?

Questionário de Revisão

1. **Faça uma breve explanação sobre a Segurança da Informação, suas principais características, importância e implicações na área das TICs.**

   Segurança da Informação é proteger um conjunto de dados e seus valores. A SI é composta por 3 pilares:

   - Condifencialidade → proteção dos dados não autorizados (controle de acesso aos dados).
   - Integridade → manter dados completos e confiáveis (inalterados durante transmissão, armazenamento ou processamento).
   - Disponibilidade → manter dados disponíveis quando necessário. Sistemas funcionando mesmo após situações inesperadas. (redundância, backup e recuperação)

   Os principais objetivos são: cuidar de riscos associados à falta de segurança e limitar/regular acesso (lógico ou físico) à informação ou ambiente que a sustenta, através de diferentes estratégias e métodos.

2. **A Segurança da Informação prima pela manutenção das características definidas pelo acrônimo CID – Confidencialidade, Integridade e Disponibilidade (em inglês CIA – Confidentiality, Integrity and Availability). Explique o aparente antagonismo entre Confidencialidade e Disponibilidade.**

   O antagonismo pode ocorrer ao ler as palavras, que diante de um significado sem contexto, se contrariam.

   Porém as duas palavras são 2 de 3 pilares existentes que constituem a Segurança da Informação, o primeiro garantindo um controle de acesso aos dados somente para entidades autorizadas para realizar aquela atividade, já o segundo se refere à disponibilidade do sistema que deve ser mantida mesmo após uma falha no hardware ou um ataque cibernético, por exemplo.

3. **Explique a Política de Segurança da Informação sob a perspectiva da ISO 27.002.**

   “Prover orientação da Direção e apoio para a Segurança da Informação de acordo com os requisitos do negócio e com as leis de regulamentação.” (ISO 27.002-5, 2013)

   Sugere que a empresa, funcionário e diretoria desempenham um papel fundamental para a Segurança da Informapção, uma vez que estão ligados diretamente ao fluxo de dados e informação dentro do sistema. Assim, para um bom desenvolvimento e prática da SI, é necessário que a Direção de uma empresa esteja de acordo e promova iniciativas de segurança.

   Exemplos → estabelecer estratégias incluindo técnicas de segurança, alocar recursos adequados necessários para estabelecer a SI, cumprir com leis e regulamentos, monitorar e revisar o desempenho na parte de Segurança da Informação.

4. **Considerando o que foi estudado a respeito da Esteganografia, é possível detectar a presença de uma mensagem oculta em um arquivo? Como?**

   Sim, é possível detectar uma mensagem oculta em um arquivo através de técnicas de Esteganálise: destruindo tudo, adicionando mais informação (sobrescervendo a mensagem), alterando o formato do arquivo ou comprimindo o arquivo (baseado no fato de algoritmos de compressão desejam remover informação extra do arquivo).

   Podemos classificá-las em 3 tipos de ataque: **visual** (inspecionar arquivo visualmente e procurar falhas), **estruturais** (identificar mudança na estrutura de um arquivo, sugerindo mudanças) ou **estatísticos** (aplicar testes para verificar informações escondidas.)

5. **Considerando o que foi apresentado a respeito de esteganografia, qual a quantidade de informação conseguimos ocultar em uma imagem FULL HD (1920 × 1080 pixels)? E em um filme HD de 30 minutos?**

   Imagem:

   - Resolução: 1920×1080 px
   - Bits: 1920 × 1080 × 3 (RGB) x 8 (bits) = 49.766.400

- Ocultar: 5.971.968 bits (746,5KB) (12%)

Filme HD:

- Resolução: 1280×720 px
- Bits por frame: 1280 × 720 × 3 (RGB) x 8 (bits) = 22.118.400
- Ocultar: 2.654.208 bits (331KB) por frame (12%)
- 30 fps = Ocultar 595,8MB por minuto
- Filme de 30 min = 17,9GB de informação

6. **Como foi tratado no conteúdo sobre Autenticação, o Firebase é uma plataforma de serviços que, entre outros, oferece um mecanismo de autenticação público e gratuito. Qual é o tipo desse mecanismo, e quais fatores de autenticação são usados por esse mecanismo?**

   A plataforma Firebase oferece desde autenticação realizadas por senhas (Tradicional) ou números de telefone (Centralizado) até um modelo Federeado , com identidades como Google e Twitter.

7. **A norma ISO 27.002 estabelece que "Convém documentar qualquer tipo de circunstância excepcional que exija a utilização de identificador de usuário compartilhado por um grupo de pessoas", e que, nesses casos, "controles adicionais podem ser necessários para manter as responsabilidades dos indivíduos que vão utilizar este identificador". Explique o que você entende sobre este requisito de segurança, e dê um exemplo em que isso seja necessário e como pode ser aplicado, nesse caso.**

   Esse requisito se refere ao compartilhamento de usuários genéricos dentro de uma empresa, e garante que deve ser documentado cada ação realizada por cada indivíduo para um melhor controle dos acessos e quem os realizou. Assim, pode-se gerar um histórico para a conta compartilhada e registrar horários e ações de cada funcionário. Além desse requisito, podemos adotar mecanismos de segurança adicionais para uma mitigação de ataques internos e externos ou perda de dados importantes.

Exemplo: uma pequena empresa compartilha uma conta “Admin” de usuário Windows no escritório, e é utilizado o controle de horário e ações para um histórico geral de cada funcionário. Também são utilizados controles adicionais como rastramento de solicitações de acesso à essa conta e revisões periódicas de quem a acessou para garantique somente pessoas autorizadas consegam tal feito.

8. **No que se refere à controle de acesso, o que diferencia o DAC do MAC? Qual deles é implementado por meio de uma Matriz de Acesso? Dê um exemplo dessa implementação.**

DAC → Discretionary Access Control	MAC → Mandatory Access Control
Controle de acesso baseado na identidade do solicitante	Controle de acesso baseado na comparação de Rótulos e Autorização de Segurança
Define o que o indivíduo está autorizado a fazer	OBRIGATÓRIA
Entidade pode conceder acesso a outras entidades sobre seus recursos	Entidade não pode conceder acesso a outras

- **Rótulo** → determina a criticidade dos recursos
- **Autorização** → determina quais entidades tem acesso a quais recursos

9. **Como mostrado na aula sobre Criptografia, a Cifra de César é um modelo criptográfico muito simples que usa o deslocamento (ou rotação) de caracteres para embaralhar a mensagem. Foi usado este método para produzir a seguinte mensagem cifrada: “N NINYVNPNB QR FRTHENAPN QN VASBEZNPNB RFGN ZHVGB SNPVY”. Sabendo-se que a mensagem foi escrita em português, sem o uso de acentos ou caracteres especiais e específicos dessa língua, use a técnica de força bruta e decifre a mensagem. #dica: Tente usar as suas habilidades desenvolvidas durante anos jogando o “Jogo da Forca”...**

   N NINYVNPNB QR FRTHENAPN QN VASBEZNPNB RFGN ZHVGB SNPVY

   o ojoz X → não é 1 letra depois do alfabeto

   A AVALIACAO DE SEGURANCA DA INFORMACAO ESTA MUITO FACIL → 13 letras depois no alfabeto!

Fui testando as vogais, comecei com O e depois fui pra A, já que a possibilidade era maior devido ao N isolado no começo. A partir dai, contei a diferenças de letras e fui substituindo.

10. **De acordo com o conteúdo apresentado, existem dois modelos de criptografia: Simétrica e Assimétrica. Qual desses modelos é o melhor? Justifique sua resposta.**

    O modelo mais utilizado hoje em dia, mesmo sendo o mais antigo, ainda é o de Criptografia Simétrica. Isso ocorre por que mesmo que exista um conhecimento público sobre o texto cifrado e o algoritmo de cifração, sem a chave é impraticável que exista uma decifração da informação. Então desde que a chave esteja segura pelo remetente e o destinatário, a informação estaá segura.

    A Criptografia Assimétrica, mesmo sendo mais moderna e corriguindo problemas da Cirptografia Simétrica, ainda é menos utilizada por ser mais difícil de distribuir as chaves.

    A segurança em si está relacionada com o tamanho da chave e no esforço necessário para conseguir decifrar uma mensagem, e não no tipo de criptografia utilizada.

11. **O que é o Triplo A? Qual a importância de cada componente do Triple A? Como eles interagem para garantir a segurança da informação?**

    Autenticação, Autorização, Accountability (Contabilidade).

    O primeiro verifica a identidade de um usuário/dispositivo que está tentando acessar, através de senhas e tokens. Garante o acesso somente por usuários permitidos

    O segundo, por sua vez, detemina permissões que um usuário autenticado possui para acessar recursos específicos. Limita o acesso apenas ao necessário para o usuário.

    O terceiro registra e audita atividades dos usuários após o aceso aos recursos da rede, sejam elas tentativas bem sucedidas ou falhas. Registra histórico de acontecimentos, útil para investigar e monitorar.

12. **A autenticação é a primeira linha de defesa em muitos sistemas de segurança. Quais são os mecanismos de autenticação e quais as suas aplicações em cenários segurança?**

    Existem três modelos que relacionam SP e IdP

    Tradicional → Contato direto entre o SP e IdP, onde o Usuário emite a requisição da autenticação e resposta diretamente volta diretamente. (**SP**: próprio site | **IdP**: sistema gerenciamento de contas do site)

    Centralizado → O Usuário emite a requisição da autenticação, que passa primeiramente pelo SP para depois encaminhar a autenticação do Usuário para o IdP. A resposta volta para o SP e depois chega no Usuário. (**SP**: próprio site | **IdP**: sistema gerenciamento identidade corporativa)

    Federado → O Usuário emite a requisição da autenticação, que é terceirizada para o SP de algum outro domínio. Esse por sua vez envia a autenticação do Usuário para o IdP do domínio original, que devolve a resposta ao SP terceirizado para depois chegar no usuário. (Ex: Login utilizando o Google)

13. **As consequências de falhas de segurança podem ser devastadoras. Analise os potenciais impactos de uma falha de segurança em sistemas de informação para uma organização.**

    Algumas consequências que podem ser citadas são: perda/roubo/comprometimento de dados sensíveis e confidenciais, os que trará um alto custo para investigação, recuperação de dados, etc. Além disso, as falhas de segurança trazem uma desconfiança para os clientes da empresa e pode resultar em impactos em futuras operações.

14. **O campo da segurança da informação, assim como toda a TIC, está sempre evoluindo. Quais as tendências em segurança da informação e como elas podem impactar as práticas atuais?**

    Acredito que a Segurança da Informação está utilizando cada vez mais de tecnologias como Inteligência Artificial e Machine Learning para proteção de dados e dispositivos. Além disso, o foco em proteção de Nuvem, devido ao aumento de adoção desse tipo de armazernamento, e o surgimento de novos conceitos como “Zero Trust Security” estão se tornando mais importantes também.

15. **Quais são as implicações éticas e legais do uso da esteganografia?**

    O uso da esteganografia deve cumprir com privacidade e segurança de dados e um cuidado maior com falhas em detecção de sistemas de segurança (firewall). A esteganografia pode estar sujeita a regulações específicas para cada país, que resultam em uma responsablidade legal individual de cada praticante.

16. **Quais são os diferentes tipos de mecanismos de autenticação comumente utilizados?**

    Existem três modelos que relacionam SP e IdP: Tradicional, Centralizado, Federado

17. **Em um mundo onde as transações online e o acesso remoto a sistemas são comuns, a autenticação robusta é essencial. Explique por que a autenticação é uma componente crítica para a segurança em ambientes de TICs, assim como os desafios associados ao desenvolvimento de métodos de autenticação eficazes nos mais diversos ambientes tecnológicos.**

    Por que a autenticação garante que o usuário realmente é quem ele diz ser, e em ambientes TICs isso é mais importante quando pensamos em um computador que pode ser utilizadop por qualquer um, mas o acesso só é permitido para os usuários legitmos.

18. **A autenticação multifator (MFA) combina dois ou mais métodos independentes de autenticação, aumentando a segurança. Como a autenticação multifator funciona e por que ela é considerada mais segura do que a autenticação de fator único? Quais exemplos de fatores típicos são usados em MFA, e quais são as suas vantagens e possíveis limitações?**

    A autenticação multifator funciona com duas camadas de autenticação, a primeira sendo normalmente algo que ele sabe, como sua senha ou PIN, e a segunda é normalmente algo que ele possui, como token de acesso, código único enviado por email ou sms, ou algo que ele é, como biometria

ou reconhecimento facial. Assim dificulta ainda mais a falsificação de identidade.

Outro exemplo seria o Microsoft Authenticator, aplicativo de autenticação da Microsoft único por celular. Muito bom e prático, porém se acontece algo com seu celular atual, como roubo ou perda, é bem trabalhoso para trocar o celular padrão da sua conta para outro dispositivo

19. **A biometria é cada vez mais adotada para autenticação em dispositivos móveis e sistemas de segurança. Analise o uso da biometria como método de autenticação, destacando seus principais tipos e como eles são implementados. Quais são as preocupações éticas e de privacidade associadas ao uso da biometria?**

    Algumas preocupações do uso da biometria são: privcidade e segurança dos dados, rastreamento e vigilância em massa, uso indevido e acesso não autorizado através da falsificação de identidade (cópia da digital).

20. **Apresente os principais desafios relacionados à implementação de métodos de autenticação eficazes nas TICs. Discuta como as empresas e organizações podem superar esses desafios e garantir a segurança de seus sistemas e dados, considerando a proliferação de credenciais, a dificuldade em gerenciar diversas senhas e outras credenciais de acesso, as ameaças cibernéticas em constante evolução, a necessidade de se manter atualizado com as novas técnicas e ferramentas utilizadas por criminosos e a experiência do usuário.**

    Levando os tópicos em consideração, podemos analisar que as soluções disponíveis são: utilização de autenticação multifatorial (MFA) e de gerenciamento de identidade de acesso (IAM), políticas de senhas robustas para o uso de senhas mais seguras, inclusão de soluções de segurança em camadas (firewall, detecção de intrusão, monitoramento em tempo real de ameaças, etc.), investimento em um bom sistema de segurança e instruções claras e objetivas para o cuidado por parte dos funcionários. Tudo isso sem deixar de lado a boa experiência para o usuário, com interfaces seguras e ao mesmo tempo intuitivas e viáveis, validada através de feedbacks constantes.