Banco de Dados

Quiz 02 – Segurança e Auditoria

# 01) A segurança da informação está diretamente relacionada com a proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. Assim, indique suas principais funções a seguir.

1. Proteção somente dos componentes físicos de um sistema computadorizado.
2. Proteção da informação e dos sistemas de informação contra acesso não autorizado, garantindo, assim, a confidencialidade, a integridade e a disponibilidade.
3. Garantia de que as pessoas que tenham acesso ao sistema corporativo sejam penalizadas em caso de descumprimento de regras de segurança.
4. Garantia de atualização constante de softwares de segurança da informação.
5. Todas as anteriores.

**Dica**

Note que o próprio enunciado menciona que a segurança da informação está relacionada à “proteção de conjunto de informações”.

**Feedback**

Os principais objetivos da segurança da informação são: proteção da informação e dos sistemas de informação contra acesso não autorizado, garantindo, assim, a confidencialidade, a integridade e a disponibilidade. A proteção dos componentes físicos, a punição pelo descumprimento de regras e a atualização de softwares não fazem parte da segurança da informação.

# 02) Indique se a afirmativa é verdadeira ou falsa.

# O objetivo da segurança da informação é prevenir ameaças, mesmo que isso aumente os riscos, não garantindo, dessa forma, o sigilo das informações, a confidencialidade dos dados e a saúde/continuidade da instituição.

Verdadeira Falsa

**Dica**

Lembre-se de que prevenção de ameaças e riscos são diretamente proporcionais.

**Feedback**

A afirmativa é falsa, pois o objetivo da segurança da informação é reduzir os riscos e prevenir ameaças, garantindo o sigilo das informações e assegurando a confidencialidade dos dados e a saúde/continuidade da instituição.

# 03) Levando em consideração que dado é um recurso que compõe uma informação, podemos entender que segurança da informação também se aplica a dados. Assim, indique a diferença entre dado e informação.

1. Dados são recursos isolados que não possuem valor relevante, e informação é uma organização de dados dentro de um determinado contexto.
2. Dados são simétricos e informação é assimétrica.
3. Dados são concretos e informação é abstrata.
4. Dados têm significado, informação não tem.
5. Dados são unidimensionais, informação é bidimensional.

**Dica**

Lembre-se de que dado é parte de uma informação.

**Feedback**

Dados são recursos isolados que não possuem valor relevante. Informação é uma organização de dados dentro de um determinado contexto. Dados isolados não possuem valor relevante para uma tomada decisão ou embasamento de conclusões. A organização ou processamento de dados permite ter compreensão sobre um determinado contexto, gerando, assim, informações que podem ajudar na tomada de decisões.

# 04) Segurança da informação está fundamentada em, pelo menos, três pilares. Indique quais são:

1. Investimento, crescimento e desenvolvimento.
2. Participação, educação e capacitação.
3. Cooperação, ação e disposição.
4. Disponibilidade, confidencialidade e integridade.
5. Cordialidade, temporalidade e capacidade.

**Dica**

Lembre-se de que a segurança da informação envolve acesso seguro a qualquer momento para pessoas previamente credenciadas.

**Feedback**

Segurança da informação está fundamentada em, pelo menos, três pilares: disponibilidade, confidencialidade e integridade. Isso significa que a informação deve ser íntegra e estar disponível para os acessos permitidos.

# 05) **(NÂO REVISAR E NÃO USAR POIS É CONTEÚDO DE MATERIAL COMPLEMENTAR)**

As normas ISO (International Organization for Standardization ou Organização Internacional para Padronização) são uma série de regras para a normatização de condutas e processos em organizações e entidades públicas, nos mais diferentes segmentos no mercado. Assim, indique a principal norma que uma organização deve utilizar como base para obter a certificação empresarial em gestão da segurança da informação que trata dos requisitos para implementar, manter e melhorar, continuamente, um sistema de gestão de segurança da informação e única norma internacional auditável.

1. ISO 27001
2. ISO 27002
3. ISO 27003
4. ISO 27004
5. ISO 27005

**Dica**

Normalmente as primeiras normas de uma família são as mais completas e importantes.

**Feedback**

A norma que trata especificamente dos requisitos para implementar, manter e melhorar, continuamente, um sistema de gestão de segurança da informação é a ISO 27001. É a principal norma que uma organização deve utilizar como base para obter a certificação empresarial em gestão da segurança da informação. Por isso, é conhecida como a única norma internacional auditável que define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI).

As demais normas apresentadas como alternativas, tratam de outros pontos específicos da segurança da informação:

ISO 27002: é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação.

É recomendável que a norma seja utilizada em conjunto com a ISO 27001, mas pode ser também consultada de forma independente com fins de adoção das boas práticas.

ISO 27003: A ISO 27003 contém um conjunto de diretrizes para a implementação do SGSI. Enquanto a 27001 disponibiliza apenas requisitos, aqui tem-se uma orientação detalhada.

ISO 27004: define métricas de medição para a gestão da segurança da informação. Pode ser uma importante aliada no momento de definir-se metas de níveis de serviço para a segurança da informação, ou mesmo executar o check e act do SGSI.

ISO 27005: cobre a Gestão de Riscos de segurança da informação. Grande parte do escopo da ISO 27005 pode ser interpretada como a sessão 4 da norma ISO 27001 detalhada na perspectiva dos riscos.

# 06) Em relação à segurança do banco de dados, existem técnicas que a garantem de forma básica. Indique aquela que define as ações de cada perfil de acesso.

1. Hierarquia
2. Níveis
3. Logs
4. Blocos
5. Negações

**Dica**

Lembre-se de que as técnicas não estão atreladas à estrutura e registro de ações.

**Feedback**

A técnica que define ações de cada perfil de acesso é chamada de nível. Os níveis de permissão definem as ações que cada perfil poderá ter ou poderá exercer em uma base de dados. A hierarquia está ligada à estrutura de perfis e os logs ao registro de ações. Blocos e negações não são técnicas de segurança da informação.

# 07) Para criar uma permissão ao banco de dados, usa-se as seguintes estruturas:

**CREATE LOGIN nome\_login WITH PASSWORD = 'xxxxxxxx'**

**CREATE USER nome\_usuario FOR LOGIN nome\_login**

**GRANT privilegio1, privilegio2 TO nome\_usuario**

Considerando-as, indique se a afirmativa é verdadeira ou falsa.

Para se ter acesso a um banco de dados, basta apenas executar o CREATE LOGIN.

Verdadeira Falsa

**Dica**

Lembre-se de que o login precisa estar atrelado a um usuário, ao qual será concedido privilégios.

**Feedback**

A afirmativa é falsa. O conjunto de estruturas tem que ser executado em sequência para acesso a um banco de dados, pois, sem um usuário, não será possível atribuir privilégios de acesso.

# 08) Para criar uma permissão ao banco de dados, pode-se usar as seguintes estruturas:

**CREATE LOGIN nome\_login WITH PASSWORD = 'xxxxxxxx'**

**CREATE USER nome\_usuario FOR LOGIN nome\_login**

**GRANT INSERT TO nome\_usuario**

Considerando as estruturas acima, indique se a afirmativa é verdadeira ou falsa.

Executada a sequência de estruturas de permissão, o usuário, uma vez logado, poderá executar a seleção de dados (SELECT).

Verdadeira Falsa

**Dica**

Observe o privilégio concedido na instrução GRANT.

**Feedback**

A afirmativa é falsa. A instrução **GRANT INSERT TO nome\_usuario** concede apenas o privilégio de inserção de dados e não para selecionar dados.

# 09) SQL Server Audit permite auditar um grupo de eventos ou eventos específicos. Esse recurso é muito utilizado para auditar ações como DDL e DML da base de dados e podem ser criados a nível de servidor ou de banco de dados. Indique a seguir como esse controle ocorre.

1. Por meio de alertas ou mensagens.
2. Por meio de documentos impressos automaticamente.
3. Gravado em uma tabela do banco de dados criada pelo SQL Server Audit.
4. A auditoria é baseada no registro e controle dos eventos ocorridos no banco de dados em um arquivo log.
5. Por meio do envio de arquivo de áudio para os especialistas.

**Dica**

Lembre-se de que, normalmente, a auditoria envolve registro de ações específicas em um tipo de arquivo específico.

**Feedback**

A auditoria por meio do SQL Server Audit é baseada no registro e controle dos eventos ocorridos no banco de dados em um arquivo log.

# 10) Após a criação e habilitação de uma auditoria pelo SQL Server Audit, você deve criar uma auditoria, com nível de banco de dados, para registrar as atividades no arquivo log. Assim, basta habilitá-la, que todas as ações do tipo DML (insert, update e delete) serão registradas no arquivo log. Com base na afirmativa do anterior, indique se ela é verdadeira ou falsa.

Verdadeira Falsa

**Dica**

Observe que no SQL Server Audit, na tela “Criar Especificação da Auditoria do Banco de Dados”, são solicitados alguns detalhes da auditoria, como o “Tipo de Ação de Auditoria”, o banco de dados e o usuário.

**Feedback**

A afirmativa é falsa. No SQL Server Audit, na tela “Criar Especificação da Auditoria do Banco de Dados”, é solicitado o “Tipo de Ação de Auditoria”, em que deverão ser informadas quais ações (insert, update, delete, select), em qual banco de dados e para qual usuário deverão ser registradas para o arquivo de log.