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 Sim

B Não

C Indica uma simples observação a ser feita

D Falta informação nessa checagem para classificar

E Não se aplica a esta norma

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
A resposta correta é: 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 9001:2008

C ABNT NBR ISO/IEC 27001:2013

D ABNT NBR ISO 14001:2004

E ABNT NBR ISO/IEC 20000-1:2011

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
A alternativa correta é a ABNT NBR ISO/IEC 27002:2013. Esta norma técnica é um código de prática para a gestão da segurança da informação. Ela fornece diretrizes para estabelecer, implementar, manter e melhorar continuamente a gestão da segurança da informação em uma organização. As recomendações desta norma são genéricas e destinadas a serem aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.

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 Um site onde as organizações podem obter certificações ISO.

B Uma revista anual sobre as atualizações das normas ISO.

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

D Uma conferência onde são discutidos os padrões ISO.

E Uma organização que define as normas ISO.

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
Trata-se de uma pesquisa anual sobre o número de certificados válidos para os padrões do sistema de gerenciamento ISO em todo o mundo.

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 evitar toda e qualquer ameaça cibernética.

B Para garantir que nenhum incidente de segurança ocorra.

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

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

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

✓ **Resposta correta**

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A certificação ISO/IEC 27001 mostra que a organização segue um padrão reconhecido globalmente para o SGSI, ajudando a gerenciar riscos de segurança da informação e demonstrando conformidade a partes interessadas.

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

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

C 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.

D 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.

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

✓ **Resposta correta**

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A alternativa correta é a D, que sugere o estabelecimento de 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. Esta alternativa está alinhada com as diretrizes da norma ABNT NBR ISO/IEC 27002:2013, que recomenda a implementação de controles contra *malware* através de medidas como a conscientização da informação, o controle de acesso adequado e a criação de planos de continuidade de negócio. Portanto, uma política formal de proteção é uma estratégia eficaz para mitigar os riscos associados à importação de arquivos e softwares potencialmente maliciosos.

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 Definir padrões para testes de penetração cibernética.

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

C Estabelecer diretrizes para o descarte seguro de dados organizacionais.

D Fornecer um padrão para comunicações de rede seguras.

E Criar uma estrutura para treinamento em segurança cibernética.

✓ **Resposta correta**

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A Norma ISO/IEC 27001 foi desenvolvida para fornecer um modelo para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um SGSI.

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 Computação, Internet, Dados.

E Certificação, Inovação, Desenvolvimento.

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
A tríade CID é um modelo de segurança da informação que visa preservar a confidencialidade, integridade e disponibilidade das informações.

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

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
A norma ABNT NBR ISO/IEC 27001:2013 é uma norma internacional que fornece o modelo para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Um dos benefícios de sua adoção é a oportunidade de identificar e eliminar fraquezas no sistema de segurança da informação da organização. Portanto, a alternativa correta é: "Oportunidade de identificar e eliminar fraquezas".

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 Oportunidade de identificar e eliminar fraquezas

B Mecanismo para minimizar o fracasso do sistema

C Participação da gerência na Segurança da Informação

D Fornece segurança a todas as partes interessadas

E Isola recursos com outros sistemas de gerenciamento

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
A alternativa que não representa um benefício da adoção da norma ABNT NBR ISO/IEC 27001:2013 é a opção E: "Isola recursos com outros sistemas de gerenciamento". Esta norma, na verdade, promove a integração de recursos e sistemas de gerenciamento, ao invés de isolá-los. Portanto, a afirmação é incorreta e não representa um benefício da adoção da norma.

Questão **1** de 9

1 2 3 4 5
6 7 8 9

○ Corretas **(9)**
○ Em branco **(0)**