



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

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

07/03/2023



1ª Questão

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

Dentre as opções a seguir, qual Norma Técnica apresenta um código de prática para a gestão da segurança da informação?

- ☐ ABNT NBR ISO/IEC 20000-1:2011
- ☐ ABNT NBR ISO 14001:2004
- ☒ ABNT NBR ISO/IEC 27002:2013
- ☐ ABNT NBR ISO 9001:2008
- ☐ ABNT NBR ISO/IEC 27001:2013

Respondido em 07/03/2023 16:49:47

**Explicação:**

A resposta correta é: ABNT NBR ISO/IEC 27002:2013



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:

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

Respondido em 07/03/2023 16:49:59

**Explicação:**

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




3ª 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:

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

Respondido em 07/03/2023 16:49:23

Explicação:


A resposta correta é: Mediação completa.



4ª Questão

Acerto: 1,0 / 1,0

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

- ☐ *Personal Unblocking Key.*
- ☐ *Ransomware.*
- ☒  *Disaster Recovery.*
- ☐ *Personal Identification Number.*
- ☐ *Daily Backup.*

Respondido em 07/03/2023 16:50:09

Explicação:


A resposta correta é: *Disaster Recovery.*



5ª Questão

Acerto: 1,0 / 1,0

Um funcionário de uma empresa concluiu que existe uma probabilidade de 67% de sobrecarga e problemas no serviço de distribuição de conteúdo de vídeo em um eventual aumento na demanda do servidor. Dentro da GR, essa conclusão pode ser obtida na etapa de:

- ☒  Processo de avaliação de riscos.
- ☐ Terminação de riscos.
- ☐ Definição do contexto.
- ☐ Monitoramento e controle de riscos.
- ☐ Aceitação do risco (residual).

Respondido em 07/03/2023 16:50:28

Explicação:


A resposta correta é: Processo de avaliação de riscos.



6ª Questão

Acerto: 1,0 / 1,0

O Risco é um conceito importante quando se trata do Plano de Continuidade de Negócios (PCN). A respeito do Risco, selecione a opção correta:

- ☐ Evento súbito e imprevisto que provoca grandes perdas ou danos a uma organização.
- ☐ É um conceito abstrato e com baixa chance de se transformar em um desastre.
- ☐ Não pode ser analisado em termos probabilísticos, uma vez que sempre está presente.
- ☒  Possível evento que pode causar perdas ou danos, ou dificultar o atingimento de objetivos.
- ☐ Normalmente não podem ser controlados.

Respondido em 07/03/2023 16:50:56

Explicação:

A resposta correta é: Possível evento que pode causar perdas ou danos, ou dificultar o atingimento de objetivos.




7ª

Questão

Acerto: 1,0 / 1,0

Redes de computadores conectadas à internet são alvos de invasões por parte de hackers. A ferramenta para permitir o acesso à rede apenas por endereços autorizados é:

- ☐ Criptografia.
- ☒  Firewall.
- ☐ Modem.
- ☐ Certificado digital.
- ☐ Antivírus.

Respondido em 07/03/2023 16:51:16

Explicação:

A resposta correta: Firewall.




8ª

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:

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

Respondido em 07/03/2023 16:52:34

Explicação:

A resposta correta é: Autenticação.

Indique a alternativa que pode conter um relacionamento mais apropriado entre os conceitos de AMEAÇA, IMPACTO, INCIDENTE e VULNERABILIDADE tratados pela Gestão de Riscos na Tecnologia da Informação.



ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Firewall da rede	Sem contrato de manutenção periódica	Defeito no firmware	Perda da confidencialidade nos acessos a internet



ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor Web	Ataque Hacker DDoS	Falta de atualizações do sistema operacional	Indisponibilidade



ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor de aplicação	Falta de atualizações do sistema operacional	Exploração de vulnerabilidades conhecidas	Perda de Confidencialidade, Integridade e Disponibilidade



ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Firewall da rede	Falta de atualizações do IOS	Perda de desempenho	Não suporta atualizações de hardware



ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor Web	Servidor de aplicação acessível pela internet	Ataque Hacker DDoS	Integridade

Respondido em 07/03/2023 16:54:22

Explicação:

A resposta correta é:

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor de aplicação	Falta de atualizações do sistema operacional	Exploração de vulnerabilidades conhecidas	Perda de Confidencialidade, Integridade e Disponibilidade

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:



Botnet



DDoS



Spyware



Spam



Ransomware

Respondido em 07/03/2023 16:52:53

Explicação:

A resposta correta é: Ransomware

