GRAN CONCURSOS

TECNOLOGIA DA INFORMAÇÃO

Gestão de Segurança da Informação: Norma NBR ISO/IEC n. 27.001:2022

Presidente: Gabriel Granjeiro

Vice-Presidente: Rodrigo Calado

Diretor Pedagógico: Erico Teixeira

Diretora de Produção Educacional: Vivian Higashi

Gerência de Produção de Conteúdo: Magno Coimbra

Coordenadora Pedagógica: Élica Lopes

CÓDIGO:

230322091449

PATRÍCIA QUINTÃO

Mestre em Engenharia de Sistemas e computação pela COPPE/UFRJ, Especialista em Gerência de Informática e Bacharel em Informática pela UFV. Atualmente é professora no Gran Cursos Online; Analista Legislativo (Área de Governança de TI), na Assembleia Legislativa de MG; Escritora e Personal & Professional Coach. Atua como professora de Cursinhos e Faculdades, na área de Tecnologia da Informação, desde 2008. É membro: da Sociedade Brasileira de Coaching, do PMI, da ISACA, da Comissão de Estudo de Técnicas de Segurança (CE-21:027.00) da ABNT, responsável pela elaboração das normas brasileiras sobre gestão da Segurança da Informação. Autora dos livros: Informática FCC - Questões comentadas e organizadas por assunto, 3ª. edição e 1001 questões comentadas de informática (Cespe/UnB), 2ª. edição, pela Editora Gen/Método. Foi aprovada nos seguintes concursos: Analista Legislativo, na especialidade de Administração de Rede, na Assembleia Legislativa do Estado de MG; Professora titular do Departamento de Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia; Professora substituta do DCC da UFJF; Analista de TI/Suporte, PRODABEL; Analista do Ministério Público MG; Analista de Sistemas, DATAPREV, Segurança da Informação; Analista de Sistemas, INFRAERO; Analista - TIC, PRODEMGE; Analista de Sistemas, Prefeitura de Juiz de Fora; Analista de Sistemas, SERPRO; Analista Judiciário (Informática), TRF 2ª Região RJ/ES, etc.

GRAN CONCURSOS

SUMÁRIO

APRESENTAÇÃO

Olá, querido(a) amigo(a)! É um prazer revê-lo(a).

A norma ISO/IEC 27001, referência na área da **gestão da segurança da informação**, teve nova publicação em 23 de novembro de 2022, passando a ser intitulada **ABNT NBR ISO/IEC 27001:2022 Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos.**


Terceira edição
23.11.2022

Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

A **Norma ABNT NBR ISO/IEC 27001:2022** é uma das normas da família ISO/IEC 27000, as quais tratam de **Sistema de Gestão da Segurança da Informação (SGSI).** Ela cancela e substitui a ABNT NBR ISO/IEC 27001:2013, a qual foi tecnicamente revisada.

Nesta aula veremos uma série de questões relacionadas à norma, com destaque para os conceitos mais cobrados nos últimos certames.

Desde 2006 faço parte da Comissão de Estudo de Técnicas de Segurança (CE-21:027.00), responsável pela criação das normas de segurança no âmbito brasileiro, sob a coordenação da ABNT.

Resumidamente, cabe destacar que toda norma ao ser criada/traduzida passa por uma série de revisões junto ao comitê, em seguida é encaminhada para consulta pública e só então a versão oficial homologada é publicada e vendida diretamente pela ABNT.

Que Deus o(a)s abençoe, e vamos ao que interessa ☺!

Um abraço,

Profª. Patrícia Quintão

Instagram: @patricialquintao

GESTÃO DE SEGURANÇA DA INFORMAÇÃO: NORMA NBR ISO/IEC N. 27.001:2022

1. SEÇÕES (ESTRUTURA) DA NORMA ABNT NBR ISO/IEC 27001:2022

A Norma **ABNT NBR ISO/IEC 27001:2022** é dividida em **11 seções e Anexo A.** As seções de 0 a 3 são introdutórias (e não são obrigatórias para a implementação), enquanto **as seções de 4 a 10 são** obrigatórias – significando que TODOS os seus **requisitos** devem ser implementados em uma organização se ela quer estar em conformidade com a norma.

Figura. Seções da Norma ABNT NBR ISO/IEC 27001:2022.

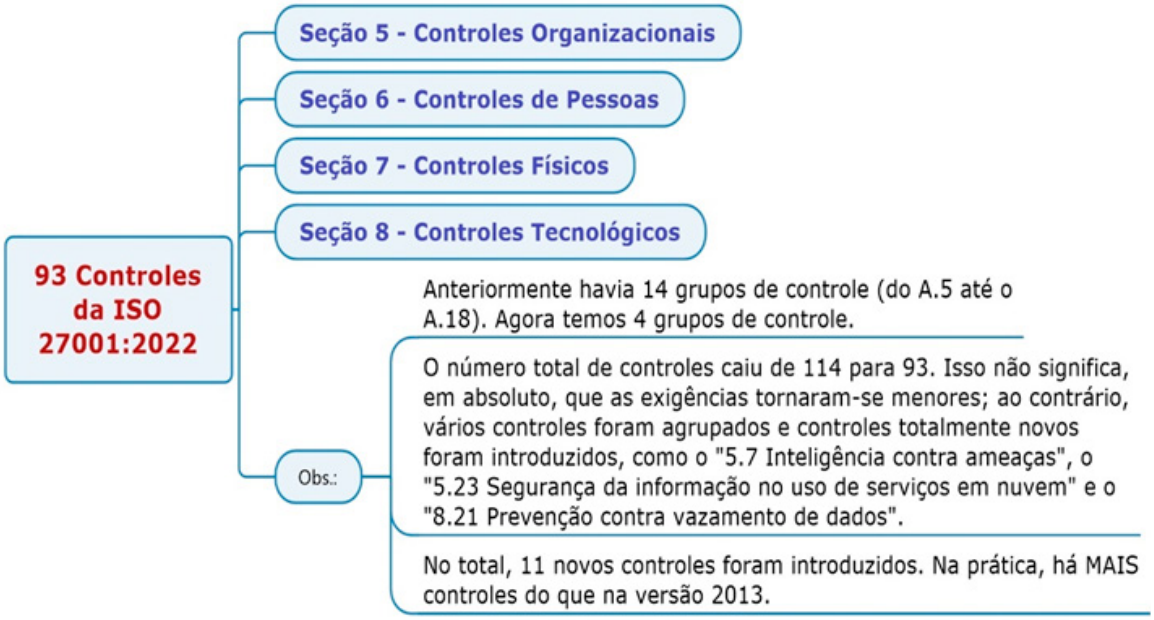
Fonte: Quintão (2023)

Seção 0: Introdução	Destaca o propósito da ISO 27001 e sua compatibilidade com outras normas de gestão.
Seção 1: Escopo	Explica que **a norma é aplicável a qualquer tipo de organização**.
Seção 2: Referência normativa Seção 3: Termos e definições	Refere-se à ISO/IEC 27000 como uma norma em que referências normativas, termos e definições são dadas.
Seção 4: Contexto da organização	Descreve **o contexto da organização,** incluindo o ambiente interno e externo, as necessidades e expectativas das partes interessadas e os objetivos de segurança da informação
Seção 5: Liderança	Descreve os **requisitos de liderança para o SGSI,** incluindo a política de segurança da informação, a atribuição de papéis e responsabilidades.
Seção 6: Planejamento	Descreve os requisitos de **planejamento para o SGSI,** incluindo o risco de segurança da informação, o tratamento de riscos e os objetivos de segurança da informação e planejamento para alcançá-los.
Seção 7: Apoio	Descreve os **requisitos de apoio para o SGSI,** incluindo recursos, competência das pessoas, conscientização, comunicação e informação documentada.
Seção 8: Operação	Descreve os **requisitos de operação para o SGSI,** incluindo atividades de planejamento e controle operacionais, avaliação/ tratamento dos riscos de segurança da informação.
Seção 9: Avaliação do desempenho	Define **requisitos para o monitoramento, medição, análise/ avaliação, auditoria interna e análise crítica** pela Direção.
Seção 10: Melhoria	Descreve os **requisitos de melhoria para o SGSI,** incluindo a melhoria contínua e requisitos para não conformidades e ações corretivas.

O Anexo A da **norma ABNT ISO/IEC 27001:2022** lista **93 controles de segurança da informação** que podem ser usados para implementar um sistema de gestão de segurança da informação (SGSI).

Os controles são organizados em quatro domínios**:**

- Controles **organizacionais** (37 controles)
- Controles de **pessoas** (8 controles)
- Controles **físicos** (14 controles)
- Controles **tecnológicos** (34 controles)



Os controles do Anexo A não são obrigatórios, mas são uma boa prática para organizações que desejam implementar um SGSI eficaz. O grau de implementação de cada controle deve ser determinado pela organização, levando em consideração seus riscos e necessidades específicos.

O Anexo A é uma ferramenta valiosa para organizações que desejam entender os controles de segurança da informação disponíveis e como eles podem ser usados para implementar um SGSI eficaz.

DIRETO DO CONCURSO

001. (CESPE/TJ-PA/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS (DESENVOLVIMENTO)/2020/ADAPTADA) Conforme a NBR ISO/IEC 27001 [versão 2022], implementar e operar um sistema de gestão de segurança da informação (SGSI) no processo PDCA envolve o requisito

a) definir a abordagem de como será realizada a análise e avaliação dos riscos na organização.

b) realizar a medição da eficácia dos controles estabelecidos no SGSI para verificar se estão atendidos.

c) integrar os stakeholders na comunicação das ações de melhoria.

d) elaborar o plano de tratamento dos riscos, identificando-se as ações de gestão apropriadas, os recursos a serem utilizados e as responsabilidades para a gestão dos riscos em segurança da informação.

e) obter autorização da direção da organização para a implementação e operação do SGSI.

Conforme visto, a seção 8, intitulada **Operação**, **parte da etapa execução (Do) do ciclo PDCA** e **define a** implementação da avaliação e tratamento de risco, **assim como controles e outros processos necessários para atingir os objetivos de segurança da informação.**

8 Operação

...

8.3 Tratamento de riscos de segurança da informação

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

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

Letra d.

1.1. ESCOPO

- A **Norma NBR ISO/IEC 27001:2022** especifica os **requisitos para estabelecer, implementar, manter e melhorar continuamente (EIMM) um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto da organização.**

> **DICA**
> Lembre-se do famoso "**EIMM**" para as 4 etapas, que são:
> **1 – E: Estabelecer**
> **2 – I: Implementar**
> **3 – M: Manter**
> **4 – M: Melhorar**

- **Também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.**
- Os requisitos definidos são **genéricos** e é pretendido que sejam **aplicáveis a TODAS as organizações, independentemente de tipo, tamanho e natureza.**
- **A exclusão de quaisquer dos requisitos especificados nas Seções 4 a 10 não é aceitável quando a organização busca a conformidade com esta Norma.**

QUESTÃO INÉDITA

002. (INÉDITA/2023) A norma ISO/IEC 27001:2022 trata

a) da gestão de riscos em sistemas de gestão da segurança da informação.
b) de requisitos de sistema de gestão da segurança da informação, métricas e medidas, e diretrizes para implementação.
c) de requisitos para auditoria e certificação de um sistema de gestão da segurança da informação.
d) das recomendações de controles para segurança da informação da antiga ISO/IEC 17799.
e) de requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

Vide a seguir os comentários extraídos da pág. 1 da norma ISO/IEC 27001:2022: "**esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente (EIMM) um Sistema de Gestão de Segurança da Informação (SGSI)** dentro do contexto da organização. **Também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. Letra e.**

1.2. REFERÊNCIAS NORMATIVAS

O documento **ISO/IEC 27000**, Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary é **indispensável à aplicação deste da Norma.**

A norma ISO/IEC 27000 apresenta uma **introdução geral de um sistema de gestão de segurança da informação** e da **família de normas** da série ISO/IEC 27000.

A ISO/IEC 27000 fornece um **glossário**, contendo definições da maioria dos termos usados em toda a família de normas da série ISO/IEC 27000, e descreve o escopo e objetivos para cada membro da família.

1.3. TERMOS E DEFINIÇÕES

Aplicam-se a esta Norma os termos e definições da **ISO/IEC 27000**. Alguns exemplos:

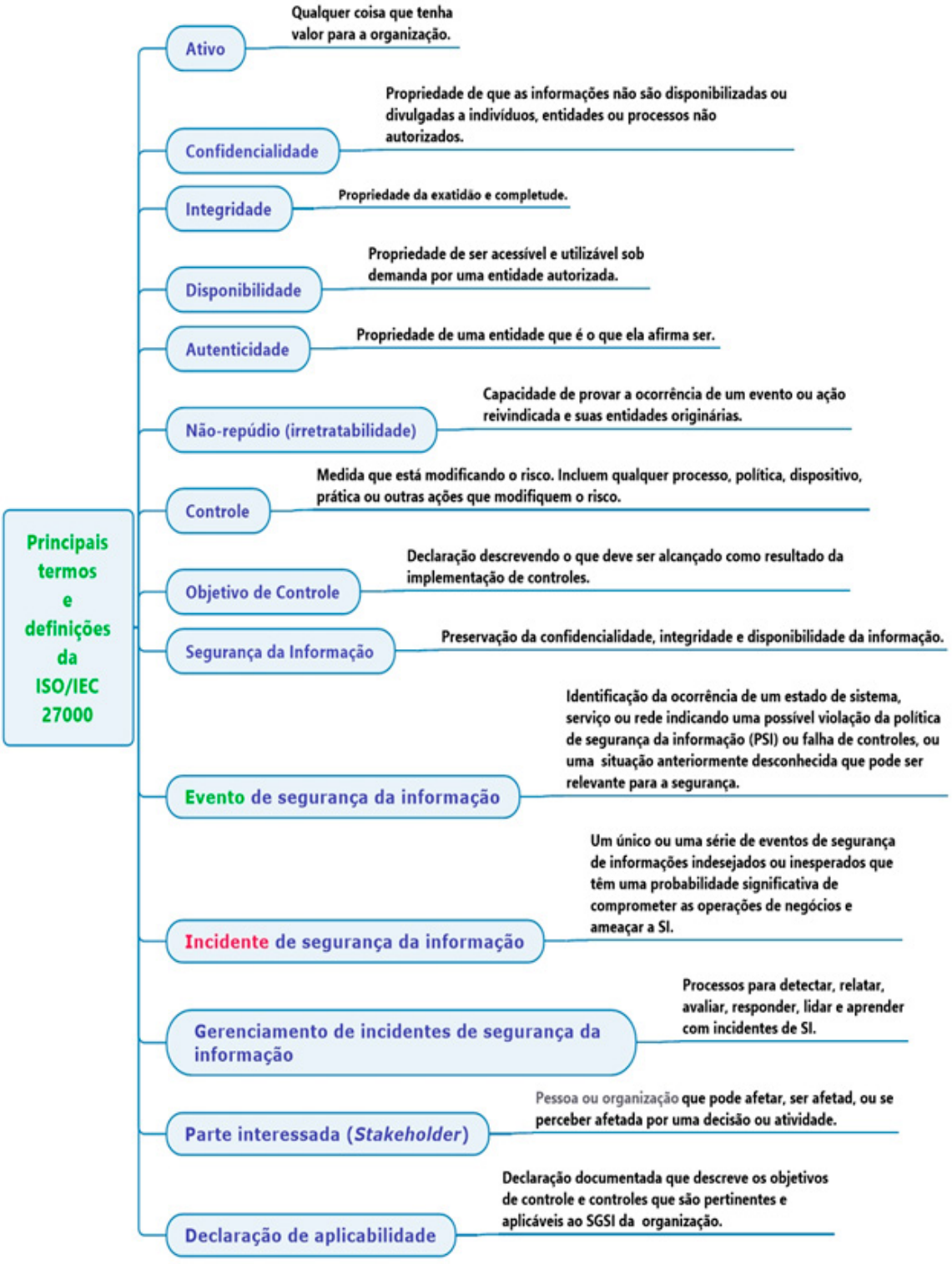


Figura. Termos e definições (Parte I).

Fonte: Quintão (2023)

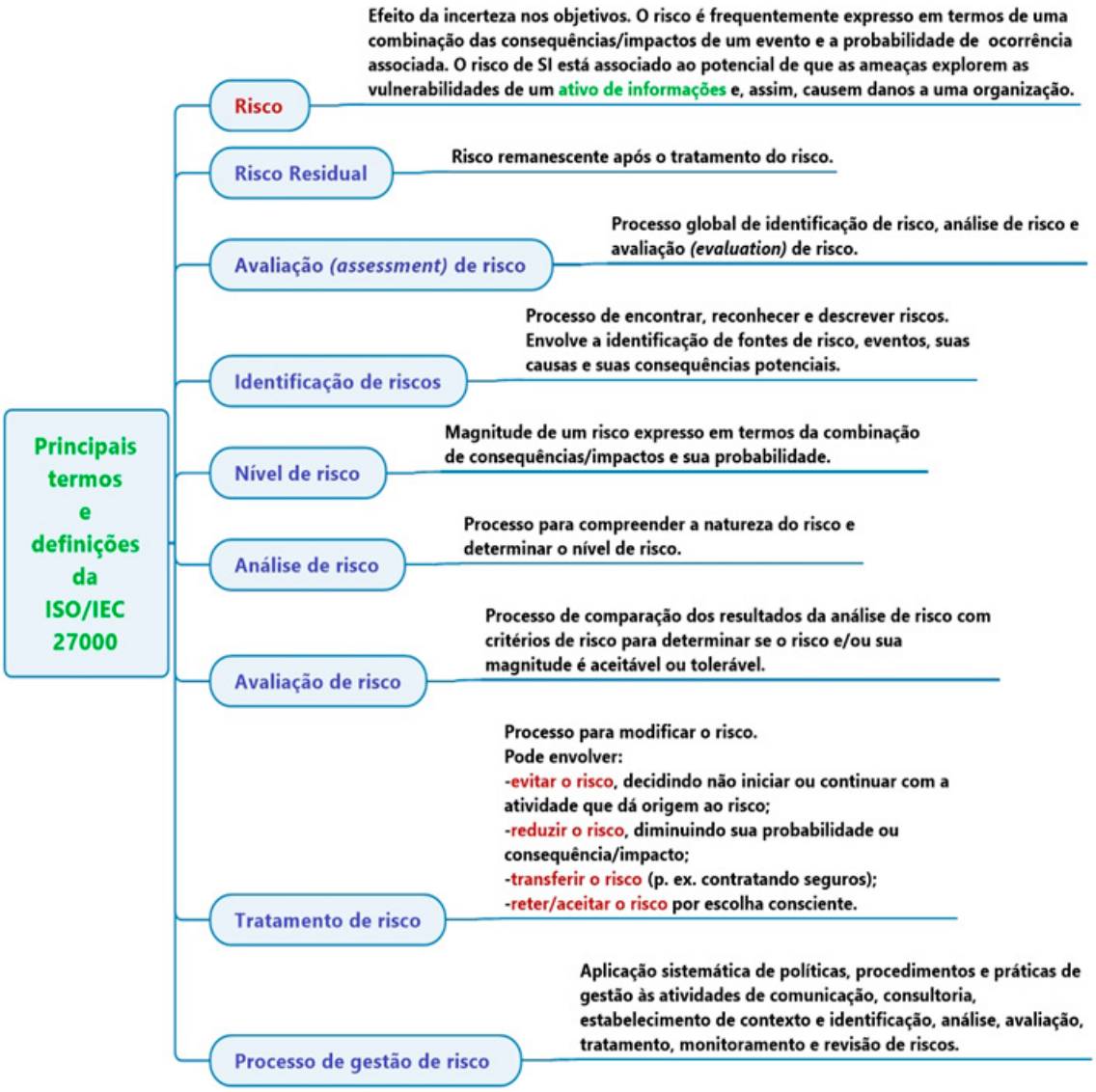


Figura. Termos e definições (Parte II).

Fonte: Quintão (2023)

1.4. CONTEXTO DA ORGANIZAÇÃO

- A organização deve **determinar as questões internas e externas relevantes para o seu propósito** e que afetam a sua capacidade para o alcance dos resultados pretendidos do seu **SGSI**.
- A organização deve determinar:
  - **partes interessadas** relevantes para o **SGSI;**
  - **requisitos relevantes dessas partes interessadas**;
  - **quais desses requisitos serão endereçados pelo SGSI**.

- A organização deve determinar os **limites** e a **aplicabilidade** do sistema de gestão da segurança da informação para estabelecer o seu escopo.

Ao determinar este escopo, a organização deve considerar:

a)as questões internas e externas referenciadas em 4.1;

b)os requisitos referenciados em 4.2;

c)as interfaces e dependências entre as atividades desempenhadas pela organização e aquelas que são desempenhadas por outras organizações.

- O escopo deve estar disponível como informação documentada.
- A organização deve estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação, incluindo os processos necessários e suas interações, de acordo com os requisitos deste documento.

1.5. LIDERANÇA

- **A Alta Direção deve:**

1. demonstrar sua liderança e comprometimento em relação ao SGSI, por meio dos seguintes **meios:**

a) assegurando que a **política de segurança da informação** e os **objetivos de segurança da informação** estão estabelecidos e são compatíveis com a direção estratégica da organização;

b) garantindo a **integração dos requisitos** do sistema de gestão da segurança da informação nos processos da organização;

c) assegurando que os **recursos necessários** para o sistema de gestão da segurança da informação estejam **disponíveis**;

d) **comunicando** a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação;

e) **assegurando que o sistema de gestão da segurança da informação alcance seus resultados** pretendidos;

f) **orientando e apoiando pessoas que contribuam para eficácia do sistema de gestão da segurança da informação**;

g) promovendo a **melhoria contínua**; e

h) **apoiando outros papéis relevantes da gestão** para demostrar como sua liderança se aplica às áreas sob sua responsabilidade.

2. Estabelecer uma política de segurança da informação (PSI).

A **PSI** deve estar disponível como informação documentada, ser comunicada dentro da organização e estar disponível para as partes interessadas;

3. Assegurar que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídos e comunicados.

A **Alta Direção** deve atribuir a responsabilidade e autoridade para:

a) assegurar que o SGSI está em conformidade com os requisitos desta Norma;

b) relatar sobre o desempenho SGSI para a Alta Direção.

DIRETO DO CONCURSO

003. (CESPE/TCE-RO/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/DESENVOLVIMENTO DE SISTEMAS/2019) De acordo com a NBR ISO/IEC n. 27001:2022, a alta direção de uma organização deve demonstrar liderança e comprometimento em relação ao sistema de gestão da segurança da informação. Para isso, ela deve

I – assegurar que a política de segurança da informação seja compatível com a direção estratégica da organização.

II – comunicar a importância da conformidade com os requisitos do sistema de gestão da segurança da informação.

III – analisar criticamente os códigos quanto ao uso de técnicas de programação segura.

IV – orientar pessoas que contribuam para a eficácia do sistema de gestão da segurança da informação.

Estão certos apenas os itens

a) I e II.

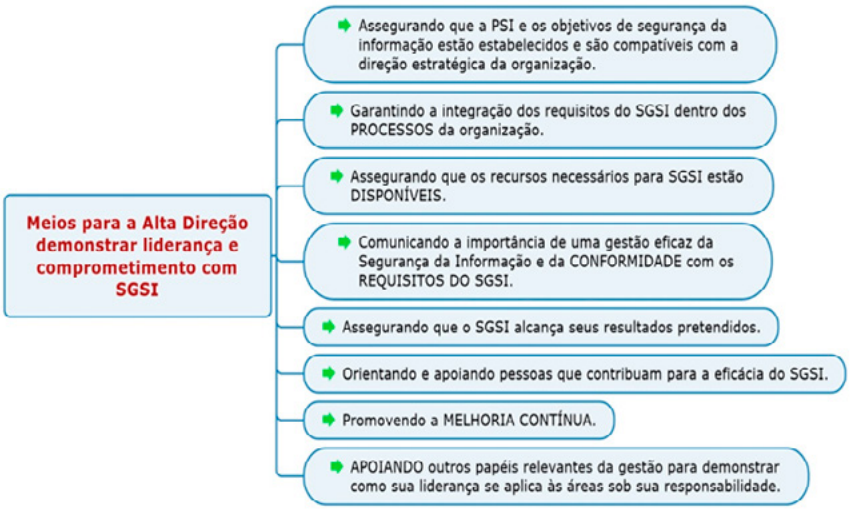
b) I e III.

c) III e IV.

d) I, II e IV.

e) II, III e IV.

Vamos aos comentários das assertivas:



I – Certa. A Seção 5.1 da norma ISO/IEC 27001:2022 destaca que "a Alta Direção deve demonstrar sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação assegurando que **a política de segurança da informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da organização"**.

II – Certa. A Seção 5.1 da norma ISO/IEC 27001:2022 destaca que "a Alta Direção deve comunicar a importância de uma gestão eficaz da segurança da informação e **da conformidade com os requisitos do sistema de gestão da segurança da informação"**.

III – Errada. Analisar criticamente os códigos quanto ao uso de técnicas de programação segura não é papel da Alta Direção.

IV – Certa. A Seção 5.1 da norma ISO/IEC 27001:2022 destaca que a Alta Direção deve orientar e apoiar pessoas que contribuam para eficácia do sistema de gestão da segurança da informação.

Conforme visto, as assertivas I, II e IV estão corretas.

Letra d.

1.6. PLANEJAMENTO

1.6.1 AÇÕES PARA ABORDAR RISCOS E OPORTUNIDADES

- No **planejamento** do **SGSI**, a **organização deve determinar** os **riscos e oportunidades** que precisam ser abordados **para assegurar que o SGSI pode alcançar seus resultados pretendidos, prevenir ou reduzir os efeitos indesejados e alcançar a melhoria contínua**.
- A **organização deve planejar as ações** para abordar estes riscos e oportunidades; e como **integrar** e **implementar** as **ações dentro dos processos** do seu **SGSI**, além de como **avaliar a eficácia destas ações**.
- A **organização deve estabelecer** e aplicar um **processo de avaliação de riscos de SI** que:

a) estabeleça e mantenha os critérios de aceitação do risco e critérios para realizar as avaliações dos riscos de SI;

b) assegure que as contínuas avaliações de riscos de SI produzam resultados comparáveis, válidos e consistentes;

c) identifique os riscos de SI;

d) analise os riscos de SI, avaliando suas consequências potenciais, a probabilidade realística de ocorrência e os níveis de risco;

e) avalie os riscos de SI, comparando os resultados da análise dos riscos com os critérios de riscos estabelecidos e priorizando os riscos analisados para o tratamento do risco.

- A **organização deve** reter **informação documentada** sobre o processo de avaliação de riscos da segurança da informação.
- A **organização** também **deve** estabelecer e aplicar um **processo de tratamento dos riscos** de SI, incluindo:

a) selecionar as **opções** apropriadas de **tratamento dos riscos** de SI;

b) **determinar** todos os **controles** necessários para **implementar** as **opções de tratamento** escolhidas;

c) **comparar os controles** determinados com aqueles do Anexo A, verificando possíveis omissões;

d) **elaborar** uma **Declaração de Aplicabilidade** que contenha: os controles necessários; a justificativa para inclusões; se os controles necessários são implementados ou não; e a justificativa para a exclusão de quaisquer controles do anexo A;

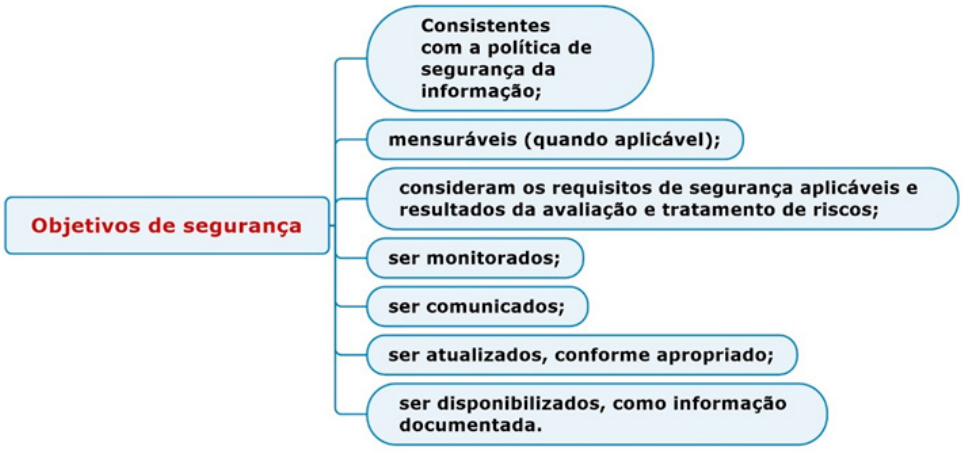
e) preparar um **plano para tratamento dos riscos** de SI;

f) obter a **aprovação** dos responsáveis pelos riscos do **plano** aqui destacado e a **aceitação** dos **riscos residuais** de SI.

- A **organização deve** reter a **informação documentada** relativa ao processo de tratamento de riscos de SI.

6.2 Objetivos da segurança da informação e planejamento para alcançá-los.

- A **organização deve** estabelecer os **objetivos de SI** para as funções e níveis relevantes.



Fonte: Quintão (2023)

- A organização deve reter **informação documentada** dos objetivos de SI.
- Quando do planejamento para alcançar os seus **objetivos de SI, a organização deve** determinar **O QUE será feito, QUAIS recursos serão necessários, QUEM será responsável, QUANDO estará concluído e COMO os resultados serão avaliados.**

- Quando a organização determinar as necessidades para as mudanças do sistema de gestão **da segurança da informação, estas mudanças devem ser conduzidas de uma forma planejada.**

1.7. APOIO

- A **organização deve**

a) determinar e prover **recursos** necessários para o **EIMM** do **SGSI**;

b) **determinar** a **competência** necessária das pessoas que realizam o trabalho sob o seu controle e que afeta o desempenho da SI;

c) **assegurar** que essas pessoas são **competentes,** com base na **educação**, **treinamento** ou **experiência** apropriados;

d) **onde aplicável, tomar ações** para **adquirir a competência** necessária, avaliando a eficácia das ações tomadas;

e) reter **informação documentada** como evidência da competência.

- **Pessoas que realizam o trabalho** sob controle da organização **devem estar cientes da PSI**, das suas **contribuições** para a **eficácia** e **desempenho** do **SGSI** e das **implicações da não conformidade** com os requisitos do **SGSI**.
- A **organização deve determinar** as **comunicações** internas e externas **relevantes para o SGSI** incluindo **O QUE, QUANDO, QUEM será comunicado**, e **COMO se comunicar**.
- O **SGSI deve incluir** **informação documentada** **requerida por esta norma e pela organização.**

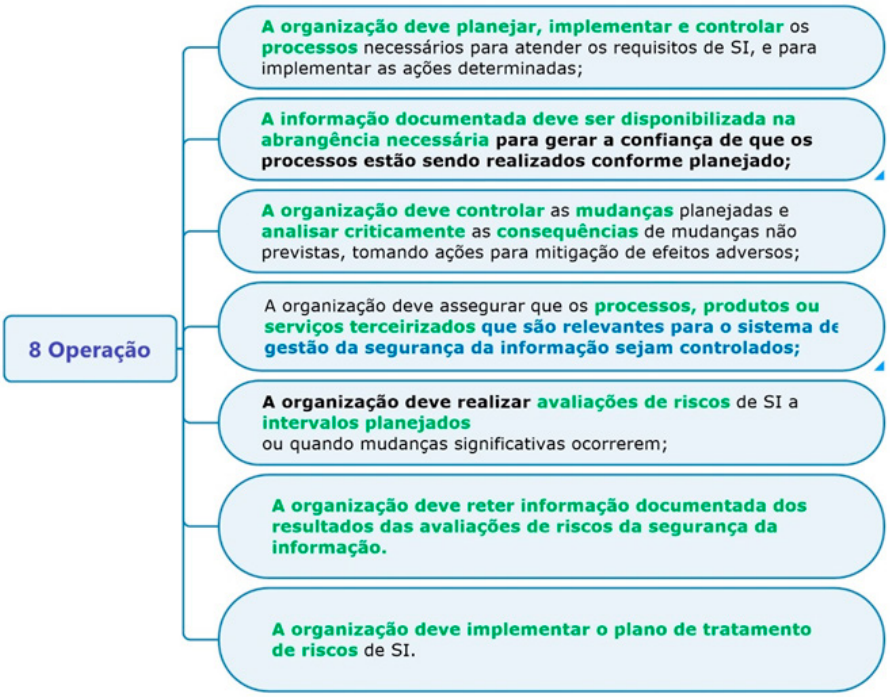
> A **abrangência da** **informação documentada para o** **SGSI** pode variar, de acordo com: **tamanho** da organização **e seu tipo de atividades, processos, produtos e serviços; a complexidade dos processos e suas interações** e a **competência das pessoas**.

Nesse contexto, a organização deve assegurar de forma apropriada a **identificação, descrição, formato e seu meio** (por exemplo, papel, eletrônico), **análise crítica e aprovação para pertinência e adequação**.

Para esse controle, devem ser consideradas as atividades de: **distribuição**, **acesso**, **recuperação e uso**, **armazenagem** e **preservação**, incluindo a preservação da legibilidade, **controle de mudanças**, **retenção** e **disposição**.

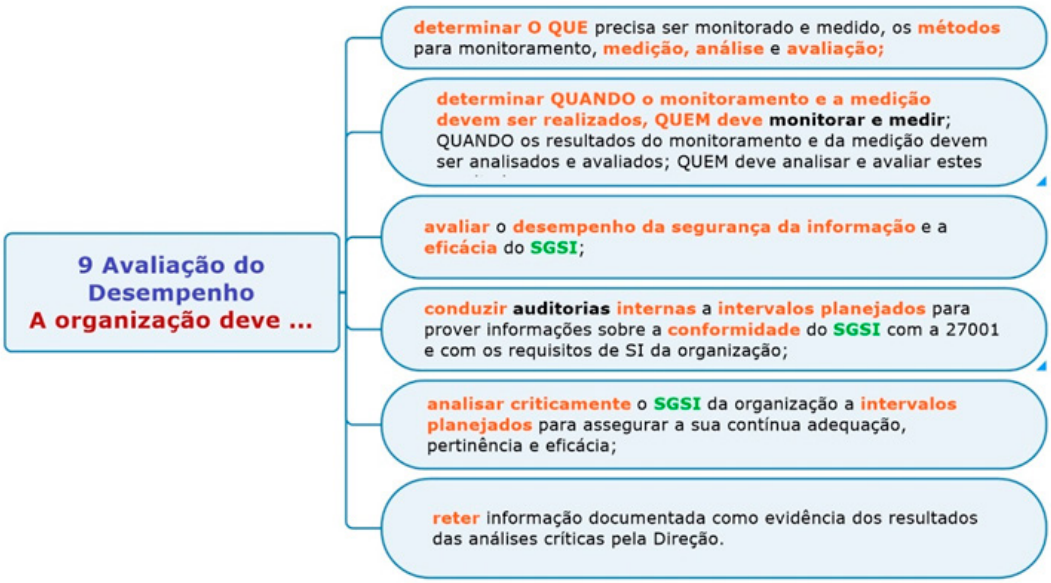
A **informação documentada** **de** origem externa **deve** **ser** **identificada** também **como apropriado, e controlada.**

1.8. OPERAÇÃO



- Os resultados do tratamento de riscos de SI devem ser retidos como informação documentada pela organização.

1.9. AVALIAÇÃO DO DESEMPENHO



1.10. MELHORIA

A **organização** deve **continuamente melhorar** a pertinência, adequação e eficácia do **SGSI**.

Ao detectar **não conformidades**, a **organização deve**:

- **reagir** e tomar ações para **controlar, corrigi-la e lidar com as consequências**;
- **avaliar** a necessidade de **ações** para **eliminar as causas**, para **evitar** que se repita ou ocorra;
- **implementar** quaisquer **ações** necessárias;
- **analisar criticamente** a eficácia das **ações corretivas** tomadas;
- realizar **mudanças** no **SGSI**, quando necessário.

A organização deve reter **informação documentada como evidência** da natureza das **não conformidades encontradas** e dos **resultados** de qualquer **ação** corretiva.

ANEXO A

Vejamos os 93 controles a seguir:

Tabela A.1 – Controles de Segurança da Informação

5	Controles organizacionais	
5.1	Políticas de segurança da informação	**Controle** A política de segurança da informação e as políticas específicas por tema devem ser definidas, **aprovadas pela direção**, **publicadas, comunicadas e reconhecidas pelo pessoal pertinente e pelas partes interessadas pertinentes,** e analisadas criticamente em intervalos planejados e quando ocorrerem mudanças significativas.
5.2	Papéis e responsabilidades pela segurança da informação	**Controle** Papéis e responsabilidades pela segurança da informação devem ser definidos e alocados de acordo com as necessidades da organização.
5.3	Segregação de funções	**Controle** Funções conflitantes e áreas de responsabilidade devem ser segregadas.
5.4	Responsabilidades da direção	**Controle** A direção deve requerer que todo o pessoal aplique a segurança da informação de acordo com a política da segurança da informação estabelecida, com as políticas específicas por tema e com os procedimentos da organização.
5.5	Contato com autoridades	**Controle** A organização deve estabelecer e manter contato com as autoridades relevantes.
5.6	Contato com grupos de interesse especial	**Controle** A organização deve estabelecer e manter contato com grupos de interesse especial ou com outros fóruns de especialistas em segurança e associações profissionais.
5.7	Inteligência de ameaças	**Controle** As informações relacionadas a ameaças à segurança da informação devem ser coletadas e analisadas para produzir inteligência de ameaças.
5.8	Segurança da informação no gerenciamento de projetos	**Controle** A segurança da informação deve ser integrada ao gerenciamento de projetos.

5.9	Inventário de informações e outros ativos associados	**Controle** Um inventário de informações e outros ativos associados, incluindo proprietários, deve ser desenvolvido e mantido.
5.10	Uso aceitável de informações e outros ativos associados	**Controle** Regras para o uso aceitável e procedimentos para o manuseio de informações e outros ativos associados devem ser identificados, documentados e implementados.
5.11	Devolução de ativos	**Controle** O pessoal e outras partes interessadas, conforme apropriado, devem devolver todos os ativos da organização em sua posse após a mudança ou o encerramento da contratação ou acordo.
5.12	Classificação das informações	**Controle** As informações devem ser classificadas de acordo com as necessidades de segurança da informação da organização, com base na confidencialidade, integridade, disponibilidade e requisitos das partes interessadas relevantes.
5.13	Rotulagem de informações	**Controle** Um conjunto adequado de procedimentos para rotulagem de informações deve ser desenvolvido e implementado de acordo com o esquema de classificação de informações adotado pela organização.
5.14	Transferência de informações	**Controle** Regras, procedimentos ou acordos de transferência de informações devem ser implementados para todos os tipos de recursos de transferência dentro da organização e entre a organização e outras partes.
5.15	Controle de acesso	**Controle** Regras para controlar o acesso físico e lógico às informações e a outros ativos associados devem ser estabelecidas e implementadas com base nos requisitos de segurança da informação e de negócios.
5.16	Gestão de identidade	**Controle** O ciclo de vida completo das identidades deve ser gerenciado.
5.17	Informações de autenticação	**Controle** A alocação e a gestão de informações de autenticação devem ser controladas por uma gestão de processo, incluindo aconselhar o pessoal sobre o manuseio adequado de informações de autenticação.

5.18	Direitos de acesso	**Controle** Os direitos de acesso às informações e a outros ativos associados devem ser provisionados, analisados criticamente, modificados e removidos de acordo com a política de tema específico e com as regras da organização para o controle de acesso.
5.19	Segurança da informação nas relações com fornecedores	**Controle** Processos e procedimentos devem ser definidos e implementados para gerenciar a segurança da informação e os riscos associados com o uso dos produtos ou serviços dos fornecedores.
5.20	Abordagem da segurança da informação nos contratos de fornecedores	**Controle** Requisitos relevantes de segurança da informação devem ser estabelecidos e acordados com cada fornecedor, com base no tipo de relacionamento com o fornecedor.
5.21	Gestão da segurança da informação na cadeia de fornecimento de TIC	**Controle** Processos e procedimentos devem ser definidos e implementados para gerenciar os riscos da segurança da informação associados à cadeia de fornecimento de produtos e serviços de TIC.
5.22	Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores	**Controle** A organização deve monitorar, analisar criticamente, avaliar e gerenciar regularmente a mudança nas práticas da segurança da informação dos fornecedores e na prestação de serviços.
5.23	Segurança da informação para uso de serviços em nuvem	**Controle** Os processos de aquisição, uso, gestão e saída de serviços em nuvem devem ser estabelecidos de acordo com os requisitos da segurança da informação da organização.
5.24	Planejamento e preparação da gestão de incidentes da segurança da informação	**Controle** A organização deve planejar e se preparar para gerenciar incidentes da segurança da informação, definindo, estabelecendo e comunicando processos, papéis e responsabilidades de gestão de incidentes da segurança da informação.
5.25	Avaliação e decisão sobre eventos da segurança da informação	**Controle** A organização deve avaliar os eventos da segurança da informação e decidir se categoriza como incidentes da segurança da informação.

5.26	Resposta a incidentes da segurança da informação	**Controle** Os incidentes da segurança da informação devem ser respondidos de acordo com os procedimentos documentados.
5.27	Aprendizado com incidentes de segurança da informação	**Controle** O conhecimento adquirido com incidentes de segurança da informação deve ser usado para fortalecer e melhorar os controles da segurança da informação.
5.28	Coleta de evidências	**Controle** A organização deve estabelecer e implementar procedimentos para identificação, coleta, aquisição e preservação de evidências relacionadas a eventos da segurança da informação.
5.29	Segurança da informação durante a disrupção	**Controle** A organização deve planejar como manter a segurança da informação em um nível apropriado durante a disrupção.
5.30	Prontidão de TIC para continuidade de negócios	**Controle** A prontidão de TIC deve ser planejada, implementada, mantida e testada com base nos objetivos de continuidade de negócios e nos requisitos de continuidade da TIC.
5.31	Requisitos legais, estatutários, regulamentares e contratuais	**Controle** Os requisitos legais, estatutários, regulamentares e contratuais pertinentes à segurança da informação e à abordagem da organização para atender a esses requisitos devem ser identificados, documentados e atualizados.
5.32	Direitos de propriedade intelectual	**Controle** A organização deve implementar procedimentos adequados para proteger os direitos de propriedade intelectual.

5.33	Proteção de registros	**Controle** Os registros devem ser protegidos contra perdas, destruição, falsificação, acesso não autorizado e liberação não autorizada.
5.34	Privacidade e proteção de DP	**Controle** A organização deve identificar e atender aos requisitos relativos à preservação da privacidade e à proteção de DP, de acordo com as leis e os regulamentos aplicáveis e requisitos contratuais.
5.35	Análise crítica independente da segurança da informação	**Controle** A abordagem da organização para gerenciar a segurança da informação e sua implementação, incluindo pessoas, processos e tecnologias, deve ser analisada criticamente, de forma independente, a intervalos planejados ou quando ocorrerem mudanças significativas.
5.36	*Compliance* com políticas, regras e normas para segurança da informação	**Controle** O *compliance* da política de segurança da informação da organização, políticas, regras e normas de temas específicos deve ser analisado criticamente a intervalos regulares.
5.37	Documentação dos procedimentos de operação	**Controle** Os procedimentos de operação dos recursos de tratamento da informação devem ser documentados e disponibilizados para o pessoal que necessite deles.

6	**Controles de pessoas**	
6.1	Seleção	**Controle** Verificações de antecedentes de todos os candidatos a serem contratados devem ser realizadas antes de ingressarem na organização e de modo contínuo, de acordo com as leis, os regulamentos e a ética aplicáveis, e devem ser proporcionais aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.

6.2	Termos e condições de contratação	**Controle** Os contratos trabalhistas devem declarar as responsabilidades do pessoal e da organização para a segurança da informação.
6.3	Conscientização, educação e treinamento em segurança da informação	**Controle** O pessoal da organização e partes interessadas relevantes devem receber treinamento, educação e conscientização em segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas e procedimentos específicas por tema, pertinentes para as suas funções.
6.4	Processo disciplinar	**Controle** Um processo disciplinar deve ser formalizado e comunicado, para tomar ações contra pessoal e outras partes interessadas relevantes que tenham cometido uma violação da política da segurança da informação.
6.5	Responsabilidades após encerramento ou mudança da contratação	**Controle** As responsabilidades e funções de segurança da informação que permaneçam válidas após o encerramento ou a mudança da contratação devem ser definidas, aplicadas e comunicadas ao pessoal e a outras partes interessadas pertinentes.
6.6	Acordos de confidencialidade ou não divulgação	**Controle** Acordos de confidencialidade ou não divulgação que reflitam as necessidades da organização para a proteção das informações devem ser identificados, documentados, analisados criticamente em intervalos regulares e assinados pelo pessoal e por outras partes interessadas pertinentes.
6.7	Trabalho remoto	**Controle** Medidas de segurança devem ser implementadas quando as pessoas estiverem trabalhando remotamente para proteger as informações acessadas, tratadas ou armazenadas fora das instalações da organização.
6.8	Relato de eventos de segurança da informação	**Controle** A organização deve fornecer um mecanismo para que as pessoas relatem eventos da segurança da informação observados ou suspeitos por meio de canais apropriados em tempo hábil.

7	**Controles físicos**	
7.1	Perímetros de segurança física	**Controle** Perímetros de segurança devem ser definidos e usados para proteger áreas que contenham informações e outros ativos associados.
7.2	Entrada física	**Controle** As áreas seguras devem ser protegidas por controles de entrada e pontos de acesso apropriados.
7.3	Segurança de escritórios, salas e instalações	**Controle** Segurança física para escritórios, salas e instalações deve ser projetada e implementada
7.4	Monitoramento de segurança física	**Controle** As instalações devem ser monitoradas continuamente para acesso físico não autorizado
7.5	Proteção contra ameaças físicas e ambientais	**Controle** Proteção contra ameaças físicas e ambientais, como desastres naturais e outras ameaças físicas intencionais ou não intencionais à infraestrutura, deve ser projetada e implementada.
7.6	Trabalho em áreas seguras	**Controle** Medidas de segurança para trabalhar em áreas seguras devem ser projetadas e implementadas.
7.7	Mesa limpa e tela limpa	**Controle** Regras de mesa limpa para documentos impressos e mídia de armazenamento removível e regras de tela limpa para os recursos de tratamento das informações devem ser definidas e adequadamente aplicadas.
7.8	Localização e proteção de equipamentos	**Controle** Os equipamentos devem ser posicionados com segurança e proteção.
7.9	Segurança de ativos fora das instalações da organização	**Controle** Os ativos fora das instalações da organização devem ser protegidos.
7.10	Mídia de armazenamento	**Controle** As mídias de armazenamento devem ser gerenciadas por seu ciclo de vida de aquisição, uso, transporte e descarte, de acordo com o esquema de classificação e com os requisitos de manuseio da organização.

7.11	Serviços de infraestrutura	**Controle** As instalações de tratamento de informações devem ser protegidas contra falhas de energia e outras disrupções causadas por falhas nos serviços de infraestrutura.
7.12	Segurança do cabeamento	**Controle** Os cabos que transportam energia ou dados, ou que sustentam serviços de informação, devem ser protegidos contra interceptação, interferência ou danos.
7.13	Manutenção de equipamentos	**Controle** Os equipamentos devem ser mantidos corretamente para assegurar a disponibilidade, integridade e confidencialidade da informação.
7.14	Descarte seguro ou reutilização de equipamentos	**Controle** Os itens dos equipamentos que contenham mídia de armazenamento devem ser verificados para assegurar que quaisquer dados confidenciais e *software* licenciado tenham sido removidos ou substituídos com segurança antes do descarte ou reutilização.
8	**Controles tecnológicos**	
8.1	Dispositivos *endpoint* do usuário	**Controle** As informações armazenadas, tratadas ou acessíveis por meio de dispositivos *endpoint* do usuário devem ser protegidas.
8.2	Direitos de acessos privilegiados	**Controle** A atribuição e o uso de direitos de acessos privilegiados devem ser restritos e gerenciados
8.3	Restrição de acesso à informação	**Controle** O acesso às informações e a outros ativos associados deve ser restrito de acordo com a política específica por tema sobre controle de acesso.
8.4	Acesso ao código-fonte	**Controle** Os acessos de leitura e escrita ao código-fonte, ferramentas de desenvolvimento e bibliotecas de *software* devem ser adequadamente gerenciados.
8.5	Autenticação segura	**Controle** Tecnologias e procedimentos de autenticação seguros devem ser implementados, com base em restrições de acesso à informação e à política específica por tema de controle de acesso.

8.6	Gestão de capacidade	**Controle** O uso dos recursos deve ser monitorado e ajustado de acordo com os requisitos atuais e esperados de capacidade.
8.7	Proteção contra *malware*	**Controle** Proteção contra *malware* deve ser implementada e apoiada pela conscientização adequada do usuário.
8.8.	Gestão de vulnerabilidades técnicas	**Controle** Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas; a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas
8.9	Gestão de configuração	**Controle** As configurações, incluindo configurações de segurança, de *hardware*, *software*, serviços e redes, devem ser estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente.
8.10	Exclusão de informações	**Controle** As informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento devem ser excluídas quando não forem mais necessárias.
8.11	Mascaramento de dados	**Controle** O mascaramento de dados deve ser usado de acordo com a política específica por tema da organização sobre o controle de acesso e outros requisitos específicos por tema relacionados e requisitos de negócios, levando em consideração a legislação aplicável.
8.12	Prevenção de vazamento de dados	**Controle** As medidas de prevenção de vazamento de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.
8.13	*Backup* das informações	**Controle** Cópias de *backup* de informações, *software* e sistemas devem ser mantidas e testadas regularmente de acordo com a política específica por tema acordada sobre *backup*.
8.14	Redundância dos recursos de tratamento de informações	**Controle** Os recursos de tratamento de informações devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade.

8.15	*Log*	**Controle** *Logs* que registrem atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados.
8.16	Atividades de monitoramento	**Controle** As redes, sistemas e aplicações devem ser monitorados por comportamentos anômalos e por ações apropriadas, tomadas para avaliar possíveis incidentes de segurança da informação.
8.17	Sincronização do relógio	**Controle** Os relógios dos sistemas de tratamento de informações utilizados pela organização devem ser sincronizados com fontes de tempo aprovadas.
8.18	Uso de programas utilitários privilegiados	**Controle** O uso de programas utilitários que possam ser capazes de substituir os controles de sistema e as aplicações deve ser restrito e rigorosamente controlado.
8.19	Instalação de *software* em sistemas operacionais	**Controle** Procedimentos e medidas devem ser implementados para gerenciar com segurança a instalação de *software* em sistemas operacionais.
8.20	Segurança de redes	**Controle** Redes e dispositivos de rede devem ser protegidos, gerenciados e controlados para proteger as informações em sistemas e aplicações.
8.21	Segurança dos serviços de rede	**Controle** Mecanismos de segurança, níveis de serviço e requisitos de serviços de rede devem ser identificados, implementados e monitorados.
8.22	Segregação de redes	**Controle** Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados nas redes da organização.
8.23	Filtragem da *web*	**Controle** O acesso a *sites* externos deve ser gerenciado para reduzir a exposição a conteúdo malicioso.
8.24	Uso de criptografia	**Controle** Regras para o uso efetivo da criptografia, incluindo o gerenciamento de chaves criptográfica devem ser definidas e implementadas.

8.25	Ciclo de vida de desenvolvimento seguro	**Controle** Regras para o desenvolvimento seguro de *software* e sistemas devem ser estabelecidas e aplicadas.
8.26	Requisitos de segurança da aplicação	**Controle** Requisitos de segurança da informação devem ser identificados, especificados e aprovados ao desenvolver ou adquirir aplicações.
8.27	Princípios de arquitetura e engenharia de sistemas seguros	**Controle** Princípios de engenharia de sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados a qualquer atividade de desenvolvimento de sistemas.
8.28	Codificação segura	**Controle** Princípios de codificação segura devem ser aplicados ao desenvolvimento de *software*.
8.29	Testes de segurança em desenvolvimento e aceitação	**Controle** Processos de teste de segurança devem ser definidos e implementados no ciclo de vida do desenvolvimento.
8.30	Desenvolvimento terceirizado	**Controle** A organização deve dirigir, monitorar e analisar criticamente as atividades relacionadas à terceirização de desenvolvimento de sistemas.
8.31	Separação dos ambientes de desenvolvimento, teste e produção	**Controle** Ambientes de desenvolvimento, testes e produção devem ser separados e protegidos.
8.32	Gestão de mudanças	**Controle** Mudanças nos recursos de tratamento de informações e sistemas de informação devem estar sujeitas a procedimentos de gestão de mudanças.
8.33	Informações de teste	**Controle** Informações de teste devem ser adequadamente selecionadas, protegidas e gerenciadas.
8.34	Proteção de sistemas de informação durante os testes de auditoria	**Controle** Testes de auditoria e outras atividades de garantia envolvendo a avaliação de sistemas operacionais devem ser planejados e acordados entre o testador e a gestão apropriada.

RESUMO

Figura. Dicas da Norma ABNT NBR ISO/IEC 27001:2022.

Fonte: Quintão (2023)

Controles da Norma

5	**Controles Organizacionais**
5.1	Políticas de segurança da informação
5.2	Papéis e responsabilidades pela segurança da informação
5.3	Segregação de funções
5.4	Responsabilidades da direção
5.5	Contato com autoridades
5.6	Contato com grupos de interesse especial
5.7	Inteligência de ameaças
5.8	Segurança da informação no gerenciamento de projetos
5.9	Inventário de informações e outros ativos associados
5.10	Uso aceitável de informações e outros ativos associados
5.11	Devolução de ativos
5.12	Classificação das informações
5.13	Rotulagem de informações
5.14	Transferência de informações
5.15	Controle de acesso
5.16	Gestão de identidade
5.17	Informações de autenticação
5.18	Direitos de acesso
5.19	Segurança da informação nas relações com fornecedores
5.20	Abordagem da segurança da informação nos contratos de fornecedores
5.21	Gestão da segurança da informação na cadeia de fornecimento de TIC
5.22	Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores

5.23	Segurança da informação para uso de serviços em nuvem
5.24	Planejamento e preparação da gestão de incidentes da segurança da informação
5.25	Avaliação e decisão sobre eventos da segurança da informação
5.26	Resposta a incidentes da segurança da informação
5.27	Aprendizado com incidentes de segurança da informação
5.28	Coleta de evidências
5.29	Segurança da informação durante a disrupção
5.30	Prontidão de TIC para continuidade de negócios
5.31	Requisitos legais, estatutários, regulamentares e contratuais
5.32	Direitos de propriedade intelectual
5.33	Proteção de registros
5.34	Privacidade e proteção de DP
5.35	Análise crítica independente da segurança da informação
5.36	*Compliance* com políticas, regras e normas para segurança da informação
5.37	Documentação dos procedimentos de operação

6	**Controles de Pessoas**
6.1	Seleção
6.2	Termos e condições de contratação
6.3	Conscientização, educação e treinamento em segurança da informação

6.4	Processo disciplinar
6.5	Responsabilidades após encerramento ou mudança da contratação
6.6	Acordos de confidencialidade ou não divulgação
6.7	Trabalho remoto
6.8	Relato de eventos de segurança da informação

7	**Controles físicos**
7.1	Perímetros de segurança física
7.2	Entrada física
7.3	Segurança de escritórios, salas e instalações
7.4	Monitoramento de segurança física
7.5	Proteção contra ameaças físicas e ambientais
7.6	Trabalho em áreas seguras
7.7	Mesa limpa e tela limpa
7.8	Localização e proteção de equipamentos
7.9	Segurança de ativos fora das instalações da organização
7.10	Mídia de armazenamento
7.11	Serviços de infraestrutura
7.12	Segurança do cabeamento
7.13	Manutenção de equipamentos
7.14	Descarte seguro ou reutilização de equipamentos

8	**Controles tecnológicos**
8.1	Dispositivos *endpoint* do usuário
8.2	Direitos de acessos privilegiados
8.3	Restrição de acesso à informação
8.4	Acesso ao código-fonte
8.5	Autenticação segura
8.6	Gestão de capacidade

8.7	Proteção contra *malware*
8.8.	Gestão de vulnerabilidades técnicas
8.9	Gestão de configuração
8.10	Exclusão de informações
8.11	Mascaramento de dados
8.12	Prevenção de vazamento de dados
8.13	*Backup* das informações
8.14	Redundância dos recursos de tratamento de informações
8.15	*Log*
8.16	Atividades de monitoramento
8.17	Sincronização do relógio
8.18	Uso de programas utilitários privilegiados
8.19	Instalação de *software* em sistemas operacionais
8.20	Segurança de redes
8.21	Segurança dos serviços de rede
8.22	Segregação de redes
8.23	Filtragem da *web*
8.24	Uso de criptografia
8.25	Ciclo de vida de desenvolvimento seguro
8.26	Requisitos de segurança da aplicação
8.27	Princípios de arquitetura e engenharia de sistemas seguros
8.28	Codificação segura
8.29	Testes de segurança em desenvolvimento e aceitação
8.30	Desenvolvimento terceirizado
8.31	Separação dos ambientes de desenvolvimento, teste e produção
8.32	Gestão de mudanças
8.33	Informações de teste
8.34	Proteção de sistemas de informação durante os testes de auditoria

Figura. 93 Controles da ISO 27001.

Fonte: Elaboração própria (2023)

QUESTÕES COMENTADAS EM AULA

001. (CESPE/TJ-PA/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS (DESENVOLVIMENTO)/2020/ADAPTADA) Conforme a NBR ISO/IEC 27001 [versão 2022], implementar e operar um sistema de gestão de segurança da informação (SGSI) no processo PDCA envolve o requisito
a) definir a abordagem de como será realizada a análise e avaliação dos riscos na organização.
b) realizar a medição da eficácia dos controles estabelecidos no SGSI para verificar se estão atendidos.
c) integrar os stakeholders na comunicação das ações de melhoria.
d) elaborar o plano de tratamento dos riscos, identificando-se as ações de gestão apropriadas, os recursos a serem utilizados e as responsabilidades para a gestão dos riscos em segurança da informação.
e) obter autorização da direção da organização para a implementação e operação do SGSI.

002. (INÉDITA/2023) A norma ISO/IEC 27001:2022 trata
a) da gestão de riscos em sistemas de gestão da segurança da informação.
b) de requisitos de sistema de gestão da segurança da informação, métricas e medidas, e diretrizes para implementação.
c) de requisitos para auditoria e certificação de um sistema de gestão da segurança da informação.
d) das recomendações de controles para segurança da informação da antiga ISO/IEC 17799.
e) de requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

003. (CESPE/TCE-RO/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/DESENVOLVIMENTO DE SISTEMAS/2019) De acordo com a NBR ISO/IEC n. 27001:2022, a alta direção de uma organização deve demonstrar liderança e comprometimento em relação ao sistema de gestão da segurança da informação. Para isso, ela deve
I – assegurar que a política de segurança da informação seja compatível com a direção estratégica da organização.
II – comunicar a importância da conformidade com os requisitos do sistema de gestão da segurança da informação.
III – analisar criticamente os códigos quanto ao uso de técnicas de programação segura.
IV – orientar pessoas que contribuam para a eficácia do sistema de gestão da segurança da informação.

Estão certos apenas os itens

a) I e II.

b) I e III.

c) III e IV.

d) I, II e IV.

e) II, III e IV.

EXERCÍCIOS

004. (CESPE/TJ-AM/ANALISTA JUDICIÁRIO/ANALISTA DE SISTEMAS/2019/ADAPTADA) Julgue o próximo item, relativo à gestão de segurança da informação.
De acordo com a norma NBR ISO/IEC 27001 [de 2022], uma organização que vise estabelecer um sistema de gestão de segurança da informação (SGSI) deve entender o contexto interno e externo da organização em relação aos riscos e aplicar um processo de avaliação de riscos de segurança da informação e uma análise qualitativa e quantitativa.

005. (CESPE/TCE-RN/ASSESSOR TÉCNICO DE INFORMÁTICA/CONTROLE EXTERNO/2015/ADAPTADA) Julgue os itens a seguir, acerca de gestão de segurança da informação à luz das normas ISO/IEC 27001 (de 2022) e 27002.
Se, para manutenção de máquinas de uma organização é necessário eliminar quaisquer dados sensíveis das máquinas antes de serem manipuladas por pessoal externo à organização, diz-se que esse controle refere-se **ao domínio de controles físicos.**

006. (CESPE/TCE RN/ASSESSOR TÉCNICO DE INFORMÁTICA/CONTROLE EXTERNO/2015) Julgue os itens a seguir, acerca de gestão de segurança da informação à luz das normas ISO/IEC 27001 e 27002.
A política de segurança deve ser aprovada pelo gestor máximo da instituição, assinada pelo chefe da informática, e divulgada para o pessoal de tecnologia da informação e comunicação (TIC).

007. (CESPE/TCE-RN/ASSESSOR TÉCNICO DE INFORMÁTICA/CONTROLE EXTERNO/2015) Julgue os itens a seguir, acerca de gestão de segurança da informação à luz das normas ISO/IEC 27001 e 27002.
Um dos objetivos das auditorias internas do SGSI é determinar se seus controles são executados conforme esperado.

008. (CESPE/MCT/TECNOLOGISTA PLENO/SEGURANÇA DE SISTEMAS DE INFORMAÇÃO/ADAPTADA/2008) Uma organização que deseje implantar um sistema de gestão de segurança da informação (SGSI) deve adotar como base a norma ABNT NBR ISO/IEC 27001:2022

009. (INÉDITA/2023) A seção 4.3 da norma ISO/IEC 27001:2022 trata os itens que a organização deve considerar quando da determinação do escopo.

010. (CESPE/INMETRO/PESQUISADOR/CIÊNCIA DA COMPUTAÇÃO/2010) Com relação aos controles recomendados nas normas 27001 e 27002, é correto destacar que todos os controles que constam da norma devem ser implementados.

011. (CESPE/INMETRO/PESQUISADOR/CIÊNCIA DA COMPUTAÇÃO/2010) Com relação aos controles recomendados nas normas 27001 e 27002, é correto destacar que a implementação dos controles permite garantir a segurança da informação.

012. (CESPE/INMETRO/PESQUISADOR/CIÊNCIA DA COMPUTAÇÃO/2010) Com relação aos controles recomendados nas normas 27001 e 27002, é correto destacar que a norma 27001 define os controles que devem ser implementados.

013. (CESPE/INMETRO/PESQUISADOR/CIÊNCIA DA COMPUTAÇÃO/2010) Com relação aos controles recomendados nas normas 27001 e 27002, é correto destacar que a norma 27002 define os requisitos de um sistema de gestão de segurança da informação.

014. (CESPE/TCU/ANALISTA DE CONTROLE EXTERNO – TI/2007) A ISO 17799 define diretrizes para certificação de que uma organização está em conformidade à própria norma. Essa certificação é conferida por meio de uma auditoria de terceira parte, nos moldes da ISO 19011.

015. (CESPE/BANCO DA AMAZÔNIA/TÉCNICO CIENTÍFICO/ESPECIALIDADE: TI/SEGURANÇA DA INFORMAÇÃO/2010) São exemplos de ativos de uma organização a informação e os processos de apoio, sistemas e redes. Os requisitos de segurança, em uma organização, são identificados por meio de análise sistemática dos riscos de segurança.

016. (FGV/MPE-AL/ANALISTA DO MINISTÉRIO PÚBLICO/DESENVOLVIMENTO DE SISTEMAS/2018) Assinale a opção que melhor descreve o princípio geral da norma ISO/IEC 27001.
a) Definir os procedimentos e tarefas adequados à mitigação de riscos no âmbito de um sistema de gestão de segurança da informação.
b) Definir os requisitos necessários para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação.
c) Estabelecer os papéis, responsabilidades e atuação dos profissionais de segurança da informação numa organização.
d) Orientar e alertar as organizações e seus respectivos profissionais em diversos aspectos relativos à gestão de segurança da informação.
e) Prover uma coleção de artefatos tecnológicos que permitam a identificação, avaliação e eliminação de ataques aos ativos de segurança da informação.

017. (FCC/MPE-PE/ANALISTA MINISTERIAL/INFORMÁTICA/2018/ADAPTADA) Dentre os controles mencionados no Anexo A da norma NBR ISO/IEC 27001:2022 está: "Todos os funcionários da organização e, onde pertinente, as partes externas devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções." Este controle é parte do domínio:
a) Segurança nas operações.
b) Política de segurança da informação.
c) Controles de pessoas.
d) Organização da segurança da informação.
e) Segurança física e do ambiente.

018. (FCC/ARTESP/ESPECIALISTA EM REGULAÇÃO DE TRANSPORTE I/TECNOLOGIA DA INFORMAÇÃO/2017) Uma organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua da gestão da segurança da informação. Dentre esses recursos estão as pessoas que realizam o trabalho sob o controle da organização. Segundo a norma ABNT NBR ISO/IEC 27001:2022, todas estas pessoas devem estar cientes
a) do plano de continuidade de negócios e de suas responsabilidades e papéis, já que todos participam quando é necessário colocar este plano em prática.
b) do plano estratégico, que estabelece a direção a ser seguida pela organização para melhorar o sistema de gestão da segurança da informação.
c) do plano operacional, que define as ações e metas traçadas para atingir os objetivos das decisões estratégicas relacionadas à segurança da informação.
d) de suas responsabilidades no processo de gestão de riscos de segurança da informação, atuando como observadoras das ações dos demais funcionários na identificação de potenciais riscos de segurança da informação.
e) das implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

019. (FGV/DPE-RJ/TÉCNICO SUPERIOR ESPECIALIZADO/SEGURANÇA DA INFORMAÇÃO/2014) Uma instituição pretende implantar um sistema de gestão da segurança da informação. Para isso, ela deve seguir as orientações da norma:
a) ISO 27001.
b) ISO 27002.
c) ISO 27005.
d) ISO 27006.
e) ISO 27010.

020. (ESAF/MPOG/ANALISTA DE PLANEJAMENTO E ORÇAMENTO-APO-TI/2008) A segurança da informação tem como objetivo a preservação da
a) confidencialidade, interatividade e acessibilidade informações.
b) complexidade, integridade e disponibilidade das informações.
c) confidencialidade, integridade e acessibilidade das informações.
d) universalidade, interatividade e disponibilidade das informações.
e) confidencialidade, integridade e disponibilidade das informações.

021. (FCC/INFRAERO/ANALISTA/SEGURANÇA DA INFORMAÇÃO/2011/ADAPTADA) Sobre a norma ABNT NBR ISO/IEC 27001:2022, é INCORRETO afirmar:
a) Promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI de uma organização.
b) Foi desenvolvida para organizações privadas e seus requisitos genéricos não são aplicáveis às organizações públicas ou privadas de pequeno porte.
c) Especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização.
d) Especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes.

022. (FUMARC/PRODEMGE/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/2011) A norma ISO/IEC 27001 foi elaborada para prover um modelo de sistema de gestão de segurança da informação (SGSI) e também para avaliar a conformidade deste pelas partes interessadas internas e externas.

023. (FCC/TRE-RR/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS/2015) Considere que um determinado Tribunal Regional Eleitoral esteja definindo uma forma de gerenciar riscos da infraestrutura de TI, incluindo a determinação de políticas, procedimentos, diretrizes, práticas e estruturas organizacionais para estabelecer proteções e contramedidas. De acordo com a Norma ISO/IEC 27002, essa definição para segurança da informação é denominada
a) Ativo.
b) Evento.
c) Controle.
d) Recurso.
e) Política.

GABARITO

1. d
2. e
3. d
4. C
5. C
6. E
7. C
8. C
9. C
10. E
11. E
12. E
13. E
14. E
15. C
16. b
17. c
18. e
19. a
20. e
21. b
22. C
23. c

GABARITO COMENTADO

004. (CESPE/TJ-AM/ANALISTA JUDICIÁRIO/ANALISTA DE SISTEMAS/2019/ADAPTADA) Julgue o próximo item, relativo à gestão de segurança da informação.

De acordo com a norma NBR ISO/IEC 27001 [de 2022], uma organização que vise estabelecer um sistema de gestão de segurança da informação (SGSI) deve entender o contexto interno e externo da organização em relação aos riscos e aplicar um processo de avaliação de riscos de segurança da informação e uma análise qualitativa e quantitativa.

Na Seção 4.1 Entendendo a organização e seu contexto, a norma destaca que "*a organização deve determinar as questões internas e externas que são relevantes para o seu propósito e que afetam sua capacidade de alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação*".

NOTA A determinação destas questões refere-se ao estabelecimento do contexto interno e externo da organização apresentado na ABNT ISO 31000:2018, 5.4.1.

Ainda, a Seção 6 da norma NBR ISO/IEC 27001 cita que a **organização deve** estabelecer e aplicar um **processo de avaliação de riscos de segurança da informação.**

Certo.

---

005. (CESPE/TCE-RN/ASSESSOR TÉCNICO DE INFORMÁTICA/CONTROLE EXTERNO/2015/ADAPTADA) Julgue os itens a seguir, acerca de gestão de segurança da informação à luz das normas ISO/IEC 27001 (de 2022) e 27002.

Se, para manutenção de máquinas de uma organização é necessário eliminar quaisquer dados sensíveis das máquinas antes de serem manipuladas por pessoal externo à organização, diz-se que esse controle refere-se **ao domínio de controles físicos.**

Nesse contexto, os itens dos equipamentos que contenham mídia de armazenamento devem ser verificados para assegurar que quaisquer dados confidenciais e *software* licenciado tenham sido removidos ou substituídos com segurança antes do descarte ou reutilização. Tal controle é o 7.14 (descarte seguro ou reutilização de equipamentos) e está ligado ao domínio **controles físicos.**

Certo.

---

006. (CESPE/TCE RN/ASSESSOR TÉCNICO DE INFORMÁTICA/CONTROLE EXTERNO/2015) Julgue os itens a seguir, acerca de gestão de segurança da informação à luz das normas ISO/IEC 27001 e 27002.

A política de segurança deve ser aprovada pelo gestor máximo da instituição, assinada pelo chefe da informática, e divulgada para o pessoal de tecnologia da informação e comunicação (TIC).

A política de segurança deve ser definida no mais **alto nível da organização** e **aprovada pela direção**, sendo comunicada aos funcionários e partes externas relevantes de forma que seja entendida, acessível e relevante aos usuários pertinentes. Vide controle 5.1 da ISO/IEC 27001:2022.

Errado.

---

007. (CESPE/TCE-RN/ASSESSOR TÉCNICO DE INFORMÁTICA/CONTROLE EXTERNO/2015) Julgue os itens a seguir, acerca de gestão de segurança da informação à luz das normas ISO/IEC 27001 e 27002.

Um dos objetivos das auditorias internas do SGSI é determinar se seus controles são executados conforme esperado.

Em 9.2.1 temos que a organização deve conduzir **auditorias internas** a intervalos planejados para prover informações sobre se o SGSI:

a) está em conformidade com:

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

2) os requisitos da Norma ABNT NBR ISO/IEC 27001;

b) está efetivamente implementado e mantido.

Dessa forma, um dos objetivos das auditorias internas do SGSI é determinar se seus controles são executados conforme esperado. Quando uma não conformidade for diagnosticada, a organização deve:

a) avaliar a necessidade de ações para eliminar as causas de não conformidade;

b) realizar mudanças no SGSI, quando necessárias, dentre outras.

Certo.

---

008. (CESPE/MCT/TECNOLOGISTA PLENO/SEGURANÇA DE SISTEMAS DE INFORMAÇÃO/ADAPTADA/2008) Uma organização que deseje implantar um sistema de gestão de segurança da informação (SGSI) deve adotar como base a norma ABNT NBR ISO/IEC 27001:2022

Inevitavelmente, uma organização que deseja implantar um **Sistema de Gestão de Segurança da Informação (SGSI)** deve adotar a norma ABNT NBR ISO/IEC 27001:2022 como base. A rigor, a norma é uma especificação (documento que é utilizado para a realização de auditorias e consequente certificação) de um SGSI.

Certo.

---

009. (INÉDITA/2023) A seção 4.3 da norma ISO/IEC 27001:2022 trata os itens que a organização deve considerar quando da determinação do escopo.

A Seção 4.3 da norma ISO/IEC 27001:2022 destaca que **a organização deve determinar os limites e a aplicabilidade do sistema de gestão da segurança da informação para estabelecer seu escopo.**

Quando da **determinação do escopo**, a organização deve considerar:

- As **questões internas e externas** que são relevantes para o seu propósito e que afetam sua capacidade para alcançar os resultados pretendidos do seu sistema de gestão de segurança da informação.
- Os **requisitos das partes interessadas relevantes para a segurança da informação**.
- As **interfaces e dependências entre as atividades** desempenhadas pela organização e aquelas que são desempenhadas por outras organizações.

Segundo a norma ISO/IEC 27001:2022 o escopo deve estar disponível como **informação documentada**.

Certo.

---

010. (CESPE/INMETRO/PESQUISADOR/CIÊNCIA DA COMPUTAÇÃO/2010) Com relação aos controles recomendados nas normas 27001 e 27002, é correto destacar que todos os controles que constam da norma devem ser implementados.

A norma **NÃO** faz esta exigência! Apenas a **não implementação de um controle é que deve ser devidamente justificada**.

Errado.

---

011. (CESPE/INMETRO/PESQUISADOR/CIÊNCIA DA COMPUTAÇÃO/2010) Com relação aos controles recomendados nas normas 27001 e 27002, é correto destacar que a implementação dos controles permite garantir a segurança da informação.

A implementação dos controles garante que as boas práticas de segurança da informação estão sendo seguidas.

Errado.

---

012. (CESPE/INMETRO/PESQUISADOR/CIÊNCIA DA COMPUTAÇÃO/2010) Com relação aos controles recomendados nas normas 27001 e 27002, é correto destacar que a norma 27001 define os controles que devem ser implementados.

Refere-se à Norma 27002, que define os controles que **PODEM** ser implementados.

A **ISO 27001**, por trazer requisitos obrigatórios, utiliza-se do **verbo "deve"**, enquanto a **ISO 27002** usa o **verbo "convém"** para suas diretrizes. Por exemplo, a ISO 27001 diz que "A Alta Direção **deve** estabelecer uma política de segurança da informação (...)". Já a 27002 traz que "**Convém** que as políticas para a segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem (...)".

Errado.

---

013. (CESPE/INMETRO/PESQUISADOR/CIÊNCIA DA COMPUTAÇÃO/2010) Com relação aos controles recomendados nas normas 27001 e 27002, é correto destacar que a norma 27002 define os requisitos de um sistema de gestão de segurança da informação.

O texto refere-se à norma ABNT NBR ISO/IEC 27001.

Errado.

---

014. (CESPE/TCU/ANALISTA DE CONTROLE EXTERNO – TI/2007) A ISO 17799 define diretrizes para certificação de que uma organização está em conformidade à própria norma. Essa certificação é conferida por meio de uma auditoria de terceira parte, nos moldes da ISO 19011.

A ABNT NBR ISO/IEC 17799:2005 (renumerada para **ABNT NBR ISO/IEC 27002**) estabelece diretrizes e princípios gerais para estabelecer, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta norma proveem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação. Cabe ressaltar que não há certificação para pessoas, somente para as empresas. E essa certificação é baseada na ISO/IEC 27001 e não na ISO/IEC 27002!

A norma 27001 é usada para fins de certificação **(faz referência aos controles apenas para fins de checagem para certificação).** É a norma que deve ser adotada como base para uma organização que deseja implantar um Sistema de Gestão de Segurança da Informação (**SGSI**). A rigor, essa norma é uma especificação (documento que é utilizado para a realização de auditorias e consequente certificação) de um SGSI.
Errado.

---

015. (CESPE/BANCO DA AMAZÔNIA/TÉCNICO CIENTÍFICO/ESPECIALIDADE: TI/SEGURANÇA DA INFORMAÇÃO/2010) São exemplos de ativos de uma organização a informação e os processos de apoio, sistemas e redes. Os requisitos de segurança, em uma organização, são identificados por meio de análise sistemática dos riscos de segurança.

A segurança é uma palavra que está presente em nosso cotidiano e refere-se a um estado de proteção, livre de perigos e incertezas. Em uma corporação, a segurança está ligada a todos os "objetos" de valor, que necessitam de proteção. Tais objetos são considerados como **ativos** (RAMOS *et al.*, 2006).
Segundo Sêmola (2003), **ativo** é tudo aquilo que tem um valor significativo para a empresa. São os **elementos que compõem e processam a informação, incluindo ela mesma**. O termo ativo possui essa denominação, oriunda da área financeira, por ser considerado um elemento de valor para um indivíduo ou organização, e que, por esse motivo, necessita de proteção adequada (ISO/IEC-27002) (SÊMOLA, 2003, p. 45). Em linhas gerais, os ativos podem ser divididos nas categorias especificadas a seguir.

Figura. Categorias de Ativos

Cada grupo tem sua importância no ambiente corporativo, pois sem eles o negócio da organização não funciona, ou seja, ela terá problemas no seu dia a dia. Vamos ao estudo de cada um deles!!

- **Aplicações:** grupo de ativos que engloba todos os programas de computador utilizados para a automatização de processos, isto é, acesso, leitura, trânsito, armazenamento e processamento das informações. Dentre eles citamos: sistema de Folha de Pagamento, sistemas operacionais, etc.

- **Informação:** neste grupo tem-se o principal ativo da empresa que é a informação. A informação pode estar registrada em meio eletrônico ou físico. Deve-se considerar qualquer tipo de informação, independente do tipo de meio em que esteja armazenada, que seja importante para a empresa e seus negócios.
- **Usuários (ou pessoas):** este grupo refere-se aos indivíduos que utilizam a estrutura tecnológica e de comunicação da empresa e que lidam com a informação. Exemplos: usuários do setor de Recursos Humanos, direção da empresa, etc.
- **Equipamentos**: esse grupo de ativos representa toda a infraestrutura tecnológica que oferece suporte à informação durante seu uso, trânsito, processamento e armazenamento. Faz parte desse grupo qualquer equipamento no qual se armazene, processe ou transmita as informações da empresa, como microcomputadores, servidores, hubs, switches.
- **Organização**: neste grupo, segundo Technet (2006), estão incluídos os aspectos que compõem a estrutura física e organizacional das empresas. Refere-se à organização lógica e física do pessoal dentro da empresa em questão. Como exemplos de estrutura organizacional, temos, entre outros: a estrutura departamental e funcional, a distribuição de funções e os fluxos de informação da empresa os servidores. Em relação ao ambiente físico, entre outros, são considerados: salas e armários em que estão localizados os documentos, fitoteca, sala de servidores, etc.

Finalizando, conforme visto, os elementos considerados na questão (**informações, equipamentos, usuários, aplicações e processos de apoio)** são exemplos de ativos. Quanto aos **requisitos de segurança**, em uma organização, cabe destacar que são identificados por meio de análise sistemática dos riscos de segurança da informação.

Certo.

---

016. (FGV/MPE-AL/ANALISTA DO MINISTÉRIO PÚBLICO/DESENVOLVIMENTO DE SISTEMAS/2018) Assinale a opção que melhor descreve o princípio geral da norma ISO/IEC 27001.

a) Definir os procedimentos e tarefas adequados à mitigação de riscos no âmbito de um sistema de gestão de segurança da informação.

b) Definir os requisitos necessários para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação.

c) Estabelecer os papéis, responsabilidades e atuação dos profissionais de segurança da informação numa organização.

d) Orientar e alertar as organizações e seus respectivos profissionais em diversos aspectos relativos à gestão de segurança da informação.

e) Prover uma coleção de artefatos tecnológicos que permitam a identificação, avaliação e eliminação de ataques aos ativos de segurança da informação.

A **norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente (EIMM) um Sistema de Gestão de Segurança da Informação (SGSI)** dentro do contexto da organização.

Letra b.

---

017. (FCC/MPE-PE/ANALISTA MINISTERIAL/INFORMÁTICA/2018/ADAPTADA) Dentre os controles mencionados no Anexo A da norma NBR ISO/IEC 27001:2022 está: "Todos os funcionários da organização e, onde pertinente, as partes externas devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções." Este controle é parte do domínio:

a) Segurança nas operações.
b) Política de segurança da informação.
c) Controles de pessoas.
d) Organização da segurança da informação.
e) Segurança física e do ambiente.

Conforme visto a seguir, o controle aqui mencionado é parte do domínio **Controles de pessoas**, que especifica controles para antes da contratação, durante e após a contratação.

6	Controles de pessoas	
6.3	Conscientização, educação e treinamento em segurança da informação	**Controle** O pessoal da organização e partes interessadas relevantes devem receber treinamento, educação e conscientização em segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas e procedimentos específicas por tema, pertinentes para as suas funções.

Fonte: ISO/IEC 27001:2022

Letra c.

---

018. (FCC/ARTESP/ESPECIALISTA EM REGULAÇÃO DE TRANSPORTE I/TECNOLOGIA DA INFORMAÇÃO/2017) Uma organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua da gestão da segurança da informação. Dentre esses recursos estão as pessoas que realizam o trabalho

sob o controle da organização. Segundo a norma ABNT NBR ISO/IEC 27001:2022, todas estas pessoas devem estar cientes

a) do plano de continuidade de negócios e de suas responsabilidades e papéis, já que todos participam quando é necessário colocar este plano em prática.

b) do plano estratégico, que estabelece a direção a ser seguida pela organização para melhorar o sistema de gestão da segurança da informação.

c) do plano operacional, que define as ações e metas traçadas para atingir os objetivos das decisões estratégicas relacionadas à segurança da informação.

d) de suas responsabilidades no processo de gestão de riscos de segurança da informação, atuando como observadoras das ações dos demais funcionários na identificação de potenciais riscos de segurança da informação.

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

A **seção 7.3** ("**Conscientização**") da norma ABNT NBR ISO/IEC 27001:2022 **destaca** que as **pessoas que realizam trabalho** sob o controle da organização **devem estar cientes de:**

a) Política de Segurança da Informação,

b) suas **contribuições** para a **eficácia** do **SGSI;** e

c) implicações da não conformidade com os requisitos do **SGSI**.

Conforme visto, a letra E é a resposta.

Letra e.

---

019. (FGV/DPE-RJ/TÉCNICO SUPERIOR ESPECIALIZADO/SEGURANÇA DA INFORMAÇÃO/2014) Uma instituição pretende implantar um sistema de gestão da segurança da informação. Para isso, ela deve seguir as orientações da norma:

a) ISO 27001.

b) ISO 27002.

c) ISO 27005.

d) ISO 27006.

e) ISO 27010.

a) Certa. A **Norma NBR ISO/IEC 27001:2022** especifica os **requisitos para estabelecer, implementar, manter e melhorar continuamente (EIMM) um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto da organização.**

b) Errada. ISO 27002->Código de Melhores Práticas para a Gestão de Segurança da Informação.

c) Errada. ISO 27005 ->Gestão de Riscos de Segurança da Informação.

d) Errada. ISO 27006 -> Requisitos para auditorias externas em um Sistema de Gerenciamento de Segurança da Informação. Especifica como o processo de auditoria de um sistema de gerenciamento de segurança da informação deve ocorrer.

e) Errada. ISO 27010 -> Gestão de Segurança da Informação para Comunicações Inter Empresariais. Foco nas melhores formas de comunicar, acompanhar, monitorar grandes incidentes e fazer com que isso seja feito de forma transparente entre empresas particulares e governamentais.

Letra a.

---

020. (ESAF/MPOG/ANALISTA DE PLANEJAMENTO E ORÇAMENTO-APO-TI/2008) A segurança da informação tem como objetivo a preservação da

a) confidencialidade, interatividade e acessibilidade informações.

b) complexidade, integridade e disponibilidade das informações.

c) confidencialidade, integridade e acessibilidade das informações.

d) universalidade, interatividade e disponibilidade das informações.

e) confidencialidade, integridade e disponibilidade das informações.

Essa questão é bem simples e muito importante! Vamos à explicação em detalhes! A segurança da informação busca proteger os ativos de uma empresa ou indivíduo com base na preservação de alguns princípios.

Os quatro princípios considerados centrais ou principais, mais comumente cobrados em provas, são a confidencialidade, a integridade, a disponibilidade e a autenticidade (É possível encontrar a sigla **CIDA**, ou **DICA**, para fazer menção a estes princípios!).

- **Confidencialidade (sigilo):** é a garantia de que a informação não será conhecida por quem não deve. O acesso às informações deve ser limitado, ou seja, somente as pessoas explicitamente autorizadas podem acessá-las.

Perda de confidencialidade significa perda de segredo. Se uma informação for confidencial, ela será secreta e deverá ser guardada com segurança, e não divulgada para pessoas não-autorizadas. Exemplo: o número do seu cartão de crédito só poderá ser conhecido por você e pela loja onde é usado. Se esse número for descoberto por alguém mal-intencionado, o prejuízo causado pela perda de confidencialidade poderá ser elevado, já que poderão se fazer passar por você para realizar compras pela Internet, proporcionando-lhe prejuízos financeiros e uma grande dor de cabeça!

- **Integridade:** esse princípio destaca que a informação deve ser mantida na condição em que foi liberada pelo seu proprietário, garantindo a sua proteção contra mudanças

intencionais, indevidas ou acidentais. Em outras palavras, é a garantia de que a informação que foi armazenada é a que será recuperada!

A quebra de integridade pode ser considerada sob 2 aspectos:

1. alterações nos elementos que suportam a informação – são feitas alterações na estrutura física e lógica em que uma informação está armazenada. Por exemplo, quando são alteradas as configurações de um sistema para ter acesso a informações restritas;
2. alterações do conteúdo dos documentos:
   - ex1.: imagine que alguém invada o *notebook* que está sendo utilizado para realizar a sua declaração do Imposto de Renda deste ano, e, momentos antes de você enviá-la para a Receita Federal a mesma é alterada sem o seu consentimento! Neste caso, a informação não será transmitida da maneira adequada, o que quebra o princípio da integridade;

- **Disponibilidade**: é a garantia de que a informação deve estar disponível, sempre que seus usuários (pessoas e empresas autorizadas) necessitarem, não importando o motivo. Em outras palavras, é a garantia que a informação sempre poderá ser acessada!!!

Como exemplo, há quebra do princípio da disponibilidade quando você decidir enviar a sua declaração do Imposto de Renda pela Internet, no último dia possível, e o *site* da Receita Federal estiver indisponível.

A figura seguinte destaca a essência da aplicação dos três princípios acima. Ou seja, **desejamos entregar a informação CORRETA, para a pessoa CERTA, no momento CORRETO!!!** Entenderam?? Ainda, cabe destacar que **a perda de pelo menos um desses princípios já irá ocasionar impactos ao negócio** (aí surgem os **incidentes de segurança**!)

Figura. Princípios Básicos – Integridade, Confidencialidade e Disponibilidade

- **Autenticidade:** consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações. Em outras palavras, é a capacidade de garantir a identidade de uma pessoa (física ou jurídica) que acessa as informações do sistema ou de um

servidor (computador) com quem se estabelece uma transação (de comunicação, como um e-mail, ou comercial, como uma venda on-line).

Outros princípios podem ser também levados em consideração. São eles:

- **Confiabilidade:** pode ser caracterizada como a condição em que um sistema de informação presta seus serviços de forma eficaz e eficiente. Ou melhor, um sistema de informação irá "desempenhar o papel que foi proposto para si".
- **Não-repúdio (irretratabilidade):** é a garantia de que um agente não consiga negar (dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação. Essa garantia é condição necessária para a validade jurídica de documentos e transações digitais. Só se pode garantir o não-repúdio quando houver autenticidade e integridade (ou seja, quando for possível determinar quem mandou a mensagem e garantir que a mesma não foi alterada).
- **Legalidade:** aderência do sistema à legislação. Nesse caso, a informação deve estar em conformidade com os preceitos da legislação em vigor.
- **Auditoria**: é a possibilidade de rastrear o histórico dos eventos de um sistema para determinar quando e onde ocorreu uma violação de segurança, bem como identificar os envolvidos nesse processo. Visa proteger os sistemas contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, são utilizadas trilhas de auditorias e *logs*, que registram o que foi executado no sistema, por quem e quando.
- **Privacidade:** diz respeito ao direito fundamental de cada indivíduo de decidir quem deve ter acesso aos seus dados pessoais.

A privacidade é a capacidade de um sistema manter incógnito um usuário (capacidade de um usuário realizar operações em um sistema sem que seja identificado), impossibilitando a ligação direta da identidade do usuário com as ações por este realizadas. Privacidade é uma característica de segurança requerida, por exemplo, em eleições secretas.

Uma informação privada deve ser vista, lida ou alterada somente pelo seu dono. Esse princípio difere da confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada.

Quando falamos em segurança da informação, estamos nos referindo a salvaguardas para manter a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente.

Letra e.

---

021. (FCC/INFRAERO/ANALISTA/SEGURANÇA DA INFORMAÇÃO/2011/ADAPTADA) Sobre a norma ABNT NBR ISO/IEC 27001:2022, é INCORRETO afirmar:

a) Promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI de uma organização.
b) Foi desenvolvida para organizações privadas e seus requisitos genéricos não são aplicáveis às organizações públicas ou privadas de pequeno porte.
c) Especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização.
d) Especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes.

Dentre as assertivas, a B é falsa. A norma ABNT NBR ISO/IEC 27001:2022 cobre **TODOS** os tipos de organizações (por exemplo, empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos).
Letra b.

---

022. (FUMARC/PRODEMGE/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/2011) A norma ISO/IEC 27001 foi elaborada para prover um modelo de sistema de gestão de segurança da informação (SGSI) e também para avaliar a conformidade deste pelas partes interessadas internas e externas.

A norma ISO/IEC 27001 foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um **Sistema de Gestão de Segurança da Informação (SGSI)**.
A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização. É esperado que este e os sistemas de apoio mudem com o passar do tempo. É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples.
Esta norma pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas.
Certo.

---

023. (FCC/TRE-RR/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS/2015) Considere que um determinado Tribunal Regional Eleitoral esteja definindo uma forma de gerenciar riscos

da infraestrutura de TI, incluindo a determinação de políticas, procedimentos, diretrizes, práticas e estruturas organizacionais para estabelecer proteções e contramedidas. De acordo com a Norma ISO/IEC 27002, essa definição para segurança da informação é denominada

a) Ativo.
b) Evento.
c) Controle.
d) Recurso.
e) Política.

Vamos à descrição dos termos aqui listados:

a) Errada. **Ativo** é algo que tem valor para a organização e que requer adequada proteção. Exemplos: ativos primários (processos e atividades de negócio, informação) e ativos de suporte e infraestrutura (sobre os quais os elementos primários do escopo se apoiam), que são: hardware, software, rede, recursos humanos, instalações físicas, estrutura da organização [ABNT NBR ISO/IEC 17799:2005].

b) Errada. **Evento de segurança da informação** é uma ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação [ISO/IEC TR 18044:2004].

c) Certa. **Controle** é uma forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle também é usado como sinônimo para proteção ou contramedida [ABNT NBR ISO/IEC 17799:2005].

d) Errada. **Recursos de processamento de informação** designa qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem [ABNT NBR ISO/IEC 17799:2005].

e) Errada. O termo **política** designa as intenções e diretrizes globais formalmente expressas pela direção [ABNT NBR ISO/IEC 17799:2005].

Letra c.

REFERÊNCIAS

ABNT NBR ISO/IEC 270001. **Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação**. Rio de Janeiro, 2022.

ABNT NBR ISO/IEC 27002. **Segurança da informação, segurança cibernética e proteção de privacidade – Controles de segurança da informação.** Rio de Janeiro, 2022.

ABNT NBR ISO/IEC 27003. **Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Orientações.**

ABNT NBR ISO/IEC 27005. **Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro, 2008.

LEAL, R. **O que é a ISO 27001?** 2015. Disponível em: <https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/>. Acesso em: 10 ago. de 2020.

QUINTÃO, P. L. **Notas de Aula da disciplina "Tecnologia da Informação"**. 2023.

_____. **Informática-FCC-Questões Comentadas e Organizadas por Assunto, 3ª. Edição.** Ed. Gen/Método, 2014.

_____. **1001 Questões Comentadas de Informática -Cespe, 2ª. Edição.** Ed. Gen/Método, 2017.

_____. Notas de aula sobre normas da ABNT de segurança. 2023.

Abra

caminhos

crie

futuros

gran.com.br