
 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

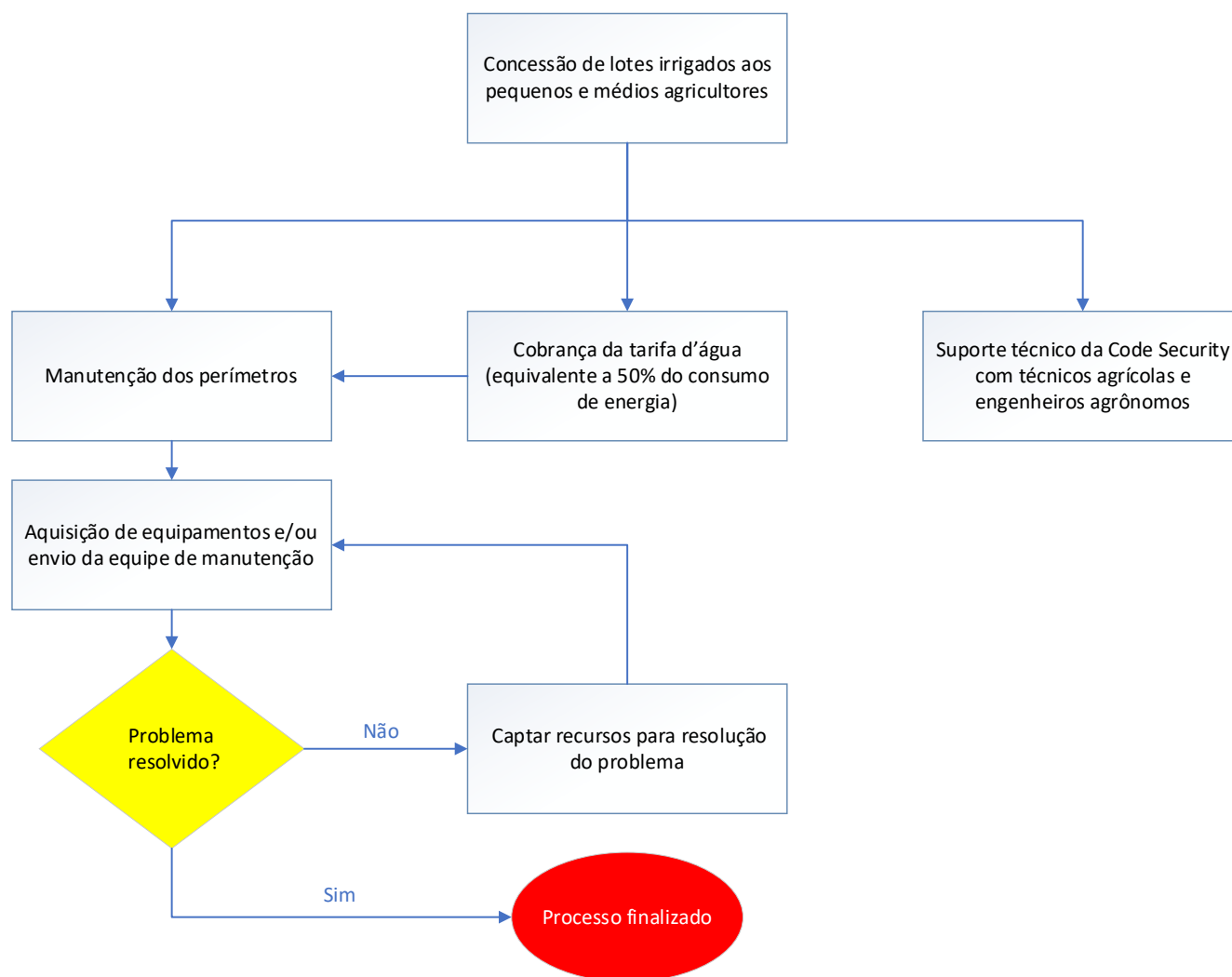
SUMÁRIO

1. ESCOLHER 1 PROCESSO DE NEGÓCIO ENTRE OS QUE FORAM IDENTIFICADOS NA ETAPA 1 E DETALHÁ-LO USANDO UMA FERRAMENTA DE CONSTRUÇÃO DE FLUXOGRAMA.	1
2. 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.	2
3. MAPEAR ITENS RELACIONADOS À TI INVISÍVEL NA ORGANIZAÇÃO.	6
4. IDENTIFICAR DISPOSITIVOS PESSOAIS UTILIZADOS NA ORGANIZAÇÃO.	8
5. IDENTIFICAR RISCOS DE SEGURANÇA FÍSICA E LÓGICA DISCUTIDOS NO MF DE FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO E ENCONTRADOS NO CONTEXTO ORGANIZACIONAL ESTUDADO.	9
5.1. Mapas de Riscos	10
GLOSSÁRIO.....	12

 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025


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

Figura 1. 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.


 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

2. 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	A análise de riscos envolve identificar vulnerabilidades, avaliar impactos financeiros, operacionais e reputacionais, e implementar medidas preventivas como controles internos rigorosos,	Combater fraudes e sabotagens, uma empresa deve adotar controles internos rigorosos, realizar auditorias frequentes e implementar sistemas de segurança

 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025


		<p>corrupção e superfaturamento. Já a produção pode ser sabotada por danos aos processos, e o marketing pode ser manipulado para prejudicar a imagem da empresa.</p>	<p>segurança de TI e treinamento de funcionários.</p>	<p>robustos. Treinamentos 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>
Erros Operacionais	<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</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>

 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

			tempo real e 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


 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

	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 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

3. 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 gerenciados pela gerência de TI da empresa.	Mapear riscos e implantar uma plataforma oficial de registros pelo setor de T.I.
3	Divisão de Poços	Pen drive, softwares instalados localmente e serviços de	Code Security (Computadores), Funcionário do setor (pen drive)	1	MÉDIO. A utilização de softwares de produtividade sem licença, não atualizados e	Aplicar LGPD. Necessário mapeamento de riscos, uma política de controle, uso (softwares, hardwares


 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

		armazenamento em nuvem.			serviços de armazenamento em nuvem logados em suas contas pessoais compromete a confidencialidade e integridade das informações.	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 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025


4. 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 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

5. 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

 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

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

5.1. 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/detectores de fumaça, ambiente mal climatizado	Falta de monitoramento e Alarmes	Falta de Rastramento/Monitoramento
Classificação	A (5-4)	A (5-3)	C (3-2)	C (3-1)


 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

Contingência	Diversificar o uso de ISPs;	Uso de termostatos, extintores de CO2, ares condicionados	Uso de câmeras de monitoramento; Aplicação de travas anti-furto (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
Classificação	B (4-2)	A (4-4)	B (3-3)	A (3-5)
Contingência	Uso de Anti-Virus; 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 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

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.

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

Compliance: Conjunto de procedimentos que asseguram 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.

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

 CODE SECURITY	TAREFA 2 – PROJETO FUNDAMENTOS DE SISTEMAS.	PFS-002-2025
		Versão: 1.0
	Classificação: interna	Última revisão: 27/04/2025

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.