Estácio

Voltar

Meus Simulados

Teste seu conhecimento acumulado

Disc.: INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Aluno(a): KATIA REJANE RABELO SILVA 202305362843

Acertos: 9,0 de 10,0 30/06/2023

1ª Questão

Acerto: 1,0 / 1,0

O item 12.2.1 da norma ABNT NBR ISO/IEC 27002:2013 diz respeito aos controles contra *malware*, cujas diretrizes para implementação recomendam a proteção contra códigos maliciosos baseada em softwares de detecção de *malware* e reparo, na conscientização da informação, no controle de acesso adequado e nos planos de continuidade de negócio.

Com base no acima exposto, e no seu conhecimento de segurança da informação e sistemas de computação, marque a alternativa que possui uma das diretrizes recomendadas:

- ☐ Instalar e atualizar regularmente *softwares* de detecção e remoção de *malware*, independentemente da fabricante, procedência e confiabilidade, para o exame de computadores e mídias magnéticas.
- ☒ ✔ Estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e *softwares*, seja de redes externas, ou por qualquer outro meio, indicando quais medidas preventivas devem ser adotadas.
- ☐ Estabelecer uma política informal proibindo o uso de *softwares* autorizados.
- ☐ Ignorar informalmente a presença de quaisquer arquivos não aprovados ou atualização não autorizada.
- ☐ Conduzir análises informais, esporádicas e descompromissadas dos *softwares* e dados dos sistemas que suportam processos críticos de negócio.

Respondido em 30/06/2023 20:29:08

Explicação:

A resposta correta é: Estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e *softwares*, seja de redes externas, ou por qualquer outro meio, indicando quais medidas preventivas devem ser adotadas.

2ª 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:

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

Respondido em 30/06/2023 20:21:13

Explicação:

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

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:

- [ ] Separação de privilégios.
- [ ] Privilégio mínimo.
- [x] Mediação completa.
- [ ] Padrões à prova de falhas.
- [ ] Compartilhamento mínimo.

Respondido em 30/06/2023 20:21:17

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?

- [ ] Realizar backups permite que você se livre de dados antigos e desnecessários, liberando espaço de armazenamento valioso.
- [ ] Os backups são importantes apenas para grandes empresas que precisam proteger grandes quantidades de dados confidenciais.
- [x] 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.
- [ ] Os backups são úteis apenas para fins de auditoria e conformidade regulatória, e não têm relação direta com a segurança da informação.
- [ ] Backup é um desperdício de tempo e recursos, uma vez que as informações raramente são perdidas ou corrompidas.

Respondido em 30/06/2023 20:22:19

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: 0,0 / 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 31000
- [ ] ISO/IEC 27001
- [ ] ISO/IEC 27000
- [x] ISO/IEC 27002
- [ ] ISO/IEC 27005

Respondido em 30/06/2023 20:22:51

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:

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

Respondido em 30/06/2023 20:28:15

Explicação:

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

7ª Questão Acerto: 1,0 / 1,0

Na questão que avalia conhecimento de informática, a menos que seja explicitamente informado o contrário, considere que: todos os programas mencionados estejam em configuração-padrão, em português; o mouse esteja configurado para pessoas destras; expressões como clicar, clique simples e clique duplo refiram-se a cliques com o botão esquerdo do mouse; e teclar corresponda à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Considere também que não haja restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados.

Assinale a alternativa que apresenta procedimento de segurança da informação que pode ser adotado pelas organizações.

- [x] realizar, periodicamente, análises de riscos, com o objetivo de contemplar as mudanças nos requisitos de segurança da informação
- [ ] descartar o inventário dos ativos, caso a organização possua
- [ ] conceder aos funcionários o acesso completo aos sistemas e à rede (intranet) da organização
- [ ] não envolver a direção com a segurança da informação, tendo em vista que ela já possui diversas outras atribuições
- [ ] direcionar os funcionários apenas para o exercício de suas funções diárias; pois treinamentos em segurança da informação ou outros eventos relacionados devem ser evitados

Respondido em 30/06/2023 20:23:48

Explicação:

A resposta correta é: realizar, periodicamente, análises de riscos, com o objetivo de contemplar as mudanças nos requisitos de segurança 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.
- [x] autenticação.
- [ ] configuração.
- [ ] cadastro.
- [ ] acessibilidade.

Respondido em 30/06/2023 20:23:08

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:

- [ ] DDoS
- [ ] Spyware
- [x] Ransomware
- [ ] Spam
- [ ] Botnet

Respondido em 30/06/2023 20:23:11

Explicação:

A resposta correta é: Ransomware

10ª Questão Acerto: 1,0 / 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?

- [ ] Imagem da organização.
- [x] Informação.
- [ ] Marca.
- [ ] Humanos.
- [ ] Colaboradores.

Respondido em 30/06/2023 20:23:35

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.