Viu algum erro neste material? Contate-nos em: degravacoes@grancursosonline.com.br

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

6. AVALIAÇÃO DE DESEMPENHO

6.1. Monitoramento, medição, análise e avaliação

A organização deve determinar:

a) o que precisa ser **monitorado** e **medido**, incluindo processos e controles da segurança da informação;

b) **os métodos para monitoramento, medição, análise e avaliação**, conforme aplicável, para assegurar **resultados válidos**. Convém que os métodos selecionados produzam **resultados comparáveis e reproduzíveis** para serem **considerados válidos**;

c) **quando** o monitoramento e a medição devem ser realizados;

d) **quem deve** monitorar e medir;

e) **quando** os resultados do monitoramento e da medição devem ser analisados e avaliados;

f) **quem deve analisar e avaliar** estes resultados.

Informação documentada deve ser disponibilizada como evidência dos resultados.

A organização deve avaliar o desempenho da segurança da informação e a eficácia do sistema de gestão da segurança da informação.

6.2. Auditoria interna

6.2.1. Geral

A organização deve conduzir **auditorias internas a intervalos planejados** para prover informações sobre se o sistema de gestão da segurança da informação:

a) **está em conformidade com**:

1. os **próprios requisitos** da organização para o seu sistema de gestão da segurança da informação;

2. os **requisitos deste documento**;

b) está **efetivamente implementado e mantido**.

6.2.2. Programa de auditoria interna

A organização deve **planejar, estabelecer, implementar e manter programa(s) de auditoria**, incluindo **frequência, métodos, responsabilidades, requisitos de planejamento e relato**.

Ao estabelecer programa(s) de auditoria interna, a organização deve considerar a **importância dos processos pertinentes e os resultados de auditorias anteriores.**

A organização **deve**:

a) **definir os critérios e o escopo** da auditoria, para cada auditoria;

b) **selecionar auditores e conduzir auditorias** que assegurem **objetividade** e **imparcialidade** do processo de auditoria;

- ser objetivo e imparcial implica ter segregação de funções, afastando pessoas do local a ser auditado da realização daquela auditoria, visando evitar possíveis fraudes do resultado.

c) assegurar que os resultados das auditorias sejam relatados para a gestão pertinente.

Informação documentada deve ser disponibilizada como evidência da implementação do(s) programa(s) de auditoria e dos resultados da auditoria.

6.3. Análise crítica pela Direção

6.3.1. Geral

A Alta Direção deve analisar criticamente o sistema de gestão da segurança da informação da organização **em intervalos planejados**, para assegurar a sua **contínua adequação**, **pertinência** e **eficácia**.

ATENÇÃO

5m

Os conceitos de "processo de realização" e de "intervalos planejados" são frequentemente mencionados na norma; portanto, são importantes para o concurso.

6.3.2. Entradas da análise crítica pela Direção

A análise crítica pela Direção deve incluir considerações em relação a:

a) situação das ações de análises críticas anteriores pela Direção;

b) mudanças nas questões internas e externas que sejam relevantes para o sistema de gestão da segurança da informação;

c) mudanças nas necessidades e expectativas das partes interessadas que sejam relevantes para o sistema de gestão da segurança da informação

d) feedback sobre o desempenho da segurança da informação, incluindo tendências para:

1. não conformidades e ações corretivas;
2. resultados da medição e monitoramento;
3. resultados de auditorias;
4. cumprimento dos objetivos da segurança da informação;

e) feedback das partes interessadas;

f) resultados da avaliação dos riscos e situação do plano de tratamento de riscos;

g) oportunidades para a melhoria contínua.

6.3.3. Resultados da análise crítica pela Direção

Os resultados da análise crítica pela Direção devem incluir **decisões relativas às oportunidades para melhoria contínua** e quaisquer necessidades de **mudanças do sistema** de gestão da segurança da informação.

Informação documentada deve ser disponibilizada como evidência dos resultados das análises críticas pela Direção.

EXERCÍCIOS DE FIXAÇÃO

1. No que diz respeito aos papéis, responsabilidades e autoridades organizacionais, o que a Alta Direção deve assegurar?

a. As responsabilidades e autoridades dos papéis relevantes para a segurança da informação não precisam ser atribuídos

b. As responsabilidades e autoridades dos papéis relevantes para a segurança da informação devem ser atribuídos, mas não comunicados

c. A Alta Direção não precisa atribuir a responsabilidade e autoridade para assegurar a conformidade do sistema de gestão da segurança da informação

d. A Alta Direção deve atribuir a responsabilidade e autoridade para assegurar que o sistema de gestão da segurança da informação esteja em conformidade com os requisitos do documento

e. A Alta Direção não precisa atribuir responsabilidades e autoridades para relatar sobre o desempenho do sistema de gestão da segurança da informação

a. As responsabilidades e autoridades dos papéis relevantes para a segurança da informação **precisam** ser atribuídos

b. As responsabilidades e autoridades dos papéis relevantes para a segurança da informação devem ser atribuídos **e comunicados**

c. A Alta Direção **precisa** atribuir a responsabilidade e autoridade para assegurar a conformidade do sistema de gestão da segurança da informação

d. A Alta Direção **deve** atribuir a responsabilidade e autoridade para assegurar que o sistema de gestão da segurança da informação esteja em conformidade com os requisitos do documento

e. A Alta Direção **precisa** atribuir responsabilidades e autoridades para relatar sobre o desempenho do sistema de gestão da segurança da informação

10m

2. De acordo com a norma ISO 27001, ao estabelecer programas de auditoria interna, qual elemento específico a organização deve considerar?

a. A capacidade da equipe de vendas em atingir suas metas.
b. A popularidade da marca no mercado.
c. A importância dos processos pertinentes e os resultados de auditorias anteriores.
d. A cor da marca da organização.
e. O tipo de lanches disponíveis na cafeteria da empresa

De acordo com a norma ISO 27001, ao estabelecer programas de auditoria interna, **a importância dos processos pertinentes e os resultados de auditorias anteriores** é o elemento específico que a organização deve considerar.

GABARITO

1. d
2. c

Este material foi elaborado pela equipe pedagógica do Gran Concursos, de acordo com a aula preparada e ministrada pelo professor Jósis Alves.
A presente degravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.