Módulo 1 – Conceitos sobre requisitos de Segurança da Informação

1. Defina, com suas próprias palavras, o que é Segurança da Informação.
2. De acordo com a norma NBR ISO/IEC 27002:2005, quais são os ativos alvo de uma política de segurança da informação? Dê um exemplo de cada tipo.
3. Escreva, com suas próprias palavras, o que é um sistema seguro.
4. O que são confidencialidade, integridade e disponibilidade? Explique cada um deles.
5. A autenticação pode ser baseada em quais métodos?
6. O que é controle de acesso?
7. O que é irretratabilidade?
8. O que é autenticidade? Como ela se diferencia (ou se assemelha) à integridade?
9. O que é posse ou controle? De um exemplo de uma situação prática.
10. O que é utilidade? De um exemplo de uma situação prática.

Módulo 2 – Visão geral de Segurança da Informação no Brasil

1. Quais são os dois fatores recentes que impulsionaram as organizações a investirem mais em Segurança da Informação?
2. Na sua opinião, por que o Brasil é um dos países mais sujeitos a ataques cibernéticos?
3. Explique, com suas próprias palavras, os desafios encontrados pelas organizações no enfrentamento dos problemas relativos à Segurança da Informação.
4. Dentre as quinze tendências identificadas, quais delas se aplicariam a Pessoas?
5. Dentre as quinze tendências identificadas, quais delas se aplicariam a Processos?
6. Dentre as quinze tendências identificadas, quais delas se aplicariam a Tecnologias?
7. Na sua opinião, por que algumas empresas resistem a aumentar os investimentos em Segurança da Informação?
8. Qual(is) o(s) risco(s) que a adoção da política de Bring Your Own Device (BYOD) pode causar às empresas do ponto de vista da Segurança da Informação?
9. Ao utilizar Inteligência Artificial para mapear e combater ameaças, qual(is) cuidado(s) deve(m) ser tomado(s)?
10. Defina, com suas próprias palavras, o que é Malha de Cibersegurança?
11. Por que Segurança da Informação para Internet das Coisas tem se tornado uma preocupação das organizações?
12. Como uma empresa poderia garantir a conformidade com aspectos de Segurança da Informação de seus parceiros de negócios?
13. O que é múltiplo fator de autenticação ou autenticação de dois fatores? O que visa garantir?

Módulo 3 – Conceitos de vulnerabilidades e ameaças

1. O que é uma vulnerabilidade?
2. O que são ameaças? De quais tipos elas podem ser? Dê um exemplo de cada tipo de ameaça.
3. Qual é a diferença entre um ataque passivo e um ativo?
4. Por que ataques passivos são mais difíceis de serem detectados?
5. O que é risco?
6. O que é um incidente de segurança da informação?
7. Quais medidas devem ser adotadas para se proteger um ativo?
8. Quais são as respostas aos riscos?
9. O pilar de implementação de um Sistema de Gestão de Segurança da Informação é formado por pessoas, processos e tecnologia. Na sua opinião, qual componente deste pilar é o mais importante e porquê?

Módulo 4 – Tipos de malware e principais ataques

1. Explique, com suas próprias palavras, o que é um ransomware.
2. Explique, com suas próprias palavras, o que é um botnet.
3. Qual a diferença entre vírus, worms e trojans (cavalo de tróia)?
4. Qual a diferença entre os ataques phishing e spear phishing?
5. Por que é necessário utilizar senhas fortes e complexas?
6. Qual a diferença entre um ataque de adivinhação por força bruta e um ataque de dicionário?
7. Num ataque de injeção SQL, o malfeitor procurar ter acesso a qual tipo de sistema?

Módulo 5 – Norma ISO/IEC série 27000

1. Do que se trata a série de normas ISO/IEC 27000?
2. Do que se tratam as normas ISO/IEC 27001, 27002 e 27005?
3. O que é um processo?
4. De acordo com a norma ISO/IEC 27002, o estabelecimento e a implementação do Sistema de Gestão de Segurança da Informação são influenciados pelo quê?
5. Quais são as etapas do modelo PDCA para a implementação do SGSI?
6. Por que o envolvimento da alta direção da organização é importante para o sucesso do estabelecimento e a implementação do SGSI?

7. O que são partes interessadas?
8. Quais são os tipos de recursos necessários para estabelecer e implementar o SGSI?
9. Por que é necessário monitorar e avaliar o SGSI a intervalos periódicos?
10. O que significa melhoria contínua?
11. Qual a diferença entre avaliação e análise de riscos?
12. O que são controles?
13. Quais são os critérios para aceitação de riscos?
14. Onde podem ser identificadas as vulnerabilidades?
15. Como podemos avaliar a probabilidade da incidência de incidentes?

Módulo 6 – Políticas e procedimentos de Segurança da Informação

1. O que é uma política de segurança?
2. Quais são as premissas para se estabelecer uma política de segurança?
3. Explique, com suas próprias palavras, as fases do ciclo de vida de um incidente de segurança.

Módulo 7 – Plano de continuidade do negócio

1. O que é um plano de continuidade do negócio?
2. Quais são as possíveis causa da indisponibilidade?
3. Quais são os impactos da indisponibilidade das informações?
4. Qual a diferença entre confiabilidade e disponibilidade?
5. Quais são as unidades de medidas utilizadas para mensurar a disponibilidade?
6. Qual a vantagem de se associar elementos em paralelo em relação à associação de elementos em série?
7. Qual a definição de ponto único de falha?
8. Quais tecnologias ou arranjos podem ser adotadas para se implementar a redundância no nível de rede, armazenamento, processamento e fornecimento de energia?

Módulo 8 – Plano de recuperação de desastres

1. O que é um plano de recuperação de desastres?
2. Explique, com suas próprias palavras, o que é RPO (Recovery Point Objective)?
3. Explique, com suas próprias palavras, o que é RTO (Recovery Time Objetive)?
4. Qual a diferença entre recuperação de desastres e restauração operacional?

5. Quais são os componentes de uma arquitetura de backup? Explique cada um deles.
6. O que é um catálogo de backup?
7. Qual a diferença entre um backup incremental e um acumulativo (ou diferencial)?

Módulo 9 – Criptografia e certificados digitais

1. Qual a diferença entre esteganografia e criptografia?
2. O que é possível proteger por meio da criptografia?
3. O que é um método criptográfico?
4. O que garante a segurança de um método criptográfico é o seu algoritmo de criptografia ou o espaço de chaves? Justifique.
5. Qual a diferenças entre os métodos criptográficos baseados em chaves simétricas e assimétricas?
6. Cite exemplos de algoritmos criptográficos que utilizam chave simétrica.
7. Cite exemplos de algoritmos criptográficos que utilizam chave assimétrica.
8. Qual(is) a(s) vantagem(ns) e desvantagem(ns) do uso de chave assimétrica em relação à chave simétrica?
9. Explique como a navegação segura em sites de Internet pode tirar proveito da combinação de chaves simétricas e assimétricas.
10. O que é Secure Sockets Layer?
11. O que é Transport Layer Security?
12. O que é função hash e para que serve? Cite exemplos.
13. O que é assinatura digital?
14. O que é certificado digital?
15. Qual(is) a(s) diferença(s) entre assinatura digital e certificado digital?

Módulo 10 – Infraestrutura de chaves públicas

1. Defina, com suas próprias palavras, o que é uma infraestrutura de chaves públicas?
2. O que é uma autoridade certificadora?
3. Por que uma autoridade certificadora raiz tem um certificado auto assinado?
4. Qual a relação entre uma autoridade certificadora raiz, intermediária e emissora?
5. Ao acessar um site, no navegador aparece uma mensagem de que o certificado do site não é confiável. Por que essa mensagem aparece?
6. O que é uma lista de certificados revogados?

Módulo 11 – Privacidade de dados

1. O que é privacidade?
2. Qual lei brasileira tem por objetivo proteger a privacidade das pessoas?
3. Qual a relação da lei brasileira de privacidade de dados com a correspondente lei europeia?
4. Quais os motivos que nortearam a articulação do Congresso Nacional para criação de uma lei nacional de proteção à privacidade?
5. O que é a Autoridade Nacional de Proteção de Dados (ANPD)?
6. O que é um dado pessoal? Dê exemplos.
7. O que é um dado pessoal sensível? Dê exemplos.
8. O que é tratamento de dados? Dê exemplos.
9. Quais são os princípios de tratamento?
10. Quais são os requisitos (bases legais) para o tratamento de dados?
11. Quais são os agentes de tratamento? Qual a relação entre eles?
12. Qual(is) a(s) diferença(s) entre privacidade de dados e segurança de dados?