

Em relação à segurança da informação e aos controles de acesso físico e lógico, considere:

I. Se um usuário não mais faz parte da lista de um grupo de acesso aos recursos de processamento da informação, é certo que o grupo seja extinto com a criação de um novo, contendo os usuários remanescentes.

II. Direitos de acesso (físicos e lógicos) que não foram aprovados para um novo trabalho devem ser retirados ou adaptados, incluindo chaves e qualquer tipo de identificação que associe a pessoa ao novo projeto.

III. O acesso às áreas em que são processadas ou armazenadas informações sensíveis deve ser controlado e restrito às pessoas autorizadas, preferencialmente por controles de autenticação, por exemplo, cartão de controle de acesso mais PIN (personal identification number).

Está correto o que se afirma em

A I e II, apenas.

B I, II e III.

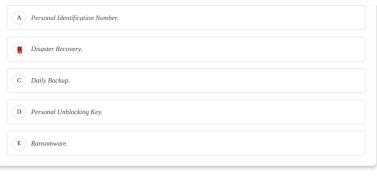
III e III.

III e IIII, apenas.

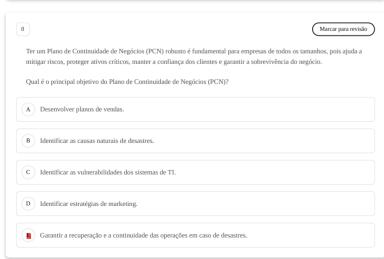


| C Spyware |
|--|
| D DDoS |
| Ransomware |
| |
| Marcar para revisão |
| (FCC/2010) Sobre segurança da informação, considere: I. Ameaça: algo que possa provocar danos à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de uma determinada vulnerabilidade. II. Vulnerabilidade: é medida pela probabilidade de uma ameaça acontecer e o dano potencial à empresa. III. Risco: ponto pelo qual alguém pode ser atacado, molestado ou ter suas informações corrompidas. Está correto o que consta APENAS em |
| (A) II e III |
| B [e III |
| 1 |
| (D) III |
| E 1 e II |
| |
| Marcar para revisão |
| A Norma ISO/IEC 27001 é uma das normas mais reconhecidas internacionalmente para a gestão da segurança da informação. |
| Qual é o principal objetivo da Norma ISO/IEC 27001? |
| A Estabelecer diretrizes para o descarte seguro de dados organizacionais. |
| B Fornecer um padrão para comunicações de rede seguras. |
| © Definir padrões para testes de penetração cibernética. |
| Criar uma estrutura para treinamento em segurança cibernética. |
| Prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). |
| |
| Marrar nara revisão |

O sistema de backup de missão crítica é também chamado de ambiente de:







Marcar para revisão

| A segurança da informação refere-se à prática de prevenir o acesso não autorizado, uso, divulgação, interrupção, modificação, inspeção, gravação ou destruição de informações. Qual problema de segurança é destacado nos exemplos de laptops levados para manutenção e discos rígidos de segunda mão comprados na Internet, como por exemplo, no eBay? |
|--|
| A Violações de não repúdio. |
| B Falha na integridade dos dados. |
| C Ausência de autenticidade dos dados. |
| Falhas na confidencialidade dos dados. |
| E Problemas na disponibilidade da informação. |

