# Respostas Atividade

**Nome: Christopher Yohan Reges Perius**

**Matéria: Segurança da informação**

a) **Segurança da informação**

**Segurança da informação é o conjunto de práticas, processos e controles que visam proteger dados e ativos informacionais contra perdas, acessos não autorizados, alterações indevidas e indisponibilidade. Inclui pilares como confidencialidade, integridade e disponibilidade. Também envolve pessoas, tecnologia e processos, buscando garantir que a informação esteja acessível apenas a quem de direito, que não seja alterada indevidamente e que esteja disponível quando necessária. Em uma organização, envolve políticas, controles técnicos e treinamentos.**

**b) Incidente de segurança**

**Incidente de segurança é qualquer evento ou série de eventos que ameaçam a confidencialidade, integridade ou disponibilidade da informação. Pode ser desde um acesso não autorizado até a divulgação acidental de dados ou uma falha que cause indisponibilidade de sistemas. Um incidente exige análise e resposta para conter o dano, recuperar serviços e, quando necessário, notificar partes interessadas. O objetivo da resposta a incidentes é minimizar impacto e restaurar operações.**

**c) Ativo**

**Ativo de informação é qualquer recurso que tenha valor para a organização e que contenha ou suporte informação — por exemplo, bases de dados, servidores, documentos, aplicações, pessoal ou até conhecimento. Ativos devem ser inventariados, classificados por criticidade e protegidos**

**proporcionalmente ao seu valor. A gestão de ativos permite priorizar controles e investimentos de segurança. Sem identificar ativos, não se pode avaliar risco corretamente.**

**d) Ameaça**

**Ameaça é qualquer circunstância ou evento com potencial para explorar uma vulnerabilidade e causar dano a um ativo. Pode ser humana (um atacante), natural (enchente) ou acidental (erro humano). Ameaças descrevem a possibilidade de ocorrência e costumam ser avaliadas quanto à probabilidade e ao impacto. Identificar ameaças ajuda a planejar controles preventivos e detectivos.**

**e) Vulnerabilidade**

**Vulnerabilidade é uma fraqueza ou falha em um ativo, processo ou controle que pode ser explorada por uma ameaça para causar dano. Exemplos: software sem atualização, configuração fraca, credenciais vazadas, ausência de segregação de funções. Vulnerabilidades não causam dano por si mesmas; elas são pontos que, se explorados, permitem à ameaça comprometer confidencialidade, integridade ou disponibilidade. Gestão de vulnerabilidades busca identificá-las, priorizá-las e remediá-las.**

**f) Risco**

**Risco é a combinação da probabilidade de ocorrência de um evento adverso (exploração de uma vulnerabilidade por uma ameaça) e o seu impacto sobre os ativos e objetivos da organização. Risco = Probabilidade × Impacto (conceitualmente). A análise de risco permite decidir quais controles implementar, quais riscos aceitar e quais mitigar. O tratamento de risco pode incluir aceitação, mitigação, transferência ou eliminação.**

**g) Ataque**

**Ataque é a ação executada por um agente (intencional) que visa explorar vulnerabilidades para comprometer a segurança de um ativo — por exemplo,**

**um exploit, phishing, DDoS ou malware. Um ataque resulta em incidentes quando bem-sucedido. Classificações comuns: interceptação, modificação, interrupção e fabricação (falsificação). A defesa inclui detecção, prevenção, resposta e recuperação.**

**h) Impacto**

**Impacto é a consequência ou dano causado por um incidente ou ataque sobre a organização, medido em termos financeiros, operacionais, de reputação, legais ou de conformidade. Pode ser perda de receita, clientes, multas por quebra de privacidade (ex.: LGPD), ou paralisação de serviços críticos. Avaliar impacto ajuda a priorizar controles e planos de recuperação (DR/BCP).**

**Questão 02**

**Resposta: C) É uma falha ou fraqueza que pode ser explorada por uma ameaça para causar dano.**
**Justificativa: A opção C corresponde à definição técnica de vulnerabilidade: uma fraqueza que, se explorada, permite dano. As outras opções descrevem ataque, impacto, ativo ou políticas.**

---

**Questão 03**

**Alternativa correta: B) I–1 II–2 III–3 IV–4.**

---

**Questão 04**

**Alternativa correta: A) as assertivas I e II são verdadeiras e II é justificativa correta de I.**

---

**Questão 05**

**Para proteger a confidencialidade dos ativos informacionais, uma organização deve aplicar controles técnicos, administrativos e físicos em conjunto. Como controles técnicos, destaco o uso de criptografia (dados em trânsito e em repouso), controles de acesso baseados em privilégios mínimos (IAM) e**

**soluções de prevenção de perda de dados (DLP) para detectar e bloquear exfiltração. Como controles administrativos, cito políticas claras de classificação de informação, processos de revisão de acesso e treinamento contínuo de funcionários sobre phishing e manuseio de dados sensíveis. No âmbito físico, controle o acesso a salas de servidores (cadeados, biometria, CCTV) e retenho logs de acesso. Um exemplo prático: criptografar a base de clientes, aplicar controle de acesso por função e exigir autenticação multifator para acesso remoto, além de treinamentos periódicos para reduzir o risco de vazamento por engenharia social.**

**Questão 06**

**Alternativa correta: B) as assertões I e II são verdadeiras, mas II não é justificativa correta de I.**

---

**Questão 07**

**Sequência: 4 – 1 – 3 – 1 – 2 – 3.**
**Alternativa correta: A) 4 – 1 – 3 – 1 – 2 – 3.**

---

**Questão 08 — Identificação de vulnerabilidades**

**(Para cada cenário, identifico uma possível vulnerabilidade explorável e relaciono ao princípio da SI.)**

**a) Mensageiro externo realizando entregas e coletas**
**Vulnerabilidade: Falta de controle de identidade e falta de verificação de inventário/recebimento. O mensageiro pode receber/entregar documentos sensíveis sem checagem, possibilitando vazamento (quebra de confidencialidade) ou perda física de documentos (disponibilidade). Medida: check-in/out com identificação, lacres, registro e restrições de acesso.**

**b) Ex-funcionários dispensados**
**Vulnerabilidade: Contas e credenciais não desativadas / falta de revogação de privilégios. Ex-funcionários podem acessar recursos ou reutilizar credenciais, afetando confidencialidade e autenticidade. Medida: processo de desligamento com revogação imediata de acessos, mudança de senhas compartilhadas e auditoria de logs.**

**c) Funcionário viajando e acessando rede remotamente**
**Vulnerabilidade: Uso de redes públicas inseguras e ausência de**

**VPN/autenticação forte. Isso expõe credenciais e tráfego a interceptação, comprometendo confidencialidade e integridade. Medida: exigir VPN corporativa, MFA e políticas de endpoint (patch e antivírus) para acesso remoto.**

**d) Uso de notebook pessoal sem cadastro**
**Vulnerabilidade: Dispositivo não gerenciado sem patches, sem antivírus, sem controle de inventário. Pode introduzir malware, exfiltrar dados ou quebrar integridade/confidencialidade. Medida: BYOD com registro no inventário, MDM/EDR, requisitos mínimos de segurança e segmentação de rede.**

---

**Questão 09**

**Alternativa correta: C) I–1, II–2, III–1, IV–3, V–4.**

**Questão 10**

**Alternativa correta: C)**

**27000: Vocabulário e conceitos fundamentais para SGSI.**

**27001: Estabelece requisitos normativos para certificação do SGSI.**

**27002: Apresenta controles de segurança e boas práticas de implementação.**
**27005: Fornece diretrizes para gestão de riscos de segurança da informação.**