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

4. APOIO

4.1. Recursos

A organização deve determinar e prover recursos necessários para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão da segurança da informação.

4.2. Competência

A organização deve:

a) determinar a competência necessária da(s) pessoa(s) que realiza(m) trabalho sob o seu controle que afete o desempenho da segurança da informação;

b) assegurar que essas pessoas sejam competentes, com base em educação, treinamento ou experiência apropriados;

Essa educação vem através de cursos, treinamentos internos, workshops, entre outros.

c) onde aplicável, tomar ações para adquirir a competência necessária e avaliar a eficácia das ações tomadas; e

Dessa forma, se foi provido um treinamento ou curso, é necessário haja uma forma pré-definida de avaliar a eficácia dessa ação, buscando observar se as pessoas foram capacitadas.

d) reter informação documentada apropriada como evidência da competência.

Com a documentação dos treinamentos, é possível observar se as pessoas foram devidamente capacitadas para exercer suas funções.

NOTA: As ações aplicáveis podem incluir, por exemplo: o fornecimento de treinamento, a mentoria ou a reatribuição dos atuais funcionários; ou empregar ou contratar pessoas competentes.

A mentoria é uma ação importante, pois pessoas mais experientes na área orientam aqueles que ainda não detém tanta experiência.

4.3. Conscientização

Pessoas que realizam trabalho sob o controle da organização devem estar cientes:

a) da política da segurança da informação;

5m

b) da sua contribuição para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e

c) das implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

4.4. Comunicação

A organização deve determinar a necessidade de comunicações internas e externas relevantes para o sistema de gestão da segurança da informação, incluindo:

ATENÇÃO

O examinador pode buscar saber quais são os tópicos da comunicação.

a) o que comunicar;
b) quando comunicar;
c) com quem comunicar;
d) como se comunicar.

4.5. Informação documentada

4.5.1. Geral

O sistema de gestão da segurança da informação da organização deve incluir:

a) informação documentada requerida por este documento; e

b) informação documentada determinada pela organização como sendo necessária para a eficácia do sistema de gestão da segurança da informação.

NOTA: A abrangência da informação documentada para o sistema de gestão da segurança da informação pode variar de uma organização para outra devido:

1. ao tamanho da organização e seu tipo de atividades, processos, produtos e serviços;

Cada organização é única, assim as documentações são diferentes entre si. Isso porque as atividades e processos organizacionais são diferentes, além da diferença da complexidade dos processos e competência das pessoas.

2. à complexidade dos processos e suas interações; e
3. à competência das pessoas.

4.5.2. Criando e atualizando

Ao criar e atualizar a informação documentada, a organização deve assegurar, de forma apropriados(as):

a) identificação e descrição (por exemplo, título, data, autor ou um número de referência);

b) formato (por exemplo, linguagem, versão do software, gráficos) e seu meio (por exemplo, papel, eletrônico); e

c) análise crítica e aprovação para pertinência e adequação.

4.5.3. Controle da informação documentada

A informação documentada requerida pelo sistema de gestão da segurança da informação e por este documento deve ser controlada para assegurar que:

a) esteja disponível e adequada para o uso, onde e quando necessário;

b) esteja protegida adequadamente (por exemplo, contra perda de confidencialidade, uso indevido ou perda de integridade).

Para o controle da informação documentada, a organização deve considerar as seguintes atividades, conforme aplicável:

c) distribuição, acesso, recuperação e uso;

d) armazenamento e preservação, incluindo a preservação da legibilidade;

e) controle de mudanças (por exemplo, controle de versão); e

Realizar o versionamento, com a criação de versões para que seja possível verificar as mudanças.

f) retenção e disposição.

A informação documentada de origem externa, determinada pela organização como necessária para o planejamento e a operação do sistema de gestão da segurança da informação, deve ser identificada como apropriado, e controlada.

10m

NOTA: O acesso pode implicar uma decisão quanto à permissão para apenas ver a informação documentada, ou na permissão e autoridade para ver e alterar a informação documentada, etc.

DIRETO DO CONCURSO

1. (2022/OBJETIVA CONCURSOS/PROCEMPA/ANALISTA EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO/SEGURANÇA DE DADOS) A Norma ISO 27001 tem como princípio geral a adoção, pela organização, de um conjunto de requisitos, processos e controles, com o objetivo de mitigar e gerir adequadamente o risco da organização. O principal modelo aplicado nos processos do Sistema de Gestão de Segurança da Informação é o:

a. Plan-Do-Check-Act (PDCA).
b. Audit-Integrity-confidentiality e privacy (AICP).
c. Do-Plan-Available-Risc (DPAR).
d. Risc-PLAN-Available-Check (RPAC).
e. Management-Do-Check-Audit (MDCA).

O principal modelo aplicado nos processos do Sistema de Gestão de Segurança da Informação que busca é o PDCA. Com isso temos o planejamento → execução → verificação → ação.

---

2. (2022/CENTRO DE SELEÇÃO E DE PROMOÇÃO DE EVENTOS UNB/CESPE/CEBRASPE/SECONT/AUDITOR DO ESTADO/TECNOLOGIA DA INFORMAÇÃO) Julgue os itens a seguir, a respeito de políticas de segurança da informação, segurança de redes de computadores e prevenção e tratamento de incidentes.
Conforme a NBR ISO/IEC 27001, a informação documentada de origem externa necessária para a eficácia do sistema de gestão de segurança da informação e voltada ao planejamento global e à sua operação deve ser classificada como pública no âmbito da organização, dispensando-se restrições e controles adicionais de acesso.

( ) Certo
( ) Errado

Não podem ser dispensadas restrições e controles adicionais de acesso. É necessário identificar, classificar e controlar.

GABARITO

1. a
2. E