**Codificação Back-End – SA3**

**Quiz 1 - Segurança da Informação**

Segurança da informação

# 1 – Dadas as afirmativas:

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

Assinale a alternativa que representa um exemplo de informação.

1. 100 pessoas visitaram um site.
2. Uma lista com 10 nomes.
3. **Em um determinado mês, 100 pessoas visitaram um site, no mês seguinte, 160 pessoas. Houve um aumento de 60% no número de acessos.**
4. 50 cursos cadastrados.
5. Todas as anteriores.

**Dica**

A informação possui 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 (100 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. Ação em que os dados devem ser disponibilizados somente para pessoas autorizadas e não podem ser divulgados a pessoas externas, que não devam ter acesso.
2. **Ação em que as informações ou dados são disponibilizados sem falhas, quando solicitados e para usuários autorizados.**
3. Ação em que não tem modificação ou exclusão dos dados, durante ou após o envio da informação.
4. Ação em que as informações são disponíveis para todos os usuários dentro de uma empresa.
5. É quando divulgamos dado confidencial para qualquer usuário.

**Dica**

Um mecanismo para garantir a disponibilidade é o uso de backups periódicos.

**Resposta e feedback**

A disponibilidade diz respeito ao acesso sem falhas a dados. Por exemplo, um determinado sistema precisa concluir e fechar a folha de pagamento do mês, se o sistema não estiver disponível, será 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. **Ação em que os dados são disponibilizados somente para pessoas autorizadas e não podem ser divulgados a pessoas externas, que não devam ter acesso.**
2. Ação em que as informações ou dados são disponibilizados sem falhas.
3. Ação em que não tem modificação ou exclusão dos dados, durante ou após o envio da informação.
4. Ação em que as informações são disponíveis para todos os usuários dentro de uma empresa.
5. Ação em que divulgamos dados confidenciais ara qualquer usuário.

**Dica**

Um dos mecanismos para garantir a confidencialidade é o uso de logins.

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

**Dica**

Um dos mecanismos para garantir a integridade é o uso de assinaturas digitais.

**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.

# Qual dos exemplos a seguir é um 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**

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

Práticas de Segurança

# 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 crachá para acessar fisicamente certos ambientes.

Auditorias

# 7 – O que seria uma auditoria?

1. É uma forma de criptografar arquivos.
2. **É um exame cuidadoso 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 a uma organização.
4. É uma política de segurança adotada para evitar compartilhamento de senhas.
5. É uma equipe 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 um exame criterioso para analisar e identificar pontos em que pode haver violação de segurança, de acordo com um conjunto de critérios estabelecidos. Por exemplo: as senhas podem ser descobertas facilmente?

Criptografia

# 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 dos objetos indicados não utiliza criptografia?

1. Sites que aparecem na URL (ex.: www.senai.com.br).
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, tornando-os vulneráveis.

# 9 – Qual é o nome da tecnologia utilizada para se obter tráfego na internet de forma criptografada, com acesso a uma rede privada e de forma segura?

1. **VPN**
2. Firewall
3. Intranet
4. Backup
5. Criptologia

**Dica**

O nome da tecnologia é Rede Privada Virtual, mais conhecida pelas iniciais de seu nome em inglês.

**Resposta e feedback**

A VPN (Virtual Private Network) criptografa o tráfego de internet e disfarça uma identidade online. Com ela, podemos ter acesso seguro a um servidor remoto, criar conexões entre computadores remotos e apresentar a conexão como se fosse uma rede privada local.

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

1. Deve-se comprar outro servidor e fingir que nada aconteceu.
2. **Deve-se verificar se existe uma cópia de segurança dos arquivos, a qual possa ser utilizada em outro equipamento.**
3. Deve-se esquecer os arquivos perdidos e proteger os outros equipamentos que sobraram.
4. Deve-se aplicar novas medidas de política de segurança, em que somente pessoas autorizadas podem ter acesso ao servidor.
5. Deve-se adotar políticas de criptografia nos arquivos, pois eles ficarão protegidos de qualquer dano.

**Dica**

A prevenção minimiza perdas.

**Resposta e feedback**

Para prevenir eventualidades, devemos estar preparados. Caso um equipamento sofra danos ou ocorra exclusão acidental de um arquivo, é uma prática essencial ter uma cópia ou um backup, principalmente em um local diferente, como outra máquina ou servidores em nuvem.