enchentes, desabamentos, curto-circuitos, quedas e picos de energia, incêndios.	Estoques e áreas de produção também estão sujeitos a incêndios e danos estruturais. A logística pode ser afetada por alagamentos, e a segurança dos funcionários deve ser priorizada em caso de emergências.	A empresa deve implementar ações preventivas, desenvolvendo planos de contingência e treinamento de seus funcionários. O monitoramento contínuo e a revisão pós-incidente são essenciais para melhorar a resposta a futuros sinistros e garantir a continuidade dos negócios.	É fundamental ter um plano de contingência claro, incluindo ações de emergência, backup de dados e recuperação de TI. Seguros adequados, comunicação transparente com stakeholders e treinamentos regulares são essenciais para minimizar impactos.
Fraudes e Sabotagens	Espionagem industrial ou comercial, roubo de informações, adulteração de dados e cópias não autorizadas de projetos, processos, sistemas, programas e dados.	O financeiro é alvo de fraudes contábeis, enquanto o TI pode sofrer com acessos indevidos e sabotagens digitais. O RH é suscetível a fraudes de pagamento e documentos falsificados, e o setor de compras pode enfrentar corrupção e superfaturamento.	A análise de riscos envolve identificar vulnerabilidades, avaliar impactos financeiros, operacionais e reputacionais, e implementar medidas preventivas como controles internos rigorosos, segurança de TI	Combater fraudes e sabotagens, uma empresa deve adotar controles internos rigorosos, realizar auditorias frequentes e implementar sistemas de segurança robustos. Treinamentos

	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025


		<p>á a produção pode ser sabotada por danos aos processos, e o marketing pode ser manipulado para prejudicar a imagem da empresa.</p>	<p>e treinamento de funcionários.</p>	<p>regulares sobre ética e políticas de segurança, além de uma cultura de denúncia, são essenciais para prevenir problemas. Também é importante ter uma política de compliance clara, realizar verificações de fornecedores e adotar um plano de resposta eficiente a incidentes.</p>
<p>Erros Operacionais</p>	<p>Perda de dados históricos, exclusão indevida de arquivos, uso equivocado de versões de sistemas, programas e dados, além da não realização de rotinas de backup.</p>	<p>Pode afetar diversos setores de uma empresa, como produção, TI, logística, financeiro, atendimento ao cliente, RH e marketing. Esses erros podem incluir falhas na produção, problemas de sistemas, erros no controle de estoque, falhas contábeis, erros no atendimento e campanhas de marketing mal executadas.</p>	<p>Erros operacionais envolvem identificar falhas nos processos da empresa, avaliar seu impacto financeiro, nos clientes e na eficiência, e implementar medidas de mitigação, como automação, treinamento contínuo e auditorias regulares. Além disso, é fundamental monitorar os processos em tempo real e</p>	<p>O uso de ferramentas de monitoramento em tempo real e a criação de um plano de contingência para corrigir rapidamente falhas ajudam a melhorar a eficiência e minimizar os impactos negativos nos negócios.</p>

	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.		PFS-003-2025
			Versão: 1.0
	Classificação: interna		Última revisão: 23/05/2025

			revisar periodicamente os procedimentos para corrigir falhas rapidamente e garantir a continuidade das operações.	
Falha de Hardware	Falhas em conexões físicas, problemas em componentes, problemas em mídias móveis como HD externo, pen drive, entre outros, e falhas intermitentes em equipamentos.	Pode afetar diversos setores de uma empresa, como TI, produção, financeiro, atendimento ao cliente e logística, interrompendo sistemas essenciais e prejudicando operações.	Identificar possíveis falhas em equipamentos essenciais, como servidores e sistemas de armazenamento, e avaliar seus impactos operacionais e financeiros. A mitigação inclui a implementação de redundância, monitoramento contínuo, manutenção preventiva e políticas de backup eficazes.	Incluem a implementação de sistemas redundantes, manutenção preventiva, atualização de equipamentos e a criação de planos de recuperação de desastres.
Falha em comunicações	Problemas em provedores de acesso, falhas em equipamentos como roteadores, switches, modems e em componentes de rede, além	Impactam setores como atendimento ao cliente, TI, marketing, logística e RH, prejudicando operações e causando erros em processos críticos.	Identificam vulnerabilidades nos sistemas de comunicação da empresa, como internet e telefonia, e avaliam os impactos operacionais, financeiros e na	Implementação de redundância nos sistemas de comunicação, monitoramento contínuo, treinamento da equipe e criação de um


	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.		PFS-003-2025
			Versão: 1.0
	Classificação: interna		Última revisão: 23/05/2025

	de falhas nos meios de transmissão de dados, como antenas, satélites, cabos, fibras, entre outros.		segurança. As estratégias de mitigação incluem redundância de sistemas, monitoramento contínuo e treinamento dos funcionários.	plano de contingência.
Erros de entrada de Dados	Todo e qualquer processo que possa levar à falta de consistência na entrada de um dado.	Erros de entrada de dados podem impactar setores como financeiro, vendas, atendimento ao cliente, TI e RH, resultando em transações incorretas, falhas nos pedidos, problemas de pagamento e perda de informações.	Identificam falhas na coleta e processamento de informações, como erros humanos e falhas de sistema. As estratégias de mitigação incluem validação automática dos dados, automação de processos, treinamento de funcionários e auditorias regulares. Monitoramento contínuo e revisão dos processos ajudam a garantir a precisão dos dados, minimizando impactos operacionais, financeiros e reputacionais.	Incluem validação automática, automação de processos, treinamento contínuo dos funcionários e auditorias regulares. Além disso, a implementação de backups e planos de recuperação de dados ajuda a corrigir erros rapidamente, garantindo maior precisão e eficiência nas operações.


 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

6. MAPEAR ITENS RELACIONADOS À TI INVISÍVEL NA ORGANIZAÇÃO.

Nº DE ORDEM	Setor	Item de TI não catalogado	Proprietário	Usuários	Risco	Obs.
1	Administrativo	Roteador, pen drives, softwares de produtividade instalados localmente e serviços de armazenamento em nuvem.	Code Security (Computadores), Funcionários do setor (Smartphones, pen drives, roteador)	3	ALTO. A utilização de Hardwares como roteadores e pendrives, além de softwares de produtividade sem licença, não atualizados e serviços de armazenamento em nuvem logados em suas contas pessoais compromete a confidencialidade e integridade das informações em vista que não são gerenciados pela gerência de TI da empresa.	Aplicar LGPD. Necessário mapeamento de riscos, uma política de controle, uso (softwares, hardwares e serviços) e conscientização, criação de um canal de solicitação de regularização dos mesmos pelo setor de T.I.
2	Gerência de Perfuração	Pen drive, app's de anotações.	Funcionários do setor	3	MÉDIO. Utilização de Hardwares como pendrives ou app's de anotações compromete os 3 pilares da segurança da informação, em vista que não são	Mapear riscos e implantar uma plataforma oficial de registros pelo setor de T.I.


 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.		PFS-003-2025
			Versão: 1.0
	Classificação: interna		Última revisão: 23/05/2025

					gerenciados pela gerência de TI da empresa.	
3	Divisão de Poços	Pen drive, softwares instalados localmente e serviços de armazenamento em nuvem.	Code Security (Computadores), Funcionário do setor (pen drive)	1	MÉDIO. A utilização de softwares de produtividade sem licença, não atualizados e serviços de armazenamento em nuvem logados em suas contas pessoais compromete a confidencialidade e integridade das informações.	Aplicar LGPD. Necessário mapeamento de riscos, uma política de controle, uso (softwares, hardwares e serviços) e conscientização, criação de um canal de solicitação de regularização dos mesmos pelo setor de T.I.
4	Gerência de engenharia	Pen drive, Softwares CAD e de produtividade, serviços de armazenamento em nuvem.	Code Security (Computadores), Funcionários do setor (Pen drive)	4	ALTO. A utilização de Hardwares como pendrives e Softwares de produtividade e CAD sem licença, não atualizados e serviços de armazenamento em nuvem logados em suas contas pessoais comprometem os 3 pilares da Segurança da Informação em vista que não são gerenciados pela gerência de TI da empresa.	Aplicar LGPD. Necessário mapeamento de riscos, uma política de controle, uso (softwares, hardwares e serviços) e conscientização, criação de um canal de solicitação de regularização dos mesmos pelo setor de T.I.

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025


7. IDENTIFICAR DISPOSITIVOS PESSOAIS UTILIZADOS NA ORGANIZAÇÃO.

Nº DE ORDEM	Setor	Dispositivo	Proprietário	Usuários	Risco	Obs.
1	Administrativo	Pen-drives, smartphones e roteador	Junior, Ismênia e Marcela	3	Alto	LGPD aplicável. Risco elevado devido ao roteador e dispositivos móveis não gerenciados pela gerência de TI da empresa
2	Gerência de Perfuração	Pen-drives e smartphones	Tiago, Isabel, Keila	3	Médio	Possível vazamento de dados sensíveis. Recomendado a implantação de política de uso de dispositivos móveis, junto com o controle de acesso e criptografia
3	Divisão de Poços	Pen-drives	Rogério	1	Baixo	Dispositivo isolado, mas vulnerável a malware. Recomendado uso de antivírus.
4	Gerência de engenharia	Pen-drives e smartphones	Luan, Eliana, Larissa e Fernando	4	Alto	Diversos usuários e dispositivos móveis. Recomendado a implantação de políticas de uso de dispositivos móveis, junto com o controle de acesso e criptografia.


 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.		PFS-003-2025
			Versão: 1.0
	Classificação: interna		Última revisão: 23/05/2025

8. IDENTIFICAR RISCOS DE SEGURANÇA FÍSICA E LÓGICA DISCUTIDOS NO MF DE FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO E ENCONTRADOS NO CONTEXTO ORGANIZACIONAL ESTUDADO.

RISCOS FÍSICOS				
Ativo	Conexão com a Internet	Servidores de Rede	Laptops	Dispositivos Móveis Corporativos
Ameaça	Rompimento ou erro físico na fibra;	Incêndio	Roubo/Furto	Roubo, perda ou uso indevido
Vulnerabilidade	Cabo de fibra exposto;	Falta de extintores/detectores de fumaça, ambiente mal climatizado	Falta de monitoramento e Alarmes	Falta de Rastreamento/Monitoramento
Probabilidade	Média	Média	Baixa	Média
Impacto	Alto	Alto	Médio	Alta
Contingência	Diversificar o uso de ISPs;	Uso de termostatos, extintores de CO2, ares condicionados	Uso de câmeras de monitoramento; Aplicação de travas antifurto (Kensington)	Restrição somente a serviços essenciais no dispositivo; Rastreamento mediante Chips

	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025


RISCOS LÓGICOS				
Ativo	Sistema Operacional	Data Center	Sistema de Gerenciamento de Projetos	E-mail Corporativo
Ameaça	Contaminação por Trojans e Malwares;	Roubo/Exclusão de Informações	Acesso não autorizado a documentos	Envio de Phishing
Vulnerabilidade	Sistema desprotegido e uso de aplicativos não licenciados.	Falta de um sistema secundário de back-up	Sistema não criptografado	Coleta de informações e dados confidenciais
Probabilidade	Média	Média	Média	Alta
Impacto	Médio	Alto	Alto	Alto
Contingência	Uso de Anti-Vírus; Instalação de softwares permitida somente a T.I.;	Utilização de Sistema de Back-up; Monitoria de entrada de dados	Atualização frequente com a equipe de terceiros; Aplicação de Criptografia a documentos sensíveis	Treinamento para operadores e filtros anti-phishing

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

8.1. Mapas de Riscos

RISCOS FÍSICOS				
Ativo	Conexão com a Internet	Servidores de Rede	Laptops	Dispositivos Móveis Corporativos
Ameaça	Rompimento ou erro físico na fibra;	Incêndio	Roubo/Furto	Uso indevido
Vulnerabilidade	Cabo de fibra exposto;	Falta de extintores/detecção de fumaça, ambiente mal climatizado	Falta de monitoramento e Alarmes	Falta de Rastreamento/Monitoramento
Classificação	A (5-4)	A (5-3)	C (3-2)	C (3-1)
Contingência	Diversificar o uso de ISPs;	Uso de termostatos, extintores de CO2, ar-condicionado	Uso de câmeras de monitoramento; Aplicação de travas antifurto (Kensington)	Restrição somente a serviços essenciais no dispositivo;


RISCOS LÓGICOS				
Ativo	Sistema Operacional	Data Center	Sistema de Gerenciamento de Projetos	E-mail Corporativo
Ameaça	Contaminação por Trojans e Malwares;	Roubo/Exclusão de Informações	Acesso não autorizado a documentos	Envio de Phishing
Vulnerabilidade	Sistema desprotegido; Aplicativos Não licenciados.	Falta de sistema para back-up	Aplicação não criptografada	Coleta de informações confidenciais

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.		PFS-003-2025
			Versão: 1.0
	Classificação: interna		Última revisão: 23/05/2025

Classificação	B (4-2)	A (4-4)	B (3-3)	A (3-5)
Contingência	Uso de Anti-Vírus; Instalação de softwares permitida somente a T.I;	Utilização de Sistema de Back-up; Monitoria de entrada de dados	Aplicação de Criptografia a documentos sensíveis	Treinamento de operadores; filtros anti-phishing

LEGENDA						
PROBABILIDADE	5	B	A	A	A	A
	4	B	B	A	A	A
	3	C	B	B	A	A
	2	C	C	B	B	A
	1	D	C	C	B	B
	(H+V)	1	2	3	4	5
		IMPACTO				


NÍVEIS DE TRATAMENTO	
A	Ação imediata - Intolerável
B	Ação Média e Curto Prazo
C	Monitoramento e Gestão
D	Risco Controlável

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

9. 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.

FLUXO DE TRABALHO DOS PERÍMETROS IRRIGADOS ADMINISTRADOS PELA CODE SECURITY


INFORMAÇÃO	ORIGEM	PROCESSAMENTO /TRANSFORMAÇÃO	SAÍDA	AMEAÇAS/ VULNERABILIDADE	PROPOSTA DE SOLUÇÃO
Concessão de lotes irrigados	Cadastro de pequenos e médios agricultores	Verificação de critérios e liberação de lote	Registro da concessão no sistema	Concessões duplicadas; concessão indevida por falhas no critério Vazamento de dados pessoais Sistema indisponível	<ul style="list-style-type: none"> Implementação de validação automática de CPF/CNPJ e histórico de concessão. (Backup e redundância do sistema cadastral) Criptografia dos dados sensíveis Autenticação multifator para acesso ao sistema
Cobrança da tarifa d'água	Sistema de medição / consumo por lote	Cálculo automático com base em parâmetros (área, consumo)	Emissão de boletos / débito automatizado	Cálculos incorretos; falha na cobrança; acesso indevido a dados financeiros	<ul style="list-style-type: none"> Auditoria periódica; uso de gateway de pagamento seguro; integração com banco; logs de transação
Suporte técnico	Relatórios de campo dos técnicos e engenheiros	Registro das ações de assistência e laudos técnicos	Histórico técnico atualizado por beneficiário	Perda de dados; inconsistência nos registros; má interpretação dos dados	<ul style="list-style-type: none"> Sistema mobile offline com sincronização; padronização dos relatórios; controle de versão
Manutenção dos perímetros	Solicitações, vistorias técnicas	Agendamento, registro de obras, atualização do status	Agenda de manutenção e relatórios de execução	Falhas de comunicação; atraso por má gestão de cronograma; falta de controle nos materiais	<ul style="list-style-type: none"> Sistema de ordens de serviço digital; rastreamento de tarefas; painel de status em tempo real
Aquisição de equipamentos / envio de equipe	Solicitação por técnicos e gestores	Aprovação de requisição, compra e despacho logístico	Equipamentos entregues /	Compra indevida; superfaturamento; desvios; ausência de rastreabilidade	<ul style="list-style-type: none"> Workflow com aprovação eletrônica; integração com ERP

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

			<i>Equipe deslocada</i>		<i>público; rastreamento via GPS/logística</i>
<i>Resolução de problemas</i>	<i>Reclamações / incidentes do campo</i>	<i>Análise de causa, despacho de solução, feedback</i>	<i>Problema resolvido/ documentado</i>	<i>Falta de resposta; perda do histórico; reincidência do mesmo problema</i>	<ul style="list-style-type: none"> <i>Sistema de chamados integrado; categorização de problemas; SLA e notificações automatizadas</i>
<i>Captação de recursos</i>	<i>Projetos, editais, propostas técnicas</i>	<i>Preparação de documentos e envio para órgãos financiadores</i>	<i>Recursos recebidos ou propostas rejeitadas</i>	<i>Perda de prazos; inconsistência nos documentos; violação de confidencialidade</i>	<ul style="list-style-type: none"> <i>Calendário de prazos com alertas; controle de versão dos documentos; acesso restrito a documentos sensíveis</i>

10.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.

CATEGORIA	ITEM	CUSTO
CAPEX	Computadores (03 - Manutenção, 07-Tarifas, 05 - Suporte)	R\$ 75.000,00
	- 15 servidores a R\$ 5.000,00 cada	
CAPEX	Storage	R\$ 218.000,00
	- Discos SSD (20 - 1,92TB = 38,4 TB) -Licenças de Software -Switch de Rede -Treinamento técnico -Infraestrutura(cabos, rack, etc)	
CAPEX	Equipamentos de Rede	R\$ 80.000,00
	- Roteadores, switches, firewalls	
CAPEX	Equipamentos para a manutenção dos perímetros	R\$ 20.000,00
	- Placas de identificação e registros dos equipamentos adquiridos para a realização das manutenções	
Total CAPEX		R\$ 393.000,00

	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

CATEGORIA	ITEM	CUSTO
OPEX (anual)	Manutenção de Hardware	R\$ 2.500.000,00
	- Contratos de manutenção e reparo	
OPEX (anual)	Energia Elétrica	R\$ 50.000,00
	- Custo de consumo de energia	
OPEX (anual)	Suporte Técnico	R\$ 40.000,00
	- Contrato de suporte técnico	
OPEX (anual)	Atualizações de Software	R\$ 50.000,00
	- Licenças e atualizações de software	
Total OPEX (anual)		R\$ 2.640.000,00

11. 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:


 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

Figura 4. Código do menu de identificação

```

Program.cs 4 X
Program.cs > Program > Main
1  using System;
2
3  0 references
4  class Program
5  {
6      0 references
7      static void Main(string[] args)
8      {
9          string repetir;
10
11         do
12         {
13             Console.Clear();
14             Console.WriteLine("Coleta de Informações Básicas");
15
16             Console.Write("Digite seu nome: ");
17             string nome = Console.ReadLine();
18
19             Console.Write("Digite sua idade: ");
20             int idade;
21             while (!int.TryParse(Console.ReadLine(), out idade))
22             {
23                 Console.Write("Idade inválida. Digite um número inteiro: ");
24             }
25
26             Console.Write("Digite sua cidade: ");
27             string cidade = Console.ReadLine();
28
29             Console.Write("Digite seu CPF ou CNPJ: ");
30             string documento = Console.ReadLine();
31
32             Console.Write("Digite sua renda familiar: R$ ");
33             decimal renda;
34             while (!decimal.TryParse(Console.ReadLine(), out renda))
35             {
36                 Console.Write("Renda inválida. Digite um valor numérico: R$ ");
37             }
38
39             Console.WriteLine("\n- Informações Coletadas -");
40             Console.WriteLine($"Nome: {nome}");
41             Console.WriteLine($"Idade: {idade} anos");
42             Console.WriteLine($"Cidade: {cidade}");
43             Console.WriteLine($"CPF/CNPJ: {documento}");
44             Console.WriteLine($"Renda Familiar: R$ {renda:N2}");
45
46             if (renda <= 3000)
47             {
48                 Console.WriteLine("Status: APTO a participar.");
49             }
50             else
51             {
52

```

FONTE: Elaborado pelos próprios autores (2025)


 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

Figura 5. Código do menu de identificação

```

49      {
50          Console.WriteLine("Status: Infelizmente, NÃO está apto a participar.");
51      }
52
53      Console.Write("\nDeseja inserir outra pessoa? (sim / não): ");
54      repetir = Console.ReadLine().ToLower();
55
56      } while (repetir == "sim");
57
58      Console.WriteLine("\nPrograma encerrado. Pressione qualquer tecla para sair.");
59      Console.ReadKey();
60  }
61  }

```

FONTE: Elaborado pelos próprios autores (2025)

Figura 6. Impressão do Menu de Identificação

```

- Informações Coletadas -
Nome: Cláudio
Idade: 65 anos
Cidade: Teresina
CPF/CNPJ: 00770720270
Renda Familiar: R$ 2,500.00
Status: apto a participar.

Deseja inserir outra pessoa? (sim / não): 

```

FONTE: Elaborado pelos próprios autores (2025)

Figura 6. Impressão do Menu de Identificação

```

- Informações Coletadas -
Nome: Cláudia
Idade: 62 anos
Cidade: Salvador
CPF/CNPJ: 00170533340
Renda Familiar: R$ 3,002.00
Status: Infelizmente, NÃO está apto a participar.

```

FONTE: Elaborado pelos próprios autores (2025)


 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.		PFS-003-2025
			Versão: 1.0
	Classificação: interna		Última revisão: 23/05/2025

Figura 7. Código do Menu de Inventário

```

1  using System;
2  using System.Collections.Generic;
3
4  0 references
5  class Program
6  {
7      18 references
8      class Item
9      {
10         2 references
11         public string Categoria { get; set; }
12         2 references
13         public string Nome { get; set; }
14         2 references
15         public int Quantidade { get; set; }
16
17         13 references
18         public Item(string categoria, string nome, int quantidade)
19         {
20             Categoria = categoria;
21             Nome = nome;
22             Quantidade = quantidade;
23         }
24     }
25
26     3 references
27     static void MostrarInventario(List<Item> inventario, string titulo)
28     {
29         Console.WriteLine($"\\n--- {titulo} ---");
30         Console.WriteLine("{0,-20} {1,-40} {2,10}", "Categoria", "Item", "Quantidade");
31
32         foreach (var item in inventario)
33         {
34             Console.WriteLine("{0,-20} {1,-40} {2,10}", item.Categoria, item.Nome, item.Quantidade);
35         }
36
37         Console.WriteLine(); // linha em branco
38     }
39 }

```

FONTE: Elaborado pelos próprios autores (2025)


 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

Figura 8. Código do Menu de Inventário

```

33 static void Main()
34 {
35     var inventarioHardware = new List<Item>
36     {
37         new Item("Computadores", "Desktop i5, 8GB RAM, SSD 256GB", 15),
38         new Item("Servidores", "Servidor rack", 15),
39         new Item("Armazenamento", "SSD 1TB", 20),
40         new Item("Rede e conectividade", "Switch Gerenciável", 2),
41         new Item("Rede e conectividade", "Roteador", 4),
42         new Item("Rede e conectividade", "Cabeamento estruturado", 0),
43         new Item("Energia", "Nobreak 1500VA", 5),
44         new Item("Energia", "Estabilizadores 500VA", 15)
45     };
46
47     var inventarioSoftware = new List<Item>
48     {
49         new Item("Sistema Operacional", "Windows 11 Pro", 15),
50         new Item("Sistema Operacional", "Windows Server 2022 Standard", 15),
51         new Item("Pacote Office", "Microsoft 365 Business Standard", 15),
52         new Item("Firewall de rede", "Firewall Fortigate", 2),
53         new Item("Firewall de software", "pfSense CE", 1)
54     };
55
56     int opcao;
57     do
58     {
59         Console.WriteLine("Menu de Inventário - Code Security");
60         Console.WriteLine("Escolha uma opção:");
61         Console.WriteLine("1. Inventário de Hardware");
62         Console.WriteLine("2. Inventário de Software");
63         Console.WriteLine("3. Inventário de Hardware e Software");
64         Console.WriteLine("0. Sair");
65         Console.Write("Escolha uma opção: ");
66
67         if (!int.TryParse(Console.ReadLine(), out opcao))
68         {
69             Console.WriteLine("Entrada inválida.\n");
70             continue;
71         }
72

```

FONTE: Elaborado pelos próprios autores (2025)


 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

Figura 9. Código do Menu de Inventário

```

73         switch (opcao)
74         {
75             case 1:
76                 MostrarInventario(inventarioHardware, "Inventário de Hardware");
77                 break;
78             case 2:
79                 MostrarInventario(inventarioSoftware, "Inventário de Software");
80                 break;
81             case 3:
82                 var mesclado = new List<Item>();
83                 mesclado.AddRange(inventarioHardware);
84                 mesclado.AddRange(inventarioSoftware);
85                 MostrarInventario(mesclado, "Inventário de Hardware e Software");
86                 break;
87             case 0:
88                 Console.WriteLine("Saindo...");
89                 break;
90             default:
91                 Console.WriteLine("Opção inválida.\n");
92                 break;
93         }
94     } while (opcao != 0);
95 }
96 }
97 }
98

```

FONTE: Elaborado pelos próprios autores (2025)

Figura 10. Impressão do Menu de Inventário

```

Menu de Inventário - Code Security
Escolha uma opção:
1. Inventário de Hardware
2. Inventário de Software
3. Inventário de Hardware e Software
0. Sair
Escolha uma opção:

```

FONTE: Elaborado pelos próprios autores (2025)


 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

Figura 11. Impressão do Menu de Inventário

--- Inventário de Hardware ---		
Categoria	Item	Quantidade
Computadores	Desktop i5, 8GB RAM, SSD 256GB	15
Servidores	Servidor rack	15
Armazenamento	SSD 1TB	20
Rede e conectividade	Switch Gerenciável	2
Rede e conectividade	Roteador	4
Rede e conectividade	Cabeamento estruturado	0
Energia	Nobreak 1500VA	5
Energia	Estabilizadores 500VA	15

FONTE: Elaborado pelos próprios autores (2025)

Figura 12. Impressão do Menu de Inventário

--- Inventário de Software ---		
Categoria	Item	Quantidade
Sistema Operacional	Windows 11 Pro	15
Sistema Operacional	Windows Server 2022 Standard	15
Pacote Office	Microsoft 365 Business Standard	15
Firewall de rede	Firewall Fortigate	2
Firewall de software	pfSense CE	1

FONTE: Elaborado pelos próprios autores (2025)

Figura 13. Impressão do Menu de Inventário

--- Inventário de Hardware e Software ---		
Categoria	Item	Quantidade
Computadores	Desktop i5, 8GB RAM, SSD 256GB	15
Servidores	Servidor rack	15
Armazenamento	SSD 1TB	20
Rede e conectividade	Switch Gerenciável	2
Rede e conectividade	Roteador	4
Rede e conectividade	Cabeamento estruturado	0
Energia	Nobreak 1500VA	5
Energia	Estabilizadores 500VA	15
Sistema Operacional	Windows 11 Pro	15
Sistema Operacional	Windows Server 2022 Standard	15
Pacote Office	Microsoft 365 Business Standard	15
Firewall de rede	Firewall Fortigate	2
Firewall de software	pfSense CE	1

FONTE: Elaborado pelos próprios autores (2025)


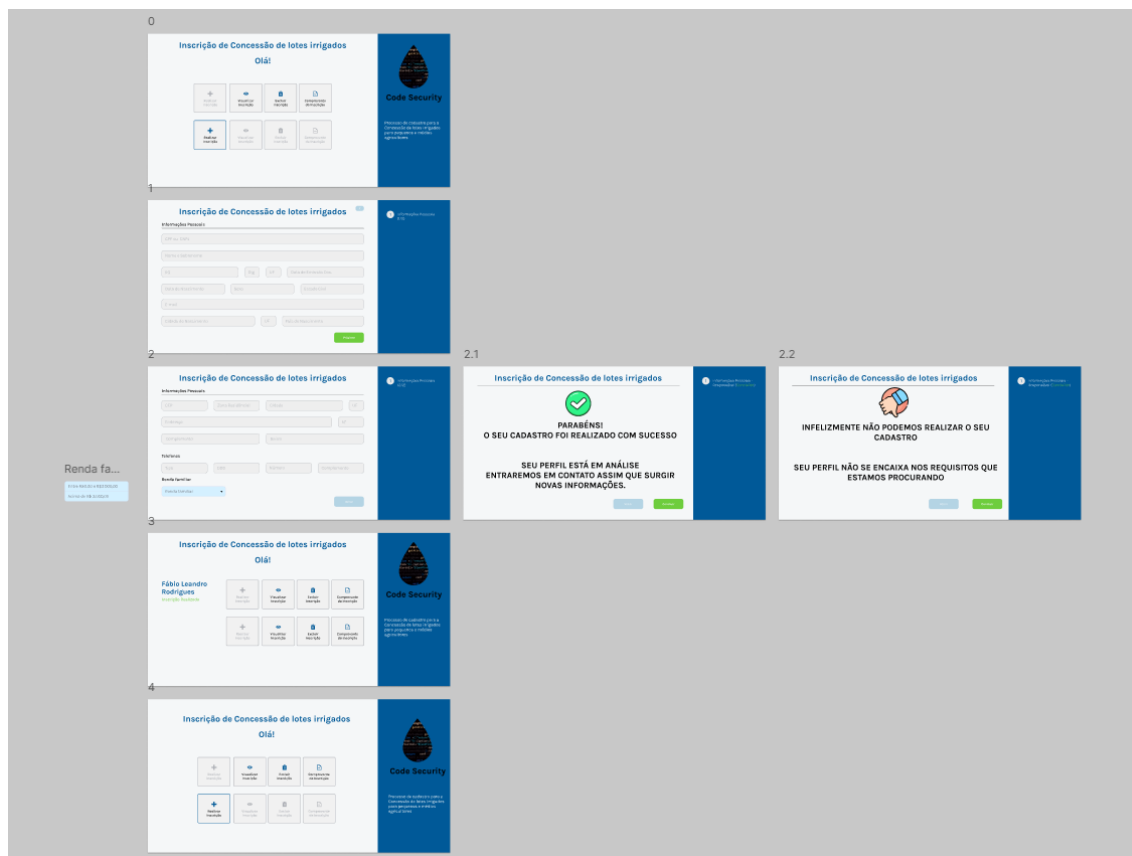

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

Figura 14. Protótipo navegável (FIGMA)




FONTE: Elaborado pelos próprios autores (2025)

 CODE SECURITY	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025


12. REALIZAR UMA ANÁLISE DE RISCOS/CONTINUIDADE/CONTINGÊNCIA DOS ITENS DE SEGURANÇA FÍSICA E LÓGICA ENCONTRADOS NO ITEM 5 DA ETAPA 2.

PLANO DE TRATAMENTO DE RISCOS
1. Evitar o risco
2. Transferir o risco
3. Mitigar o risco
4. Aceitar o risco

RISCOS FÍSICOS				
Ativo	Conexão com a Internet	Servidores de Rede	Laptops	Dispositivos Móveis Corporativos
Valor	8000,00/mês	R\$5000,00/servidor	R\$4.600,00/laptop	R\$1200,00 /dispositivo
Ameaça	Rompimento ou erro físico na fibra;	Incêndio	Roubo/Furto	Roubo, perda ou uso indevido
Vulnerabilidade	Cabo de fibra exposto;	Falta de extintores/detectores de fumaça, ambiente mal climatizado	Falta de monitoramento e Alarmes	Falta de Rastreamento/Monitoramento
Classificação do Risco	A (5+4)	A (5+3)	C (3+2)	C (3+1)
Opção de Tratamento	3. Mitigar o risco	3. Mitigar o risco; 2. Transferir o risco	1. Evitar o Risco	3. Mitigar o risco
Contingência	Uso de ISPs secundários;	Uso de termostatos, extintores de CO2; contratar seguradora	Uso de câmeras de monitoramento; Aplicação de travas antifurto (Kensington)	Restrição somente a serviços essenciais; Rastreamento mediante Chips
Valor Contingência	R\$1400,00/mês	R\$2500,00/mês	R\$500,00/equip	R\$50,00/equip
Classificação Residual	C (3+2)	B (4+2)	C (2+2)	C (2+1)

	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

RISCOS LÓGICOS				
Ativo	Sistema Operacional	Data Center	Sistema de Gerenciamento de Projetos	E-mail Corporativo
Valor	R\$1500,00/licença	R\$ 75.000,00	R\$ 5.000,00/mês	R\$76,00/usuário
Ameaça	Contaminação por Trojans e Malwares	Roubo/Exclusão de Informações	Acesso não autorizado a documentos	Envio de Phishing
Vulnerabilidade	Sistema desprotegido; uso de aplicativos não licenciados	Falta de um sistema secundário de back-up	Sistema não criptografado	Coleta de informações confidenciais
Classificação do Risco	A (4+3)	A (3+4)	B (3+3)	A (3+5)
Opção de Tratamento	3. Mitigar o risco	3. Mitigar o risco	3. Mitigar o risco	3. Mitigar o risco
Contingência	Uso de Anti-Vírus; Instalação de softwares permitida somente a T.I;	Utilização de Sistema de Back-up; Monitoria de entrada de dados	Atualização frequente com fornecedor; Aplicação de Criptografia a documentos	Treinamento para operadores e filtros anti-phishing
Valor Contingência	R\$350,00/mês	400,00/mês	~R\$50,00/usuário	R\$--,--
Classificação Residual	B (4+2)	C (2+2)	D (1+1)	B (2+3)

	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

GLOSSÁRIO

Ativo: Qualquer recurso, hardware, software ou informação valiosa para a organização, que precisa ser protegido.

Análise de Riscos: Processo de identificação, avaliação e priorização de riscos para a segurança da informação, com o objetivo de minimizar impactos.

Backup: Cópia de segurança de dados, criada para garantir a recuperação em caso de perda ou corrupção das informações originais.

CAPEX: Investimentos de capital (ex: compra de servidores, infraestrutura de rede).

Classes de Segurança da Informação: Categorias que abrangem aspectos de proteção de dados, como confidencialidade, integridade e disponibilidade.

Compliance: Conjunto de procedimentos que assegurem que a empresa esteja em conformidade com leis, regulamentos e políticas internas.

Contingência: Plano de ação destinado a manter ou restaurar operações normais após incidentes que afetam a segurança ou funcionamento dos sistemas.

Dados Confidenciais: Informações sensíveis que precisam ser protegidas contra acesso, modificação ou divulgação não autorizada.

Erro Operacional: Falha humana ou sistêmica que compromete processos internos, podendo afetar setores como produção, financeiro ou atendimento.


Evento Suscetível: Ocorrência que pode comprometer a segurança da informação, como falhas de hardware, desastres naturais ou fraudes.

Falha de Comunicação: Problemas em meios ou equipamentos de comunicação que impactam a transmissão segura e eficaz de dados.

Falha de Hardware: Defeito ou quebra em componentes físicos como servidores, HDs, roteadores, que pode interromper serviços críticos.

Fraude: Ato intencional de enganar, roubar ou manipular dados, processos ou ativos com o objetivo de ganho ilícito.

LGPD (Lei Geral de Proteção de Dados): Legislação brasileira que regula o tratamento de dados pessoais, impondo responsabilidades às organizações.

	TAREFA 3 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-003-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 23/05/2025

Mitigação: Ações destinadas a reduzir a probabilidade ou o impacto de um risco.

OPEX: Despesas operacionais recorrentes (ex: energia, manutenção, suporte).

Pen Drive: Dispositivo portátil de armazenamento de dados, muito suscetível a perdas de dados e malware.

Phishing: Técnica fraudulenta para obtenção de informações confidenciais através de e-mails ou mensagens falsas.

Plano de Continuidade de Negócios: Estratégia para garantir que as operações críticas de uma organização continuem durante e após um incidente grave.

Processo de Negócio: Sequência de atividades organizadas para produzir um resultado específico para a empresa.

Risco Físico: Ameaças aos ativos físicos da empresa, como incêndios, furtos ou danos estruturais.

Risco Lógico: Ameaças que afetam os sistemas de informação, como vírus, malwares e ataques cibernéticos.

Segurança da Informação: Conjunto de práticas que visam proteger as informações de uma organização contra acessos não autorizados, alterações e destruições.

TI Invisível: Tecnologias e dispositivos utilizados na organização, mas que não são oficialmente controlados ou monitorados pela equipe de TI.

Treinamento de Segurança: Capacitação contínua dos funcionários para conscientizá-los sobre boas práticas e prevenção de riscos de segurança da informação.

Vulnerabilidade: Fragilidade que pode ser explorada para comprometer a segurança de ativos da organização.