1)

Uma das principais normas de segurança da informação possibilita a certificação do Sistema de Gestão de Segurança da Informação (SGSI) da empresa. Os auditores líderes realizam a auditoria do SGSI, em um escopo bem definido da organização.

Qual alternativa a seguir é a norma que certifica o SGSI?

**Alternativas:**

* a)

ABNT NBR ISO/IEC 27000

* b)

ABNT NBR ISO/IEC 27001

Alternativa assinalada

* c)

ABNT NBR ISO/IEC 27002

* d)

ABNT NBR ISO/IEC 27005

* e)

ABNT NBR ISO/IEC 27007

2)

A segurança da informação possui um conjunto de funções, que são: identificação, proteção, detecção, resposta e recuperação. É preciso controles de segurança para cada uma das funções, como para fazer a proteção, como o firewall, ou para fazer a detecção, como o IDS.

Qual é a norma ou framework que define controles de segurança com base nessas cinco funções de segurança?

**Alternativas:**

* a)

CIS Controls

* b)

NIST Cybersecurity Framework

Alternativa assinalada

* c)

ABNT NBR ISO/IEC 27001

* d)

ABNT NBR ISO/IEC 27002

* e)

LGPD

3)

As políticas de segurança da informação constituem um dos principais controles de segurança da informação. Com a definição de elementos como regras, orientações, diretrizes, responsabilidades e sanções, as políticas de segurança da informação guiam as ações de todos da organização, incluindo os terceiros, prestadores de serviços, parceiros e fornecedores.

Considere as seguintes afirmações sobre as políticas de segurança:

 i. estar disponível como informação documentada

 ii. ser comunicada dentro da organização

 iii. estar disponível para as partes interessadas conforme apropriado

 iv. tratar de todos os aspectos cotidianos da organização, incluindo os relacionados às pessoas, aos processos e às tecnologias

Utilize (V) para verdadeiro e (F) para falso nas afirmações acima, e assinale a alternativa correta:

**Alternativas:**

* a)

F, F, F, F

* b)

V, V, V, V

Alternativa assinalada

* c)

V, V, V, F

* d)

V, F, V, V

* e)

F, V, F, F

4)

Dispositivos USB, como pendrives, são uma fonte de contaminação por malware. Em um ataque direcionado, por exemplo, pendrives podem ser espalhados em um estacionamento da empresa para que equipamentos internos sejam contaminados.

Considere os seguintes controles de segurança:

i. Bloqueio de porta USB;

ii. Treinamento para que funcionários não utilizem porta USB;

iii. Política de segurança proibindo o uso de porta USB;

iv. Simulação de ataque com verificação se algum funcionário usaria um pendrive espalhado intencionalmente no estacionamento.

Quais ações de segurança citadas devem fazer parte de um esforço para fortalecer a cultura de segurança da empresa?

**Alternativas:**

* a)

Apenas i

* b)

Apenas i e iii

* c)

Apenas ii e iii

* d)

Apenas iv

* e)

I, ii, iii e iv

Alternativa assinalada