Gestão Integrada de Segurança da Informação e Continuidade de Negócios

Nome: *Gabriel Domingues Silva* ***Turma:*** *25E1-1*

Tema: TP1

Prof. Fabio Campos Chaves
Instituto Infnet

Conteúdo

1 Qual é o principal objetivo de um Sistema de Gestão de Segurança da Informação (SGSI)?

O principal objetivo de um SGSI é garantir a **confidencialidade**, **integridade** e **disponibilidade** das informações dentro de uma organização, minimizando riscos e protegendo ativos contra ameaças.

2 De acordo com a ISO 27001, o que é um ativo de informação?

De acordo com a ISO 27001, um ativo de informação é qualquer recurso que tenha valor para a organização e que necessite de proteção. Isso inclui dados digitais, documentos físicos, hardware, software e o conhecimento dos colaboradores.

3 Qual das opções a seguir é um controle de segurança descrito no Anexo A da ISO/IEC 27001? Justifique a escolha.

A opção correta é o **Gerenciamento de continuidade de negócios**. A ISO/IEC 27001 descreve controles para garantir a resiliência organizacional diante de incidentes que possam comprometer a segurança da informação.

4 O ciclo PDCA é utilizado para gerenciar sistemas de gestão. Descreva objetivamente cada etapa do ciclo.

- **Plan (Planejar)**: Definir políticas, objetivos e processos para a gestão da segurança da informação.
- **Do (Executar)**: Implementar os processos e controles planejados.
- **Check (Verificar)**: Monitorar e medir os processos em relação aos objetivos estabelecidos.
- **Act (Agir)**: Tomar ações corretivas e de melhoria com base na análise dos resultados.

5 Na avaliação de riscos, o que deve ser considerado prioritariamente? Justifique.

Deve-se considerar prioritariamente a **probabilidade e impacto** dos riscos. A avaliação de riscos deve focar na identificação de ameaças que possam comprometer a confidencialidade, integridade e disponibilidade das informações.

6 Qual é a importância de implementar controles de acesso?

Os controles de acesso garantem que apenas usuários autorizados possam acessar informações sensíveis, prevenindo acessos não autorizados e minimizando o risco de violações de dados.

7 A ISO/IEC 27001 exige que as organizações realizem auditorias internas periódicas. Qual o objetivo principal dessas auditorias?

As auditorias internas têm como objetivo **avaliar a conformidade** do SGSI com os requisitos da norma, identificar falhas e sugerir melhorias contínuas para fortalecer a segurança da informação.

8 Como deve ser tratada uma não conformidade identificada no SGSI?

Uma não conformidade deve ser documentada, analisada e corrigida com ações corretivas que eliminem suas causas, evitando sua recorrência.

9 De acordo com a ISO 27001, quais são os itens obrigatórios no escopo de um SGSI?

- Definição dos ativos de informação cobertos.
- Identificação das partes interessadas.
- Requisitos de segurança aplicáveis.

10 O que é a Declaração de Aplicabilidade (SoA) na ISO 27001?

A SoA é um documento que lista os controles de segurança selecionados, justificando sua inclusão ou exclusão no SGSI de acordo com a avaliação de riscos.

11 Qual é a melhor prática para garantir que os controles de segurança da informação sejam eficazes?

A melhor prática envolve a realização de **testes periódicos**, auditorias e monitoramento contínuo da eficácia dos controles implementados.

12 O que é necessário para que um controle de acesso seja considerado bem implementado?

Um controle de acesso eficaz deve incluir autenticação forte, segregação de funções e monitoramento contínuo dos acessos.

13 No gerenciamento de fornecedores, como a ISO/IEC 27001 orienta a proteção de informações?

A norma exige que organizações estabeleçam contratos com cláusulas de segurança, monitorem o cumprimento dos requisitos e realizem avaliações periódicas dos fornecedores.

14 Estudo de Caso: Análise de Riscos

Para mitigar o risco de ataques de ransomware, a empresa deve:

- Implementar backups seguros e periódicos.
- Aplicar políticas de controle de acesso restritivo.
- Monitorar e detectar atividades suspeitas.

15 Estudo de Caso: Controles de Acesso

Para evitar acessos indevidos ao sistema financeiro:

- Implementar o princípio do menor privilégio.
- Utilizar autenticação multifator.
- Monitorar acessos e revisar permissões regularmente.

16 Estudo de Caso: Auditoria e Melhoria Contínua

Plano de ação para backups:

- Estabelecer uma política de backups periódicos.
- Implementar backups redundantes e testá-los regularmente.
- Realizar auditorias internas para verificar conformidade.

17 Estudo de Caso: Gestão de Fornecedores

Plano para fornecedores alinhados à ISO 27001:

- Exigir conformidade com normas de segurança.
- Monitorar práticas de segurança dos fornecedores.
- Realizar auditorias e avaliações periódicas.

18 Estudo de Caso: Conformidade com a Declaração de Aplicabilidade (SoA)

Para corrigir a falha na implementação de um controle da SoA:

- Revisar e atualizar a implementação do controle.
- Identificar e corrigir falhas no processo.
- Monitorar continuamente para evitar reincidências.