1

Marcar para revisão

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 a 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 checou 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"?

A Não se aplica a esta norma

B Falta informação nessa checagem para classificar

C Indica uma simples observação a ser feita

D Não

E Sim

2

Marcar para revisão

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

A ABNT NBR ISO/IEC 27002:2013

B ABNT NBR ISO 14001:2004

C ABNT NBR ISO 9001:2008

D ABNT NBR ISO/IEC 20000-1:2011

E ABNT NBR ISO/IEC 27001:2013

3

Marcar para revisão

The ISO Survey of Certifications, é uma ferramenta valiosa que fornece insights sobre a adoção e difusão de padrões ISO em todo o mundo.

Qual das alternativas abaixo melhor descreve o que é o The ISO Survey of Certifications?

A Uma conferência onde são discutidos os padrões ISO.

B Uma pesquisa anual sobre o número de certificados válidos para os padrões do sistema de gerenciamento ISO em todo o mundo.

C Uma revista anual sobre as atualizações das normas ISO.

D Um site onde as organizações podem obter certificações ISO.

E Uma organização que define as normas ISO.

4

Marcar para revisão

A certificação ISO/IEC 27001 oferece múltiplos benefícios para as organizações, proporcionando uma estrutura robusta e reconhecida para a gestão da segurança da informação.

Por que uma organização pode optar pela certificação ISO/IEC 27001?

A Para demonstrar a conformidade com os requisitos de SGSI e gerenciar riscos.

B Para garantir que nenhum incidente de segurança ocorra.

C Para substituir a necessidade de uma equipe de segurança da informação.

D Para garantir a satisfação do usuário final em todas as transações.

E Para evitar toda e qualquer ameaça cibernética.

5

Marcar para revisão

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:

A 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.

B Conduzir análises informais, esporádicas e descompromissadas dos *softwares* e dados dos sistemas que suportam processos críticos de negócio.

C Estabelecer uma política informal proibindo o uso de *softwares* autorizados.

D Ignorar informalmente a presença de quaisquer arquivos não aprovados ou atualização não autorizada.

E 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.

6

Marcar para revisão

A Norma ISO/IEC 27001 é uma das normas mais reconhecidas internacionalmente para a gestão da segurança da informação.

Qual é o principal objetivo da Norma ISO/IEC 27001?

A Fornecer um padrão para comunicações de rede seguras.

B Definir padrões para testes de penetração cibernética.

C Prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI).

D Estabelecer diretrizes para o descarte seguro de dados organizacionais.

E Criar uma estrutura para treinamento em segurança cibernética.

7

Marcar para revisão

A tríade CID é uma forma simplificada de representar os múltiplos objetivos da segurança da informação.

O que a tríade CID, que o SGSI busca preservar, representa?

A Complacência, Integridade, Durabilidade.

B Confidencialidade, Integridade, Disponibilidade.

C Consistência, Implementação, Durabilidade.

D Certificação, Inovação, Desenvolvimento.

E Computação, Internet, Dados.

8

Marcar para revisão

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

A Oportunidade de identificar e eliminar fraquezas

B Mecanismo para eliminar o sucesso do sistema

C Não participação da gerência na Segurança da Informação

D Fornece insegurança a todas as partes interessadas

E Isola recursos com outros sistemas de gerenciamento

9

Marcar para revisão

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

A Isola recursos com outros sistemas de gerenciamento

B Fornece segurança a todas as partes interessadas

C Mecanismo para minimizar o fracasso do sistema

D Oportunidade de identificar e eliminar fraquezas

E Participação da gerência na Segurança da Informação

Questão **1** de 9

1 2 3 4 5

6 7 8 9

○ Em branco **(9)**

Finalizar exercício