

Meus Simulados

Teste seu conhecimento acumulado

Disc.: **INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO**

Aluno(a): **ALESSANDRO CIPRIANO GONZAGA**

202304664111


Acertos: **9,0** de 10,0

02/07/2023

1ª Questão

Acerto: **1,0** / **1,0**

Assinale a assertiva que **NÃO** representa um dos benefícios para a adoção da norma ABNT NBR ISO/IEC 27001:2013 por uma organização:

- ☐ Oportunidade de identificar e eliminar fraquezas
- ☐ Participação da gerência na Segurança da Informação
- ☐ Fornece segurança a todas as partes interessadas
- ☒  Isola recursos com outros sistemas de gerenciamento
- ☐ Mecanismo para minimizar o fracasso do sistema

Respondido em 02/07/2023 13:03:28


Explicação:

A resposta correta é: Isola recursos com outros sistemas de gerenciamento.

2ª Questão

Acerto: **1,0** / **1,0**

Assinale a assertiva que representa um dos benefícios para a adoção da norma ABNT NBR ISO/IEC 27001:2013 por uma organização:

- ☐ Fornece insegurança a todas as partes interessadas
- ☐ Isola recursos com outros sistemas de gerenciamento
- ☐ Não participação da gerência na Segurança da Informação
- ☒  Oportunidade de identificar e eliminar fraquezas
- ☐ Mecanismo para eliminar o sucesso do sistema

Respondido em 02/07/2023 13:09:07

Explicação:

A resposta correta é: Oportunidade de identificar e eliminar fraquezas.




Questão

Acerto: 1,0 / 1,0



"Todo acesso a cada objeto deve ser verificado quanto à autoridade. Esse princípio, quando aplicado sistematicamente, é o principal fundamento do sistema de proteção". Selecione a opção que se refere a esse mecanismo de proteção:

- ☐ Compartilhamento mínimo.
- ☐ Privilégio mínimo.
- ☒  Mediação completa.
- ☐ Padrões à prova de falhas.
- ☐ Separação de privilégios.


Respondido em 02/07/2023 13:11:31

Explicação:

A resposta correta é: Mediação completa.

**4ª Questão**Acerto: **1,0 / 1,0**

O processo de proteção de dados é um conjunto de ações que têm como objetivo garantir a segurança e a privacidade das informações armazenadas por uma organização ou indivíduo. Esse processo envolve a implementação de medidas técnicas, organizacionais e legais que visam prevenir o acesso, o uso, a alteração, a destruição ou a divulgação não autorizada de dados sensíveis. Nesse sentido, qual das opções abaixo é uma razão válida para justificar a importância de se realizar backups regularmente como medida de segurança da informação?

- ☐ Os backups são importantes apenas para grandes empresas que precisam proteger grandes quantidades de dados confidenciais.
- ☒  Caso as informações sejam perdidas ou corrompidas devido a falhas de hardware, malware ou erros humanos, um backup recente pode ser restaurado, garantindo a continuidade das operações.
- ☐ Backup é um desperdício de tempo e recursos, uma vez que as informações raramente são perdidas ou corrompidas.
- ☐ Os backups são úteis apenas para fins de auditoria e conformidade regulatória, e não têm relação direta com a segurança da informação.
- ☐ Realizar backups permite que você se livre de dados antigos e desnecessários, liberando espaço de armazenamento valioso.

Respondido em 02/07/2023 13:15:17


Explicação:

Caso as informações sejam perdidas ou corrompidas devido a falhas de hardware, malware ou erros humanos, um backup recente pode ser restaurado, garantindo a continuidade das operações. Realizar backups regularmente é uma medida fundamental de segurança da informação, pois permite que, em caso de perda, corrupção ou inacessibilidade de dados, uma cópia recente e íntegra possa ser restaurada, minimizando os prejuízos para a organização. Falhas de hardware, ataques de malware e erros humanos são comuns e podem resultar na perda de dados importantes. Portanto, é crucial que backups sejam realizados regularmente e que sejam armazenados em locais seguros e protegidos contra ameaças físicas e lógicas. Além disso, backups também podem ser úteis em situações de desastres naturais, como incêndios, inundações e terremotos, que podem destruir completamente os dados armazenados em um único local.

**5ª Questão**Acerto: **1,0 / 1,0**

Um membro da comissão de segurança precisa saber informações sobre cada um dos processos da GR. Ele consultará uma dentre as normas da família ISO/IEC 27000, que definem uma série de normas

relacionadas à segurança da informação. Ele precisa obter a norma:

- ☐ ISO/IEC 27002
- ☒  ISO/IEC 27005
- ☐ ISO/IEC 31000
- ☐ ISO/IEC 27000
- ☐ ISO/IEC 27001

Respondido em 02/07/2023 13:24:12

Explicação:


A resposta correta é: ISO/IEC 27005



6ª Questão

Acerto: 1,0 / 1,0

Dos planos que constituem o PCN (Plano de Continuidade de Negócios), selecione o que define as funções e responsabilidades das equipes envolvidas com acionamento das equipes de contingência:

- ☒  Plano de Administração de Crises (PAC).
- ☐ Plano de Contingência (Emergência).
- ☐ Plano de Continuidade Operacional (PCO).
- ☐ Plano de Recuperação de Desastres (PRD).
- ☐ PDCA (Plan-Do-Check-Execute).

Respondido em 02/07/2023 13:29:21

Explicação:


A resposta correta é: Plano de Administração de Crises (PAC).



7ª Questão

Acerto: 1,0 / 1,0

O crescimento das redes abertas fez com que surgissem vários problemas de segurança, que vão desde o roubo de senhas e interrupção de serviços até problemas de personificação, em que uma pessoa faz-se passar por outra para obter acesso privilegiado. Com isso, surgiu a necessidade de verificação da identidade tanto dos usuários quanto dos sistemas e processos. Dentro desse contexto, esse ato de verificação é chamado:

- ☒  autenticação.
- ☐ cadastro.
- ☐ confiabilidade.
- ☐ configuração.
- ☐ acessibilidade.

Respondido em 02/07/2023 13:28:02

Explicação:

A resposta correta é: Autenticação.



8ª Questão

Acerto: 1,0 / 1,0

A informação é estruturação e organização dos dados. Assim, os dados constituem a matéria prima da informação. Dentro dos aspectos da segurança da informação que exigem atenção são: confidencialidade, integridade e disponibilidade. A respeito da:

I - Na confidencialidade, as informações serão acessadas por quem tiver a devida autorização.

II - Na integridade, a informação que chega ao receptor pode não ser a que foi enviada pelo emissor

III - Disponibilidade, as informações podem ser acessadas por sistemas autorizados para tal fim.

Podemos considerar como corretas:

- ☐ III apenas.
- ☒ I e III.
- ☐ I, II, III.
- ☐ I apenas.
- ☐ II e III.

Respondido em 02/07/2023 13:33:55

Explicação:

A resposta correta é: I e III.

Na integridade, a informação que chega ao receptor é a que foi enviada pelo emissor. Ou seja, não houve modificação no envio da informação.



9ª Questão

Acerto: 1,0 / 1,0

É um tipo de malware feito para extorquir dinheiro de sua vítima. Esse tipo de ciberataque irá criptografar os arquivos do usuário e exigir um pagamento para que seja enviada a solução de descryptografia dos dados da vítima. O scareware é seu tipo mais comum e usa táticas ameaçadoras ou intimidadoras para induzir as vítimas a pagar.

O texto se refere ao:

- ☐ Spyware
- ☒ Ransomware
- ☐ DDoS
- ☐ Spam
- ☐ Botnet

Respondido em 02/07/2023 13:27:14

Explicação:

A resposta correta é: Ransomware



10ª Questão

Acerto: 0,0 / 1,0

Ativos são recursos econômicos controlados por uma organização que possuem valor e podem gerar benefícios futuros. Eles são divididos em duas categorias principais: ativos tangíveis e ativos intangíveis. De maneira geral,

qual exemplo pode ser considerado um ativo lógico tangível?

- ☐ Humanos.
- ☒ Informação.
- ☐ Marca.
- ☐ Imagem da organização.
- ☒ Colaboradores.

Respondido em 02/07/2023 13:55:40

Explicação:

Ativos tangíveis lógicos são aqueles que envolvem a informação e sua representação em algoritmos, por exemplo, uma fórmula química, os detalhes sobre a safra da laranja no mercado norte-americano, o algoritmo principal de busca do Google, os detalhes técnicos das baterias dos carros do Elon Musk.