**Framework Front-End com consumo de API – SA2**

**Quiz 1 - Segurança da informação**

Segurança da informação.

1 – Confira as afirmações.

1. Dados são recursos isolados que não têm valor relevante para uma tomada de decisão ou embasamento de conclusões.
2. Informação é a organização dos dados para a compreensão de determinado contexto.

Assinale a alternativa que representa um exemplo de informação.

1. Cem pessoas visitaram um site.
2. Uma lista com dez nomes.
3. **Em um determinado mês, cem pessoas visitaram um site e, no mês seguinte, 160 pessoas. Houve um aumento de 60% no número de acessos.**
4. Cinquenta cursos cadastrados.
5. Todas as anteriores.

**Dica**

A informação tem utilidade dentro de um contexto para tomada de decisões.

**Resposta e feedback**

A informação é composta de dados organizados dentro de um contexto. Dados avulsos, sem contexto, como o número de acessos em um site ou uma lista de nomes, não compõem sozinhos uma informação. Já a análise do número de acessos em dois meses seguidos (cem visitantes em um mês e 160 no mês seguinte), mostra um aumento de 60%, informação que pode ser útil em tomadas de decisão para o setor de vendas, divulgação ou redes sociais.

Segurança da informação.

2 – A Segurança da Informação tem três pilares: disponibilidade, confidencialidade e integridade. O que seria disponibilidade?

1. É quando os dados devem ser disponibilizados somente para pessoas autorizadas, e não podem ser divulgados a pessoas externas e que não devam ter acesso.
2. **É quando as informações ou dados são disponibilizados sem falhas, quando solicitados, e para usuários autorizados.**
3. É quando não tem modificação ou exclusão dos dados, durante ou após o envio da informação.
4. É quando as informações são disponíveis para todos os usuários dentro da empresa.
5. É quando divulgamos dados confidenciais para qualquer usuário.

**Dica**

Um mecanismo para garantir a disponibilidade é o uso de *backups* periódicos, a fim de manter os dados sempre disponíveis caso ocorra algum problema.

**Resposta e feedback**

A disponibilidade diz respeito ao acesso sem falhas aos dados. Por exemplo, um determinado sistema precisa concluir e fechar a folha de pagamento do mês. Se o sistema não está disponível, seria um problema de disponibilidade de dados.

Segurança da informação.

3 – A segurança da informação tem três pilares: disponibilidade, confidencialidade e integridade. O que seria confidencialidade?

1. **É quando os dados devem ser disponibilizados somente para pessoas autorizadas e não podem ser divulgados a pessoas externas e que não devam ter acesso.**
2. É quando as informações ou dados são disponibilizados sem falhas.
3. É quando não tem modificação ou exclusão dos dados, durante ou após o envio da informação.
4. É quando as informações são disponibilizadas para todos os usuários dentro de uma empresa.
5. É quando divulgamos dados confidenciais para qualquer usuário.

**Dica**

Um dos mecanismos para garantir a confidencialidade é o uso de criptografia, aplicada na autenticação de usuários.

**Resposta e feedback**

O pilar da confidencialidade determina que somente usuários autorizados devem ter acesso a determinadas informações.

Segurança da informação.

4 - A segurança da informação tem três pilares: disponibilidade, confidencialidade e integridade. O que seria integridade?

1. É quando os dados devem ser disponibilizados somente para pessoas autorizadas e não podem ser divulgados a pessoas externas e que não devam ter acesso.
2. É quando as informações ou dados são disponibilizados sem falhas, quando solicitados e para usuários autorizados.
3. **É quando não tem modificação ou exclusão dos dados, durante ou após o envio da informação.**
4. É quando as informações são disponibilizadas para todos os usuários dentro de uma empresa.
5. É quando divulgamos dados confidenciais para qualquer usuário.

**Dica**

A integridade é um pilar que tem como responsabilidade a garantia de que não houve modificações nos dados.

**Resposta e feedback**

A integridade determina que os dados devem ser enviados, armazenados e acessados com seu conteúdo íntegro, ou seja, devemos garantir que os dados não sejam modificados ou excluídos.

Práticas de segurança.

5 – Os dados das empresas são considerados ativos importantes e imensuráveis. A Política de Segurança da Informação (PSI) determina regras e diretrizes para o acesso a dados e informações. Assinale a alternativa que contém um exemplo do tipo de política de segurança que pode ser praticado por uma empresa?

1. Enviar e-mail em nome de outro emissor.
2. Compartilhar informações com empresas parceiras.
3. Não utilizar e-mails.
4. Não ter contato com ninguém durante o expediente de trabalho.
5. **Não compartilhar senhas.**

**Dica**

Logins e senhas são de uso individual e intransferíveis.

**Resposta e feedback**

Além de não compartilhar senhas, não devemos enviar e-mails em nome de outro emissor e nem compartilhar informações internas com empresas parceiras, dentre outras ações para cumprir a política de segurança das empresas.

Controle de acesso.

6 – Assinale a alternativa que representa um exemplo de controle de acesso físico?

1. Utilizar login e senha para acessar o e-mail.
2. Fazer *backup* periódico.
3. Aplicar criptografia nos arquivos.
4. **Entrar na empresa somente com utilização de um crachá.**
5. Acessar um servidor de banco de dados da empresa.

**Dica**

O controle de acesso físico visa não permitir a presença de pessoas não autorizadas no ambiente que está sendo controlado.

**Resposta e feedback**

Controle de acesso físico está relacionado à limitação de acesso a pessoas em espaços dentro de uma organização, como exigir um crachá para acessar fisicamente certos ambientes.

Auditorias.

7 – O que seria uma auditoria?

1. É uma forma de criptografia de arquivos.
2. **É uma avaliação para analisar e identificar pontos em que pode haver violação de segurança, de acordo com alguns critérios estabelecidos.**
3. É um tipo de controle de acesso físico em uma organização.
4. É uma política de segurança adotada, para evitar compartilhamento de senhas.
5. É um usuário responsável por proteger todos os dados de uma organização.

**Dica**

A auditoria é uma forma de descobrir se a política de segurança está sendo cumprida e se há falhas a serem corrigidas.

**Resposta e feedback**

A auditoria é uma avaliação para analisar e identificar pontos em que pode haver violação de segurança, de acordo com um conjunto de critérios estabelecidos. Exemplo: as senhas podem ser descobertas facilmente?

Práticas de segurança.

8 – Do grego *kriptos* (oculto) e *grafo* (escrita), a criptografia codifica uma informação deixando-a ilegível ou dificultando a leitura por pessoas não autorizadas. Uma chave criptográfica é aquela que codifica um texto que só o emissor e o receptor podem decifrar. Qual dessas alternativas não utilizam criptografia?

1. Sites que aparecem na URL ([www.senai.com.br](http://www.senai.com.br)) o protocolo de rede HTTPs.
2. **Contratos de funcionários salvos sem senha.**
3. Assinaturas digitais.
4. Blockchain em transações de criptomoedas.
5. Virtual Private Network (VPN)

**Dica**

A criptografia está presente em grande parte das transações digitais.

**Resposta e feedback**

Sem medidas de política de segurança, como a criptografia, é comum que arquivos importantes, como contratos de funcionários, sejam armazenados

sem proteção, deixando-os vulneráveis.

Práticas de segurança.

9 – As funções de hash (funções de dispersão, em português) têm como principal objetivo gerar uma numeração única chamada hash para o dado enviado por meio da técnica de hashing. Neste contexto, qual a alternativa correta?

1. **Qualquer modificação dos dados submetidos a uma função de hash modificará a hash gerada.**
2. Um dado submetido a hash poderá ser bidirecional.
3. Qualquer modificação dos dados submetidos a uma função de hash irá retornar a mesma hash gerada.
4. Um dado submetido ao algoritmo de criptografia não poderá ser descriptografado.
5. Um dado submetido a hash poderá ser descriptografado.

**Dica**

Os dados submetidos ao hash geram chaves ou numerações únicos.

**Resposta e feedback**

A função hash aplica o cálculo de hashing para um dado, fazendo com que o resultado desse cálculo se torne único para o dado enviado. Nas linguagens de programação, os hash gerados são diferentes e dependem dos parâmetros que são enviados para os algoritmos que fazem o hashing. Nesse contexto, o programador front-end pode controlar os parâmetros de hash, mas não conhece qual numeração será gerada para um dado específico.

Backup.

10 – Se o servidor de arquivos, que armazena todos os contratos de todos os funcionários, perde todos os dados, o que deve ser feito?

1. Comprar outro servidor e fingir que nada aconteceu.
2. **Conseguir verificar se existe uma cópia de segurança dos arquivos e que possa ser utilizada em outro equipamento.**
3. Esquecer os arquivos perdidos e proteger os outros equipamentos que sobraram.
4. Aplicar medidas novas de políticas de segurança, em que somente pessoas autorizadas podem ter acesso ao servidor.
5. Adotar políticas de criptografia nos arquivos, pois assim eles ficam protegidos de qualquer desastre.

**Dica**

A prevenção minimiza perdas, ou seja, a aplicação de backups.

**Resposta e feedback**

Como acidentes acontecem, devemos estar preparados para qualquer tipo de situação. Se um equipamento para de funcionar ou, sem querer, apagamos um arquivo, é uma prática essencial ter uma cópia desses arquivos, principalmente em um local diferente, como outra máquina ou servidores em nuvem (cloud) para se ter acesso aos dados sem nenhum tipo de preocupação.