ISO/IEC 27001:2022 - SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO - OPERAÇÃO

5. OPERAÇÃO

5.1. Planejamento e controle operacionais

A organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos e para implementar as ações determinadas na Seção 6:

- estabelecendo critérios para os processos;
- implementando controles dos processos de acordo com os critérios.

A informação documentada deve ser disponibilizada na abrangência necessária para gerar a confiança de que os processos estão sendo realizados conforme planejado.

Gerar confiança é um ponto importante para a organização, pois é a partir disso que todas as partes agregadas vão conceder valor a ela.

ATENÇÃO

É possível que esse tópico esteja em uma questão de prova.

A organização deve controlar as mudanças planejadas e analisar criticamente as consequências de mudanças não intencionais, tomando ações para mitigar quaisquer efeitos adversos, conforme necessário.

A organização deve assegurar que os processos, produtos ou serviços providos externamente que são relevantes para o sistema de gestão da segurança da informação sejam controlados.

5.2. Avaliação de riscos da segurança da informação

A organização deve realizar avaliações de riscos da segurança da informação a intervalos planejados (mensalmente ou semestralmente), ou quando mudanças significativas forem propostas ou ocorrerem, levando em conta os critérios estabelecidos em 3.1.2 "a":

a) estabeleça e mantenha critérios de riscos de segurança da informação que incluam:

1. critérios de aceitação de riscos; e
2. critérios para realizar as avaliações de riscos de segurança da informação;

A organização deve reter informação documentada dos resultados das avaliações de riscos da segurança da informação.

5m

5.3. Tratamento de riscos da segurança da informação

A organização deve implementar o plano de tratamento de riscos da segurança da informação.

A organização deve reter informação documentada dos resultados do tratamento de riscos da segurança da informação.

EXERCÍCIOS DE FIXAÇÃO

1. (2023) A organização não precisa controlar as mudanças planejadas, pois apenas as mudanças não intencionais requerem análise crítica e ação para mitigar efeitos adversos.

( ) Certo
( ) Errado

A organização precisa controlar as mudanças planejadas,**inclusive as mudanças não intencionais** que requerem análise crítica e ação para mitigar efeitos adversos.

---

2. (2023) A organização não precisa estabelecer critérios de aceitação de riscos, apenas critérios para realizar as avaliações de riscos de segurança da informação são necessários.

( ) Certo
( ) Errado

A organização precisa estabelecer critérios de aceitação de riscos. Os critérios para realizar as avaliações de riscos e a aceitação do risco de segurança da informação são necessários.

GABARITO

1. E
2. E