Iniciado em	sábado, 19 Nov 2022, 22:52
Estado	Finalizada
Concluída em	sábado, 19 Nov 2022, 23:05
Tempo empregado	12 minutos 59 segundos
Notas	3,00/5,00
Avaliar	**0,30** de um máximo de 0,50(**60**%)

Questão **1**

Incorreto

Atingiu 0,00 de 1,00

As informações disponíveis, independente do nível ou do local de acesso, são chamadas de públicas. Quando acessíveis apenas de dentro das dependências da empresa, são classificadas como internas. As credenciadas podem ser visualizadas por um grupo durante tempo determinado, e as secretas apenas pela alta gestão e pelos responsáveis pela tecnologia da informação.

Público, interno, credenciados e externos são classificações para que grupo do documento de PSI?

Escolha uma opção:

- a. Padrões mínimos de qualidade.
- b. Tipos de informação.
- c. Níveis de acesso.

✖

RESPOSTA INCORRETA

É correto afirmar que são com base na classificação do tipo de informação que são definidos os níveis de acesso de cada colaborador, descrevendo regras para aplicativos, arquivos no servidor e acessos a diferentes redes; assim, acessos públicos, internos, credenciados e externos são classificações de tipo de informação. Já os níveis de acesso são representados pelos personagens de quem, como e quando acessam os dados da empresa. Os padrões mínimos de acesso dizem respeito a outro documento, ao SLA. O acesso pela sazonalidade e por tempo determinado é um credenciamento, e o monitoramento e a auditoria não são classificações do PSI.

- d. Monitoramento e auditoria.
- e. Acesso por sazonalidade e tempo determinado.

Sua resposta está incorreta.

A resposta correta é: Tipos de informação.

Questão **2**

Incorreto

Atingiu 0,00 de 1,00

A tradução de VPN é rede privada virtual. Por meio de tráfegos de dados com protocolos padrões, é possível garantir o acesso externo com segurança como se estivesse dentro da própria empresa.

Qual item do PSI essa definição atende?

Escolha uma opção:

- a. Monitoramento e auditoria.
- b. Níveis de acesso.
- c. Classificação do tipo de informação.
- d. Segurança física.
- e. Segurança lógica.

RESPOSTA INCORRETA

Seguranças física e lógica são importantes, mas não determinam acesso externo com regras internas da empresa. O monitoramento e a auditoria são realizações da TI e não do usuário final. A classificação por tipo de informação trata do mapeamento e da idealização dos diferentes personagens que fazem uso dos sistemas. É correto afirmar que para trafegar dados com protocolos padrões, garantindo acesso externo seguro, é necessário estabelecer claramente os níveis de acesso.

Sua resposta está incorreta.

A resposta correta é: Níveis de acesso.

Questão **3**

Correto

Atingiu 1,00 de 1,00

As empresas brasileiras devem prestar proteção aos dados pessoais que estão em sua posse, pois, muito mais que o zelo e o cuidado com sua base de conhecimento caso não observem essa deliberação, as empresas podem sofrer sanções como advertências, multas, bloqueios, etc.

Essa citação é aderente à qual das opções a seguir?

Escolha uma opção:

- a. Lei n.° 13.853/2019.

RESPOSTA CORRETA

É correto afirmar que o dever de prestar proteção aos dados pessoais é parte da Lei n.° 13.853/2019, pois ela descreve o zelo e o cuidado com a base de conhecimento. Já a Lei de Segurança de Dados não existe. *Phishing* e DDoS são técnicas de invasão e o ISO 27003:2015 trata da organização para implantação de sistemas de informações gerenciais.

- b. ISO 27003:2015.
- c. DDoS.
- d. *Phishing*.
- e. Lei de Segurança de Dados.

Sua resposta está correta.

A resposta correta é: Lei n.° 13.853/2019.

Questão **4**

Correto

Atingiu 1,00 de 1,00

Com reuniões periódicas, é possível observar o cumprimento das normativas, notificar por meio de relatório, e zelar pela proteção e pela distribuição das informações das políticas de segurança da informação - PSI.

Com base nessa afirmação, quem é o responsável máximo do PSI que sempre é requisitado em qualquer alteração do documento de política de segurança da informação?

Escolha uma opção:

- a. Comitê de segurança da informação. ✔

RESPOSTA CORRETA

A TI monitora e informa os resultados métricos do PSI. A chefia direta é responsável apenas por si (assim como o próprio colaborador) e pelo seu grupo. O RH informa ao setor de TI a respeito das contratações, das alterações (temporários ou permanentes) e dos desligamentos. O correto é afirmar que somente um comitê, composto por vários setores da empresa, é capaz de propor alterações no PSI. É essa pluralidade que torna capaz a visão sistêmica além da técnica na busca de soluções de proteção dos dados da instituição.

- b. Chefia direta.
- c. O próprio colaborador.
- d. Setor de tecnologia da informação - TI.
- e. Setor de recursos humanos - RH.

Sua resposta está correta.

A resposta correta é: Comitê de segurança da informação.

Questão **5**

Correto

Atingiu 1,00 de 1,00

Garantir total segurança no ambiente computacional é impossível. No entanto, existem diversas ferramentas que são importantes no monitoramento e na ação em casos de detecção de falhas ou de tentativas de invasão.

Dentro de um documento de PSI, ao falar sobre detecção, é correto afirmar que um grupo importante de segurança para esse item é/são:

Escolha uma opção:

- a. os relatórios de invasão enviados ao comitê.
- b. as ferramentas de *backup*.
- c. as ferramentas de alerta e de auditoria. ✔

RESPOSTA CORRETA

Ao falar em detecção, é correto afirmar que as ferramentas de alerta de auditoria são as responsáveis por identificar intrusos e modificações de qualquer natureza no sistema. Já o *backup* não é uma ferramenta de detecção e sim de recuperação. A base de dados em local seguro não representa nenhum tipo de detecção, assim como a lista dos equipamentos autorizados não detectam nenhum tipo de invasão e, por fim, os relatórios são apenas informativos, pois não agem no processo de detecção.

- d. a lista de equipamentos autorizados.
- e. o banco de dados em ambiente seguro.

Sua resposta está correta.

A resposta correta é: as ferramentas de alerta e de auditoria.