# ISO/IEC 27001:2022 – SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO – PLANEJAMENTO

Logo ao início, a norma já aborda as ações que podem ser tomadas

## 3.1 AÇÕES PARA ABORDAR RISCOS E OPORTUNIDADES

Logo ao início, a norma já aborda as ações que podem ser tomadas para encontrar riscos e oportunidades.

### 3.1.1. Geral

Precisamos determinar os riscos e oportunidades que precisam ser abordados para:

a) assegurar que o sistema de gestão da segurança da informação possa alcançar seus resultados pretendidos;

b) prevenir ou reduzir os efeitos indesejados; e

c) alcançar a melhoria contínua.

A organização deve planejar:

d) as ações para abordar estes riscos e oportunidades; e

e) como:

1. integrar e implementar as ações dentro dos processos do seu sistema de gestão da segurança da informação;

2. avaliar a eficácia destas ações.

Em torno desses tópicos vai ser possível encontrar questões buscando saber o que a organização deve planejar.

### 3.1.2. Avaliação de riscos de segurança da informação

A organização deve estabelecer e aplicar um processo de avaliação de riscos de segurança da informação que:

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;

b) assegure que as contínuas avaliações de riscos de segurança da informação repetidas produzam resultados comparáveis, válidos e consistentes;

Isso significa que toda vez que uma avaliação de risco for feita, será possível reproduzir resultados para comparação, validação e, assim, verificar que aquilo é consistente.

c) identifique os riscos de segurança da informação:

1. aplicando o processo de avaliação do risco de segurança da informação para identificar os riscos associados com a perda de confidencialidade, integridade e disponibilidade da informação dentro do escopo do sistema de gestão da segurança da informação; e

**Obs.:** Os escopos do sistema dentro da gestão de segurança da informação podem ser variados. Dentro dele pode estar toda a organização, somente um departamento ou, até mesmo, apenas um serviço.

2. identificando os proprietários dos riscos.

d) analise os riscos de segurança da informação:

1. avaliando as consequências potenciais que podem resultar se os riscos identificados no tópico "C" forem materializados;

2. avaliando a probabilidade realística da ocorrência dos riscos identificados no tópico que foi "C"; e

3. determinando os níveis de risco;

e) avalie os riscos de segurança da informação:

1. comparando os resultados da análise de riscos com os critérios de riscos 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;

2. priorizando os riscos analisados para o tratamento do risco.

5m

Ao analisar e avaliar os riscos, é possível ter uma lista priorizada dos riscos para que dentro desse grau de importância haja um tratamento. Dessa forma, existem riscos em potencial com maiores consequências, e assim sucessivamente, até possíveis riscos residuais. Caso não haja uma priorização, haverá uma grande demanda de recursos para fazer o tratamento dos mais diversos riscos sem um critério.

### 3.1.3. Tratamento de riscos da segurança da informação

A organização deve estabelecer e aplicar um processo de tratamento de riscos da segurança da informação para:

a) selecionar, de forma apropriada, as opções de tratamento dos riscos da segurança da informação, levando em consideração os resultados da avaliação de riscos;

b) determinar todos os controles que são necessários para implementar as opções escolhidas do tratamento de riscos da segurança da informação;

NOTA 1: As organizações podem projetar os controles, conforme requerido, ou identificá-los de qualquer outra fonte.

c) comparar os controles determinados no tópico "b" do slide anterior com aqueles do Anexo A e verificar se nenhum controle necessário foi omitido;

NOTA 2: O Anexo A contém uma lista de possíveis controles de segurança da informação. Os usuários deste documento são direcionados ao utilizar o Anexo A para assegurar que nenhum controle necessário seja omitido.

O anexo A não está nesta aula, mas é recomendado que ele esteja presente nos estudos.

NOTA 3: Os controles de segurança da informação listados no Anexo A não são exaustivos, e controles de segurança da informação adicionais podem ser incluídos, se necessário.

d) elaborar uma Declaração de Aplicabilidade que contenha:

- os controles necessários (ver tópicos "b" e "c" mencionados anteriormente);
- a justificativa para inclusões;
- se os controles necessários são implementados ou não; e
- a justificativa para a exclusão de quaisquer controles do Anexo A.

O tópico da Declaração de Aplicabilidade já foi visto em provas, por isso é necessário atenção.

e) preparar um plano para tratamento de riscos da segurança da informação; e

f) obter a aprovação dos proprietários dos riscos do plano de tratamento de riscos da segurança da informação e a aceitação dos riscos residuais de segurança da informação.

NOTA 4: O processo de tratamento e a avaliação de riscos da segurança da informação deste documento estão alinhados com os princípios e as diretrizes gerais estabelecidos na ABNT NBR ISO 31000.

## 3.2 OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO E PLANEJAMENTO PARA ALCANÇÁ–LOS

A organização deve estabelecer os objetivos da segurança da informação para as funções e níveis relevantes. Os objetivos da segurança da informação devem:

10m

**ATENÇÃO**

Compreender os objetivos é de extrema importância, pois esses tópicos têm grandes chances de estarem na prova.

a) ser consistentes com a política da segurança da informação;

b) ser mensuráveis (se praticável);

c) levar em conta os requisitos da segurança da informação aplicáveis e os resultados da avaliação e tratamento de riscos;

d) ser monitorados;
e) ser comunicados;
f) ser atualizados, conforme apropriado;
g) ser disponibilizados como informação documentada.

---

A organização deve reter informação documentada dos objetivos da segurança da informação.

Ao planejar como alcançar os seus objetivos da segurança da informação, a organização deve determinar:

h) o que será feito:
i) quais recursos serão necessários;
j) quem será responsável;
k) quando estará concluído; e
l) como os resultados serão avaliados.

## 3.3 PLANEJAMENTO DE MUDANÇAS

Quando a organização determina necessidade para mudanças do sistema de gestão da segurança da informação, estas mudanças devem ser conduzidas de uma forma planejada.

Sempre que houver uma mudança, ela deverá ser conduzida com um planejamento prévio, com toda uma autorização feita anteriormente. Isso porque ela pode refletir em atividades normais da organização.

---

**DIRETO DO CONCURSO**

**1.** (2022/INSTITUTO CONSULPLAN/IPASEM/TÉCNICO EM INFORMÁTICA) A ISO 27001 é uma norma internacional de gestão de segurança da informação, que tem como princípio geral a adoção de um conjunto de requisitos, processos e controles, que visam gerir adequadamente os riscos de segurança da informação presentes nas organizações. Sobre as características da norma ISO 27001, assinale a afirmativa INCORRETA.

a. Determina as responsabilidades e seus responsáveis, acabando com a dúvida de quem decide ou cuida de determinado assunto.

b. Com a análise de riscos e seu plano de tratamento, os controles são planejados e direcionados para evitar que qualquer ponto fraco do sistema seja explorado.

c. Recursos serão aplicados para reduzir os riscos de forma geral, ao invés de focar em uma determinada área e deixar as demais expostas, contribuindo para redução de custos.

d. Não exige que a organização esteja em conformidade com todas as leis e requisitos contratuais, impactando positivamente na gestão de riscos, redução de impacto e governança corporativa.
e. Abrange a segurança da informação em todos os níveis, fornecendo melhores práticas de gestão da segurança da informação. Além disso, seus controles são reconhecidos internacionalmente.

A questão busca encontrar um erro dentre as alternativas.
a) Determina as responsabilidades e seus responsáveis, acabando com a dúvida de quem decide ou cuida de determinado assunto.
b) Com a análise de riscos e seu plano de tratamento, os controles são planejados e direcionados para evitar que qualquer ponto fraco do sistema seja explorado.
c) Recursos serão aplicados para reduzir os riscos de forma geral, ao invés de focar em uma determinada área e deixar as demais expostas, contribuindo para redução de custos.
d) **Exige que a organização esteja em conformidade com todas as leis** e requisitos contratuais, impactando positivamente a gestão de riscos, a redução de impacto e a governança corporativa.
15m
e) Abrange a segurança da informação em todos os níveis, fornecendo melhores práticas de gestão da segurança da informação. Além disso, seus controles são reconhecidos internacionalmente.

---

**2.** Quais são as três principais características que um sistema de gestão de segurança da informação preserva ao aplicar um processo de gestão de riscos, conforme mencionado neste documento?
a. Autenticidade, confidencialidade e integridade
b. Disponibilidade, autenticidade e não repúdio
c. Confidencialidade, integridade e disponibilidade
d. Autenticidade, disponibilidade e não repúdio
e. Integridade, não repúdio e confidencialidade

Ao se falar no sistema de gestão de segurança da informação, buscamos assegurar características como aquelas elencadasno CID (confidencialidade, integridade e disponibilidade).

---

# GABARITO

1. d
2. c