

Avaliação: **7,00** ptsNota SIA: **7,00** pts

Estação de trabalho liberada pelo CPF com o token em 04/11/2023 11:23:43.

**00182-TETI-2006: GESTÃO DE RISCO**

1.

Ref.: 5236642

Pontos: **1,00** / **1,00**

O risco residual é assim classificado quando não se tem uma resposta adequada ao risco, ou ele é considerado mínimo. Mesmo assim, deve passar pela etapa de:

- ☒ Monitoramento e análise crítica de riscos.
- ☐ Tratamento do risco.
- ☐ Aceitação do crivo.
- ☐ Marcação do critério.
- ☐ Comunicação e consulta do risco.

**00217-TETI-2006: GESTÃO DE CONTINUIDADE DO NEGÓCIO**

2.

Ref.: 5250547

Pontos: **0,00** / **1,00**

Selecione a opção que se enquadra em um dos motivos pelos quais o Plano de Continuidade de Negócios (PCN) pode precisar ser ajustado:

- ☐ A avaliação e o teste das estratégias são eficazes.
- ☒ Mudança nas funções e membros da equipe de continuidade de negócios.
- ☒ A organização precisa fazer mudanças para demonstrar aos seus usuários e clientes que está se atualizando constantemente.
- ☐ Surgiu uma nova metodologia no mercado e, portanto, deve ser implementada imediatamente nas estratégias atuais.
- ☐ As funções e responsabilidades são bem definidas.

**00278-TETI-2006: BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO**

3.

Ref.: 7826114


Pontos: **1,00** / **1,00**

As informações podem ser armazenadas em diversos formatos, como em papel, em mídias digitais, em dispositivos móveis, em redes de computadores, entre outros. Para criar uma senha segura é recomendável que os colaboradores observem qual instrução?

- ☐ Sempre utilizar a mesma senha para todas as contas.
- ☐ Não se deve alterar as senhas com frequência.
- ☒ As senhas devem ter, pelo menos, oito caracteres.


- ☐ Informar a senha a terceiros como forma de redundância.
- ☐ O usuário deve utilizar apenas letras ou números.

4.

 Ref.: 5250361

Pontos: 1,00 / 1,00

Crime cibernético é todo crime executado on-line e inclui, por exemplo, o roubo de informações no meio virtual. Uma recomendação correta de segurança aos usuários da internet para se proteger contra a variedade de crimes cibernéticos é:

- ☐ Proteger a rede *wireless* com senha que utiliza criptografia *Wired Equivalent Privacy* - WEP ou com uma *Virtual Protect Network* - VPN.
- ☒  Gerenciar as configurações de mídias sociais para manter a maior parte das informações pessoais e privadas bloqueadas.
- ☐ Manter os softwares atualizados, exceto os sistemas operacionais, pois esses já possuem mecanismos de segurança como *firewall*, antivírus e *antispyware*.
- ☐ Usar a mesma senha (composta por letras maiúsculas e minúsculas, números e símbolos) em todos os sites com conteúdo de acesso restrito, mantendo essa senha protegida em um aplicativo de gerenciamento de senhas.
- ☐ Usar uma suíte de segurança para a internet com serviços como *firewall*, *blockwall* e antivírus, como o *LibreOffice Security Suit*.




00319-TETI-2010: AMEAÇAS E VULNERABILIDADES À SEGURANÇA DE INFORMAÇÃO

5.

 Ref.: 4911331

Pontos: 1,00 / 1,00

Na segurança da informação, a fragilidade de um ativo ou grupo de ativos, que pode ser explorada por uma ou mais ameaças, é chamada de:



- ☐ Incidente de segurança da informação
- ☐ Desastre
- ☐ Risco
- ☐ Ameaça
- ☒  Vulnerabilidade

6.

 Ref.: 4911322

Pontos: 0,00 / 1,00

Os malwares executam ações danosas, programadas e desenvolvidas para esse fim em um computador. Abaixo, apresentam-se diversas formas de infectar ou comprometer um computador através de códigos maliciosos, exceto:

- ☒  pelo encaminhamento de arquivos .txt pela interface de rede do computador.
- ☐ pela exploração de vulnerabilidades existentes nos programas instalados.
- ☒  pelo acesso a páginas web maliciosas, utilizando navegadores vulneráveis.
- ☐ pela execução automática de mídias removíveis infectadas.
- ☐ pela execução de arquivos previamente infectados.



00441-TETI-2010: PRINCÍPIOS DA SEGURANÇA E O CICLO DE VIDA DA INFORMAÇÃO

7.


 Ref.: 5266850

Pontos: 1,00 / 1,00

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:

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

8.

 Ref.: 5277450


Pontos: 1,00 / 1,00

Assinale a opção correta a respeito de segurança da informação, análise de riscos e medidas de segurança física e lógica.

- ☐ As medidas de segurança dividem-se em dois tipos: as preventivas e as corretivas.
- ☐ Em análises de riscos, é necessário levar em conta os possíveis ataques que podem ocorrer, contudo desconsideram-se os possíveis efeitos desses ataques.
- ☒ Analisar riscos consiste em enumerar todos os tipos de risco, quais desses riscos expõem a informação e quais as consequências dessa exposição, bem como enumerar todas as possibilidades de perda direta e indireta.
- ☐ Como medida de segurança corretiva utilizam-se firewalls e criptografia.
- ☐ Como medida de segurança preventiva utilizam-se controle de acesso lógico e sessão de autenticação.

**00451-TETI-2006: NORMAS DE SEGURANÇA DA INFORMAÇÃO**

9.

 Ref.: 5295261


Pontos: 1,00 / 1,00

Um funcionário estava varrendo o chão da sala de uma empresa, na qual se encontra um servidor de domínio de rede local, quando não reparou que o cabo de rede que conecta ele ao roteador presente no outro lado da sala estava solto passando pelo chão, e então acabou por puxar o cabo com a vassoura, arrancando-o da placa de rede do servidor.

Segundo a norma ABNT NBR ISO/IEC 27002:2013, o responsável pela segurança do servidor deixou de colocar em prática o controle relacionado à:

- ☒ Segurança do cabeamento
- ☐ Segregação de funções
- ☐ Acordo de confidencialidade
- ☐ Inventário dos ativos
- ☐ Gerenciamento de senha de usuário

10.

 Ref.: 5298264

Pontos: 0,00 / 1,00

Qual norma técnica possui o seguinte título: "Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos"?

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

- ☒ ABNT NBR ISO/IEC 27001:2013
- ☐ ABNT NBR ISO 14001:2004