

Disc.: **INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO**Acertos: **10,0 de 10,0****03/04/2023**

1ª 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:

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

Respondido em 03/04/2023 20:56:17

Explicação:

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



2ª Questão

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

Observe o que diz o item 6.1.3 da norma técnica ABNT NBR ISO/IEC 27001:2013:

6.1.3 Tratamento de riscos de segurança da informação

A organização deve definir e aplicar um processo de tratamento de riscos de segurança da informação para:


(...)

b) determinar todos os controles que são necessários para implementar as opções escolhidas do tratamento do risco da segurança da informação.

d) elaborar uma declaração de aplicabilidade, que contenha os controles necessários (ver 6.1.3 b) e c)), e a justificativa para inclusões, sejam eles implementados ou não, bem como a justificativa para a exclusão dos controles do Anexo A.

Uma empresa que está se preparando para sofrer uma auditoria verificou que não constam na Declaração de Aplicabilidade, a exclusão e nem a justificativa de exclusão dos objetivos de controle e controles constantes na norma.

De acordo com o item 6.1.3 da norma, isso é passível de ser classificado como "Não-conformidade"?

- ☒  Sim
- ☐ Não se aplica a esta norma
- ☐ Falta informação nessa checagem para classificar
- ☐ Indica uma simples observação a ser feita
- ☐ Não

Respondido em 03/04/2023 20:54:59

Explicação:


A resposta correta é: Sim.



3ª Questão

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

Quanto mais complexa for uma senha, mais difícil será para o invasor quebrá-la com o uso de programas, exclusivamente. Levando em consideração essa afirmação, selecione a opção que possui a senha com maior grau de dificuldade de ser descoberta por um invasor:

- ☒  aX1!@7s5
- ☐ SeNhA123
- ☐ MaRiA96
- ☐ 69910814sa
- ☐ X1234Y1

Respondido em 03/04/2023 21:00:02

Explicação:


A resposta correta é: aX1!@7s5



4ª Questão

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

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

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

☐ Ransomware.

Respondido em 03/04/2023 20:56:28

Explicação:

A resposta correta é: *Disaster Recovery*.



5ª Questão

Acerto: 1,0 / 1,0

Um ataque de negação de serviço tenta afetar a disponibilidade de um ativo, por exemplo, inundando um servidor de aplicação em rede com mais dados do que é capaz de processar por unidade de tempo.

Se existe uma ferramenta, dentro do domínio do servidor, que reage a um ataque de negação de serviço, ela é classificada como uma medida de controle:

- ☐ Recuperadora
- ☐ Detectora
- ☒ Reativa
- ☐ Limitadora
- ☐ Preventiva

Respondido em 03/04/2023 21:02:50

Explicação:

A resposta correta é: Reativa



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

Respondido em 03/04/2023 21:00:59

Explicação:

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



7ª 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:

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

Respondido em 03/04/2023 21:03:21

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.



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:

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

Explicação:

A resposta correta é: Autenticação.



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 descriptografia 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:

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

Respondido em 03/04/2023 20:58:18

Explicação:

A resposta correta é: Ransomware



10ª Questão

Acerto: 1,0 / 1,0

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
Servidor Web	Servidor de aplicação acessível pela internet	Ataque Hacker DDoS	Integridade

☐

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

☐

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 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

Respondido em 03/04/2023 20:57:58

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