Sistematização

Disciplina:	**Auditoria de Segurança da Informação**
Prof.	**Luiz Claudio Diogo Reis**
Aluno:	
Matrícula:	
Desafio Prático da Sistematização:	Planejando, Executando e Reportando uma Auditoria de Segurança da Informação em Sistemas Empresariais.
Contexto (Situação Problema):	A empresa fictícia TechSecure, especializada em soluções digitais para o setor financeiro, tem enfrentado sérias dificuldades na segurança da informação e na gestão de seus sistemas de informação. Após um incidente de vazamento de dados sensíveis de clientes, a diretoria determinou a realização de uma auditoria de segurança da informação para identificar falhas e fortalecer os controles internos. Além do vazamento de dados, outros problemas críticos foram identificados pela equipe de TI: - Ausência de um controle robusto de acessos: Funcionários mantêm privilégios administrativos mesmo após mudanças de função, aumentando o risco de acessos indevidos. - Falta de política formal de segurança: A empresa não possui diretrizes bem definidas para o uso seguro de seus sistemas de informação. - Backups inconsistentes: Relatórios indicam que os backups nem sempre são realizados conforme as diretrizes internas, comprometendo a disponibilidade dos dados. - Uso de senhas fracas e reutilizadas: Muitos colaboradores utilizam a mesma senha para diferentes sistemas, expondo a organização a ataques de engenharia social. - Sistemas desatualizados: Alguns softwares utilizados para operações financeiras não recebem atualizações há mais de um ano, tornando-se vulneráveis a ataques cibernéticos.

	- Falta de conformidade com normas e regulações: A empresa não implementou integralmente os requisitos da LGPD (Lei Geral de Proteção de Dados) e da ISO 27001, aumentando os riscos legais e financeiros. Diante desse cenário, você foi contratado para planejar, executar e reportar uma auditoria de segurança da informação, com o objetivo de avaliar a segurança dos sistemas da empresa TechSecure e propor, em um relatório de auditoria, soluções práticas para mitigar os riscos. Essa atividade de Sistematização será realizada em três etapas, conforme descrito a seguir.
Fase 1 - Planejamento da Auditoria:	Nesta fase da atividade você deverá identificar os seguintes elementos: a. Definição do escopo da auditoria: Quais sistemas, processos e controles serão auditados? b. Identificação dos objetivos e principais riscos da auditoria: Qual é o objetivo da auditoria? E quais são os riscos envolvidos? c. Seleção de normas e frameworks aplicáveis (ISO 27001, LGPD, COBIT, COSO, etc.): Quais frameworks, normas, leis ou padrões de mercado podem ser utilizados nesta auditoria? d. Técnicas e procedimentos de auditoria: Quais técnicas e procedimentos de auditoria podem ser utilizados nesta atividade, por exemplo, análise documental, entrevistas, testes de conformidade?
Fase 2 - Execução da Auditoria:	Nesta fase da atividade você deverá identificar os seguintes elementos: a. Aplicação prática das técnicas de auditoria: Quais controles serão testados nesta auditoria? b. Identificação de falhas nos controles internos: Quais são os possíveis achados (vulnerabilidades) nos controles? c. Avaliação da eficácia dos processos de segurança dos sistemas de informação: Diante das falhas identificadas na auditoria, como você avalia os resultados? A empresa está sujeita a um risco alto, médio ou baixo?
Fase 3 - Elaboração do Relatório Final	Nesta fase da atividade você deverá relatar o resultado da auditoria relacionando os seguintes elementos: a. Registro dos principais achados da auditoria: Quais são os principais achados nesta auditoria? b. Sugestões de melhoria para mitigar riscos identificados: Quais recomendações podem ser propostas como resultado do trabalho?

	c. Conclusão e considerações finais: Qual é a conclusão do resultado do trabalho e o que a auditoria espera por parte da área gestora do sistema?
Estrutura do Documento Final da Sistematização:	Diante das informações relacionadas acima, discuta com os seus colegas de turma e com seu professor como essas informações podem ser apresentadas no documento final da Sistematização. Vou deixar algumas sugestões para a estrutura do trabalho final, não exaustivas, como *insights* para realização da atividade. 1. Introdução: Introdução ao tema 2. Objetivo: Objetivo do trabalho de auditoria 3. Escopo: Escopo do trabalho de auditoria. 4. Período de realização: Período de execução da auditoria 5. Equipe: Equipe participante do trabalho de auditoria 6. Achados (Apontamentos): Principais apontamentos identificados no trabalho de auditoria 7. Técnicas e Procedimentos: Registro das técnicas e procedimentos de auditoria aplicados 8. Testes: Relato dos testes executados 9. Nível de risco: Nível de risco atribuído (Alto, Médio ou Baixo), com justificativa. 10. Recomendações: Sugestões de melhorias para serem implementadas 11. Conclusão e Considerações Finais: Conclusão sobre o resultado do trabalho de auditoria 12. Outros tópicos para atingirem o objetivo do trabalho