

TECNOLOGIA DA INFORMAÇÃO

Gestão de Segurança da Informação:
Norma NBR ISO/IEC n. 27.002:2013



SUMÁRIO

Apresentação	5
Gestão de Segurança da Informação: Norma NBR ISO/IEC n. 27.002:2013	6
1. Escopo	6
2. Referência Normativa	7
3. Termos e Definições	7
4. Estrutura desta Norma	10
5. Políticas de Segurança da Informação	12
5.1. Orientação da Direção para Segurança da Informação	12
6. Organização da Segurança da Informação	14
6.1. Organização Interna	14
6.2. Dispositivos Móveis e Trabalho Remoto	15
7. Segurança em Recursos Humanos	15
7.1. Antes da Contratação	15
7.2. Durante a Contratação	16
7.3. Encerramento e Mudança da Contratação	16
8. Gestão de Ativos	17
8.1. Responsabilidade pelos Ativos	17
8.2. Classificação da Informação	18
8.3. Tratamento de Mídias	18
9. Controle de Acesso	19
9.1. Requisitos do Negócio para Controle de Acesso	19
9.2. Gerenciamento de Acesso do Usuário	20
9.3. Responsabilidades dos Usuários	20
9.4. Controle de Acesso ao Sistema e à Aplicação	21
10. Criptografia	22
10.1. Controles Criptográficos	23
11. Segurança Física e do Ambiente	26

11.1. Áreas Seguras	27
11.2. Equipamento	32
12. Segurança nas Operações.....	40
12.1. Responsabilidades e Procedimentos Operacionais.....	41
12.2. Proteção Contra Malware	43
12.3. Cópias de Segurança	43
12.4. Registros e Monitoramento	44
12.5. Controle de Software Operacional.....	44
12.6. Gestão de Vulnerabilidades Técnicas.....	45
12.7. Considerações quanto à Auditoria de Sistemas da Informação	45
13. Segurança nas Comunicações.....	45
13.1. Gerenciamento da Segurança em Redes	46
13.2. Transferência de Informação	46
14. Aquisição, Desenvolvimento e Manutenção de Sistemas.....	47
14.1. Requisitos de Segurança de Sistemas de Informação	47
14.2. Segurança em Processos de Desenvolvimento e de Suporte	48
14.3. Dados para Teste	49
15. Relacionamento na Cadeia de Suprimento.....	49
15.1. SI na Cadeira de Suprimento	50
15.2. Gerenciamento da Entrega do Serviço do Fornecedor	50
16. Gestão de Incidentes de Segurança da Informação	51
16.1. Gestão de Incidentes de SI e Melhorias.....	51
17. Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio	52
17.1. Continuidade da Segurança da Informação (SI)	52
17.2. Redundâncias.....	55
18. Conformidade	55
18.1. Conformidade com Requisitos Legais e Contratuais.....	56
18.2. Análise Crítica da Segurança da Informação.....	57
Resumo.....	58
Questões Comentadas em Aula	60

O conteúdo deste livro eletrônico é licenciado para Nome do Concurseiro(a) - 000.000.000-00, vedada, por quaisquer meios e a qualquer título, a sua reprodução, cópia, divulgação ou distribuição, sujeitando-se aos infratores à responsabilização civil e criminal.

Questões de Concurso	61
Gabarito.....	76
Referências.....	77

O conteúdo deste livro eletrônico é licenciado para Nome do Concurseiro(a) - 000.000.000-00, vedada, por quaisquer meios e a qualquer título, a sua reprodução, cópia, divulgação ou distribuição, sujeitando-se aos infratores à responsabilização civil e criminal.

APRESENTAÇÃO

Olá, querido(a) amigo(a), tudo bem?

Rumo ao estudo da **Norma ABNT NBR ISO/IEC 27002 - Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Controles de Segurança da Informação.**

FORÇA e muita DETERMINAÇÃO nos estudos!

Em caso de dúvidas, acesse o fórum do curso ou entre em contato.

Um forte abraço,

Profª Patrícia Quintão

Instagram: @coachpatriciaquintao

WhatsApp: (31) 99442.0615

GESTÃO DE SEGURANÇA DA INFORMAÇÃO: NORMA NBR ISO/IEC N. 27.002:2013

A Norma ABNT NBR ISO/IEC 27002:2013 é projetada para as organizações usarem como uma **referência na seleção de controles dentro do processo de implementação de um Sistema de Gestão de Segurança da Informação (SGSI)**, ou como um documento de orientação para as organizações implementarem controles de Segurança da Informação (SI) comumente aceitos.

Organizações de todos os tipos e tamanhos (incluindo o setor privado e público, organizações comerciais e sem fins lucrativos), coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal.

A informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações têm valor para o negócio da organização e, consequentemente, **requer proteção contra vários riscos**.

Uma SI eficaz **reduz estes riscos**, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos.

A SI é alcançada pela **implementação de um conjunto adequado de controles**, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados.

É essencial que uma organização identifique os seus requisitos de SI. Existem **três fontes principais de requisitos de SI**:

- **avaliação de riscos**, por meio da qual são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio;
- **a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais**, além do seu ambiente sociocultural;
- **conjuntos particulares de princípios, objetivos e os requisitos do negócio** para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.

Controles podem ser selecionados desta Norma ou de outros conjuntos de controles, ou novos controles podem ser projetados para atender às necessidades específicas, conforme apropriado.

1. ESCOPO

A Norma NBR ISO/IEC 27002:2013 fornece **diretrizes para práticas de gestão de SI e normas de SI para as organizações**, incluindo a seleção, implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da SI da organização.

A Norma é projetada para organizações que pretendam:

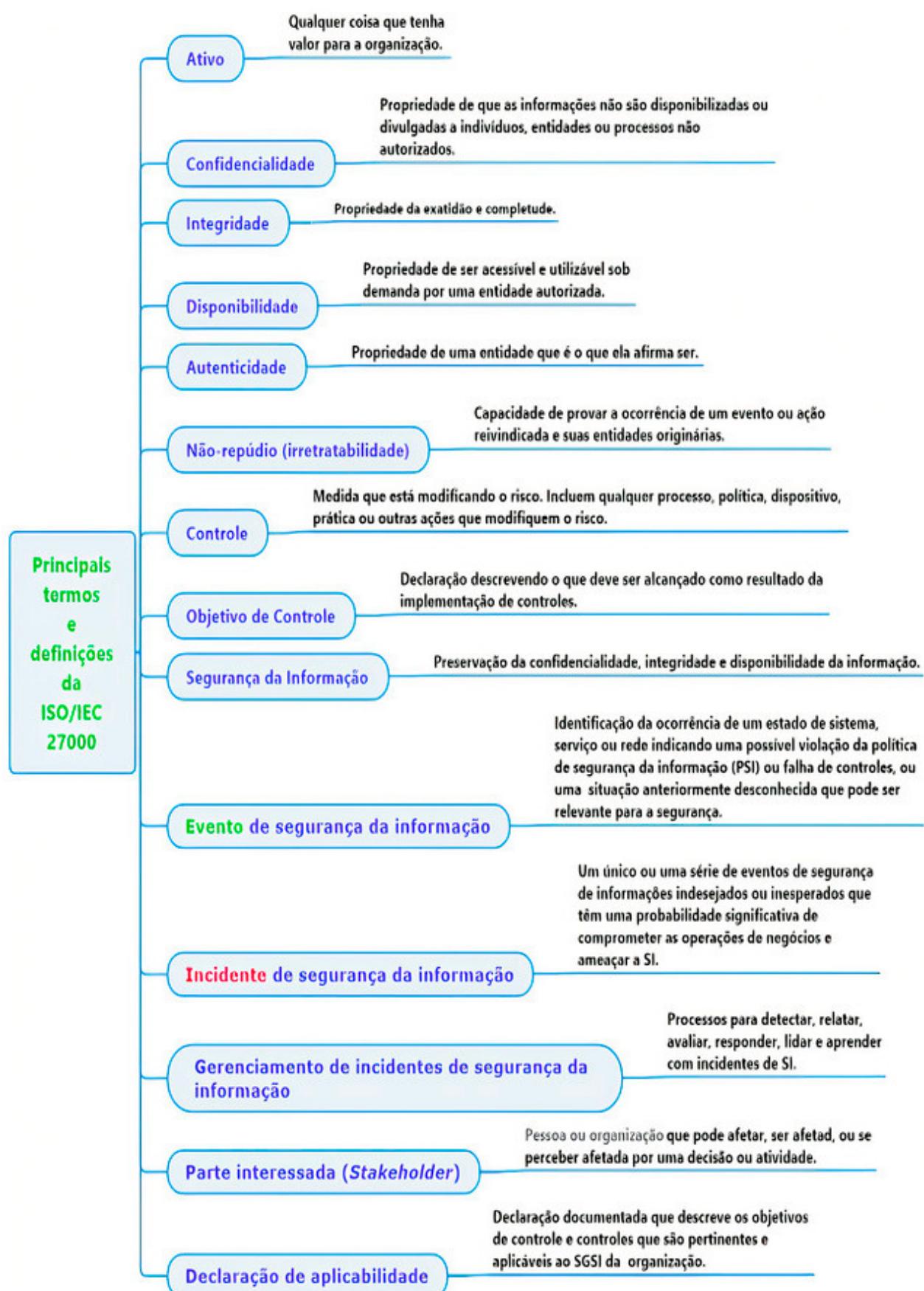
- **selecionar controles** dentro do processo de implementação de um SGSI baseado na Norma 27001;
- **implementar controles** de SI comumente aceitos;
- **desenvolver seus próprios princípios** de gestão da SI.

2. REFERÊNCIA NORMATIVA

O documento **ISO/IEC 27000**, *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary* é **indispensável à aplicação da ISO 27002**, pois traz a **visão geral e o vocabulário** comum da **família** de normas que tratam de **SGSI**.

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 (2020)

O conteúdo deste livro eletrônico é licenciado para Nome do Concurseiro(a) - 000.000.000-00, vedada, por quaisquer meios e a qualquer título, a sua reprodução, cópia, divulgação ou distribuição, sujeitando-se aos infratores à responsabilização civil e criminal.

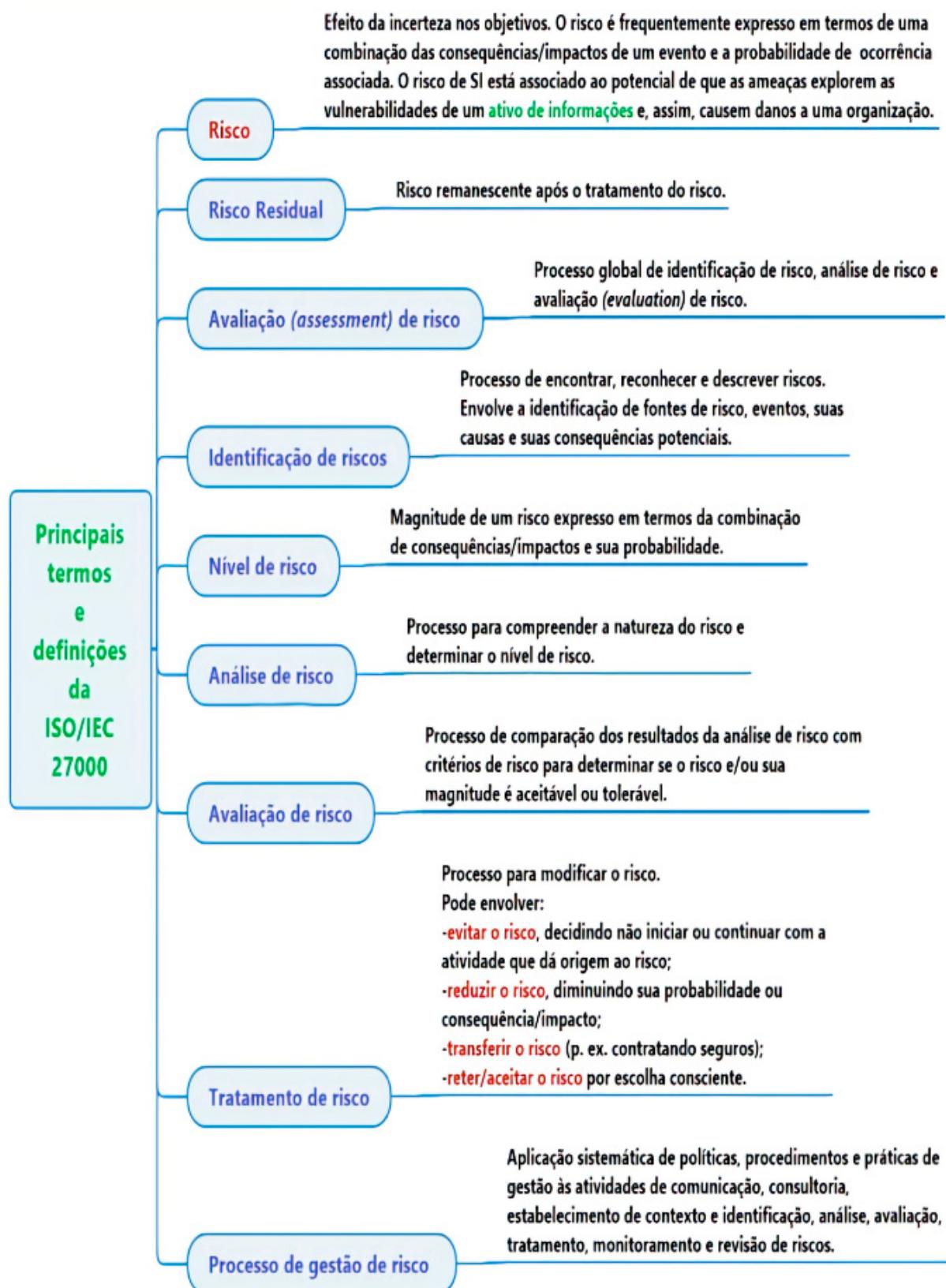


Figura. Termos e definições (Parte II). Fonte: Quintão (2020)

4. ESTRUTURA DESTA NORMA

As principais seções da norma ABNT NBR ISO IEC 27002:2013 são as seguintes:



Figura. Seções da norma ABNT NBR ISO IEC 27002:2013. Fonte: Quintão (2020)

A ordem das seções **não** segue um grau de importância, ficando a cargo de cada organização identificar as **seções aplicáveis** e a relevância de cada uma.

O conteúdo deste livro eletrônico é licenciado para Nome do Concurseiro(a) - 000.000.000-00, vedada, por quaisquer meios e a qualquer título, a sua reprodução, cópia, divulgação ou distribuição, sujeitando-se aos infratores à responsabilização civil e criminal.

As **14 seções da ISO 27002 que contém controles** são:



Conforme visto, a norma contém **14 seções de controles de SI** de um total de **35 objetivos de controles** e **114 controles de segurança**.

Cada **seção** definindo os controles de SI **contém um ou mais objetivos de controle**.

Cada **seção principal** contém um objetivo de controle declarando o que se espera ser alcançado; e um ou mais **controles** que podem ser **aplicados para se alcançar o objetivo do controle**.

Cada **controle** possui um **conjunto de diretrizes de implementação**, as quais apresentam informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle.

N. Seção	Nome	Objetivos de Controle (categorias)	Controles
5	Políticas de Segurança da Informação.		
6	Organização da Segurança da Informação.		
7	Segurança em Recursos Humanos.		
8	Gestão de Ativos.		
9	Controle de Acesso.		
10	Criptografia		
11	Segurança Física e do Ambiente.		
12	Segurança nas Operações		
13	Segurança nas Comunicações		
14	Aquisição, desenvolvimento e Manutenção de Sistemas		
15	Relacionamento na Cadeia de Suprimento		
16	Gestão de Incidentes de Segurança da Informação		
17	Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio		
18	Conformidade		
Total		35	114

5. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

5. Políticas de segurança da informação.

5.1 Orientação da Direção para segurança da informação.

5.1.1 Políticas para segurança da Informação.

5.1.2 Análise crítica das políticas para Segurança da Informação.

5.1. ORIENTAÇÃO DA DIREÇÃO PARA SEGURANÇA DA INFORMAÇÃO

Objetivo: prover orientação da direção e apoio para a SI de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Esse objetivo é dividido em **dois controles**.

5.1.1. Políticas para Segurança da Informação

Controle: convém que um conjunto de políticas de SI deve ser definido, aprovado pela direção, publicado e comunicado para os funcionários e partes externas relevantes.

Diretrizes para implementação. Sobre **políticas de SI**, convém que:

- Contemplem **requisitos** oriundos da **estratégia do negócio**; de **regulamentações, legislação e contratos; do ambiente de ameaça da SI**, atual e futuro;
- Contenham **declarações** relativas a:
 - **definição** da SI, **objetivos e princípios** para orientar todas as atividades relativas à SI;
 - atribuição de **responsabilidades** para os **papéis** definidos;
 - **processos** para o **tratamento dos desvios** e exceções;
- A PSI seja apoiada por **políticas de tópicos** específicos:
 - Controle de acesso (ver Seção 9);
 - Classificação e tratamento da informação (ver 8.2);
 - Segurança física e do ambiente (ver Seção 11);
 - Tópicos orientados aos usuários finais, como:
 - uso aceitável dos ativos (ver 8.1.3);
 - mesa limpa e tela limpa (ver 11.2.9);
 - transferência de informações (ver 13.2.1);
 - dispositivos móveis e trabalho remoto (ver 6.2);
 - restrições sobre o uso e instalação de software (ver 12.6.2);
 - *Backup* (ver 12.3);
 - Transferência da informação (ver 13.2);
 - Proteção contra *malware* (ver 12.2);
 - Gerenciamento de vulnerabilidades técnicas (ver 12.6.1);
 - **Controles criptográficos** (ver Seção 10);
 - Segurança nas comunicações (ver Seção 13);
 - Proteção e privacidade da informação de identificação pessoal (ver 18.1.4);
 - Relacionamento na cadeia de suprimento (ver Seção 15).
- Estas **políticas sejam comunicadas** aos funcionários e partes externas.

5.1.2. Análise Crítica das Políticas para Segurança da Informação

Controle: convém que as políticas de SI devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Diretrizes para implementação. Sobre **análise crítica das políticas de SI**, convém que:

- **cada PSI tenha um gestor** que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação das políticas de SI;

- inclua a avaliação de **oportunidades para melhoria** da PSI da organização;
- leve em consideração os **resultados da análise crítica pela direção**;
- seja obtida a **aprovação da direção** para a política revisada.

6. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

6. Organização da Segurança da Informação.

6.1. Organização interna.

- 6.1.1. Responsabilidades e papéis pela Segurança da Informação.
- 6.1.2. Segregação de Funções.
- 6.1.3. Contato com Autoridades.
- 6.1.4. Contato com grupos Especiais.
- 6.1.5. Segurança da Informação no gerenciamento de projetos.

6.2. Dispositivos móveis e trabalho remoto.

- 6.2.1. Política para uso de dispositivo móvel.
- 6.2.2. Trabalho Remoto.

Esta Seção possui **dois objetivos**.

6.1. ORGANIZAÇÃO INTERNA

Objetivo: estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.

Esse objetivo é dividido em **cinco controles**:

6.1.1. Responsabilidades e Papéis pela Segurança da Informação

Controle: convém que todas as responsabilidades pela SI sejam definidas.

6.1.2. Segregação de Funções

Controle: convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.

6.1.3. Contato com Autoridades

Controle: convém que contatos apropriados com autoridades relevantes sejam mantidos.

6.1.4. Contato com Grupos Especiais

Controle: convém que contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em SI sejam mantidos.

6.1.5. Segurança da Informação no Gerenciamento de Projetos

Controle: convém que a SI seja considerada no gerenciamento de projetos, **independente-mente do tipo de projeto.**

6.2. DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

Objetivo: garantir a segurança das informações no trabalho remoto e no uso de dispositivo móveis.

Esse objetivo é dividido em **dois controles**:

6.2.1. Política para Uso de Dispositivo Móvel

Controle: convém que uma política e medidas que apoiam a SI sejam adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.

6.2.2. Trabalho Remoto

Controle: convém que uma política e medidas que apoiam a SI sejam **implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.**

7. SEGURANÇA EM RECURSOS HUMANOS

7. Segurança em Recursos Humanos.

7.1. Antes da Contratação.

7.1.1. Seleção.

7.1.2. Termos e Condições de Contratação.

7.2. Durante a Contratação.

7.2.1. Responsabilidades da Direção.

7.2.2. Conscientização, educação e treinamento em segurança da informação.

7.2.3. Processo disciplinar.

7.3. Encerramento e mudança da contratação.

7.3.1. Responsabilidades pelo encerramento ou mudança da contratação.

Esta Seção possui **três objetivos**.

7.1. ANTES DA CONTRATAÇÃO

Objetivo: assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.

Esse objetivo é dividido em dois controles.

7.1.1. Seleção

Controle: convém que **verificações do histórico sejam realizadas para todos os candidatos a emprego**, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.

7.1.2. Termos e Condições de Contratação

Controle: convém que as obrigações contratuais com funcionários e partes externas declarem a sua responsabilidade e as da organização para a segurança da informação.

7.2. DURANTE A CONTRATAÇÃO

Objetivo: assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.

Esse objetivo é dividido em **três controles**.

7.2.1. Responsabilidade da Direção

Controle: convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.

7.2.2. Conscientização, Educação e Treinamento em Segurança da Informação

Controle: convém que todos os funcionários da organização e, onde pertinente, partes externas recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

7.2.3. Processo Disciplinar

Controle: convém que exista um processo disciplinar formal, implantado e comunicado, **para tomar ações contra funcionários que tenham cometido uma violação** de segurança da informação.

7.3. ENCERRAMENTO E MUDANÇA DA CONTRATAÇÃO

Objetivo: proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

Esse objetivo é dividido em **um controle**.

7.3.1. Responsabilidades pelo Encerramento ou Mudança da Contratação

Controle: convém que as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação sejam definidas, comunicadas aos funcionários ou partes externas e cumpridas.

8. GESTÃO DE ATIVOS

8. Gestão de ativos.

8.1. Responsabilidade pelos ativos.

8.1.1. Inventário dos ativos.

8.1.2. Proprietário dos ativos.

8.1.3. Uso aceitável dos ativos.

8.1.4. Devolução dos ativos.

8.2. Classificação da informação.

8.2.1. Classificação da Informação.

8.2.2. Rótulos e tratamento da informação.

8.2.3. Tratamento dos ativos.

8.3. Tratamento de mídias.

8.3.1. Gerenciamento de mídias removíveis.

8.3.2. Descarte de mídias.

8.3.3. Transferência física de mídias.

Esta Seção é de grande importância para a prova e possui **três objetivos**.

8.1. RESPONSABILIDADE PELOS ATIVOS

Objetivo: identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.

Esse objetivo é dividido em **quatro controles**.

8.1.1. Inventário dos Ativos

Controle: convém que os ativos associados à informação e aos recursos de processamento da informação sejam identificados, e um inventário destes ativos seja estruturado e mantido.

8.1.2. Proprietário dos Ativos

Controle: convém que os ativos mantidos no inventário tenham um proprietário.

8.1.3. Uso Aceitável dos Ativos

Controle: convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação sejam identificadas, documentadas e implementadas.

8.1.4. Devolução dos Ativos

Controle: convém que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

8.2. CLASSIFICAÇÃO DA INFORMAÇÃO

Objetivo: assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

Esse objetivo é dividido em **três controles**:

8.2.1. Classificação da Informação

Controle: convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

8.2.2. Rótulos e Tratamento da Informação

Controle: convém que um conjunto apropriado de procedimento para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotada pela organização.

8.2.3. Tratamento dos Ativos

Controle: convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela organização.

8.3. TRATAMENTO DE MÍDIAS

Objetivo: prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.

Esse objetivo é dividido em **três controles**:

8.3.1. Gerenciamento de Mídias Removíveis

Controle: convém que existam procedimentos implementados para o gerenciamento de mídias removíveis de acordo com o esquema de classificação adotado pela organização.

8.3.2. Descarte de Mídias

Controle: convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.

8.3.3. Transferência Física de Mídias

Controle: convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.

9. CONTROLE DE ACESSO

9. Controle de Acesso.

9.1. Requisitos do negócio para controle de acesso.

9.1.1. Política de controle de acesso.

9.1.2. Acesso às redes e aos serviços de rede.

9.2. Gerenciamento de acesso do usuário.

9.2.1. Registro e cancelamento de usuário.

9.2.2. Provisionamento para acesso de usuário.

9.2.3. Gerenciamento de direitos de acesso privilegiados.

9.2.4. Gerenciamento da informação de autenticação secreta de usuários.

9.2.5. Análise crítica dos direitos de acesso de usuário.

9.2.6. Retirada ou ajuste dos direitos de acesso.

9.3. Responsabilidades dos usuários.

9.3.1. Uso da informação de autenticação secreta.

9.4. Controle de acesso ao sistema e à aplicação.

9.4.1. Restrição de acesso à informação.

9.4.2. Procedimentos seguros de entrada no sistema (*log-on*).

9.4.3. Sistema de Gerenciamento de senha.

9.4.4. Uso de programas utilitários privilegiados.

9.4.5. Controle de acesso ao código-fonte de programas.

Esta Seção possui **quatro objetivos**.

9.1. REQUISITOS DO NEGÓCIO PARA CONTROLE DE ACESSO

Objetivo: limitar o acesso à informação e aos recursos de processamento da informação.

Esse objetivo é dividido em **dois controles**:

9.1.1. Política de Controle de Acesso

Controle: convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.

9.1.2. Acesso às Redes e aos Serviços de Rede

Controle: convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

9.2. GERENCIAMENTO DE ACESSO DO USUÁRIO

Objetivo: assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.

Esse objetivo é dividido em **seis controles**:

9.2.1. Registro e Cancelamento de Usuário

Controle: convém que um processo formal de registro e cancelamento de usuários seja implementado para permitir atribuição dos direitos de acesso.

9.2.2. Provisionamento para Acesso de Usuário

Controle: convém que um processo formal de provisionamento de acesso do usuário seja implementado para conceder ou revogar os direitos de acesso do usuário para todos os tipos de usuários em todos os tipos de sistemas e serviços.

9.2.3. Gerenciamento de Direitos de Acesso Privilegiados

Controle: convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados.

9.2.4. Gerenciamento da Informação de Autenticação Secreta de Usuários

Controle: convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal.

9.2.5. Análise Crítica dos Direitos de Acesso de Usuário

Controle: convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.

9.2.6. Retirada ou Ajuste dos Direitos de Acesso

Controle: convém que os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos e/ou acordos, ou ajustados após a mudança destas atividades.

9.3. RESPONSABILIDADES DOS USUÁRIOS

Objetivo: tornar os usuários responsáveis pela proteção das suas informações de autenticação.

Esse objetivo possui um **único controle**.

9.3.1. Uso da Informação e Autenticação Secreta

Controle: convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.

9.4. CONTROLE DE ACESSO AO SISTEMA E À APLICAÇÃO

Objetivo: prevenir o acesso não autorizado aos sistemas e aplicações.

Esse objetivo é dividido em **cinco controles**.

9.4.1. Restrição de Acesso à Informação

Controle: convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso.

9.4.2. Procedimentos Seguros de Entrada no Sistema (Log-On)

Controle: convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema (log-on).

9.4.3. Sistema de Gerenciamento de Senha

Controle: convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.

9.4.4. Uso de Programas Utilitários Privilegiados

Controle: convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado.

9.4.5. Controle de Acesso ao Código-Fonte de Programas

Controle: convém que o acesso ao código-fonte de programa seja restrito.

Nesse sentido, convém que:

- o **acesso ao código-fonte de programas e de itens associados** (como desenhos, especificações) sejam **estritamente controlados**;
- para os **códigos-fonte de programas**, seja implementada **guarda centralizada do código**;
- seja **evitado** manter as **bibliotecas de programa-fonte** no **mesmo ambiente** dos **sistemas operacionais**;
- seja **implementado o controle** do programa-fonte e das bibliotecas de programa-fonte;

- o pessoal de **suporte** não tenha **acesso irrestrito** às **bibliotecas de programa-fonte**;
- a **atualização** das **bibliotecas de programa-fonte** e itens associados, e a **entrega de fontes** de programas a programadores sejam **apenas** efetuadas **após** o recebimento da **autorização** pertinente;
- as **listagens** dos **programas** sejam mantidas em um **ambiente seguro**;
- seja mantido um **registro de auditoria** de todos os **acessos a código-fonte** de programas;
- a **manutenção** e a cópia das bibliotecas de **programa-fonte** estejam **sujeitas** a procedimentos estritos de **controles de mudanças**.

10. CRIPTOGRAFIA

10. Criptografia.

10.1 Controles criptográficos.

10.1.1 Política para o uso de controles criptográficos.

10.1.2 Gerenciamento de chaves.

DIRETO DO CONCURSO

001. (FGV/TCE-SE/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/SEGURANÇA DA INFORMAÇÃO/2015) Com relação à norma ISO/IEC 27002:2013, está correto afirmar que:

- a) ela indica a necessidade do uso do ciclo PDCA nos processos da organização;
- b) a revisão de 2013 criou uma seção específica para controles criptográficos;
- c) não é mais necessário o gerenciamento de ativos, cuja cláusula foi suprimida na revisão de 2013;
- d) organizações agora podem ser certificadas na última revisão (2013) da ISO 27002;
- e) ela tem foco no gerenciamento de risco na segurança da informação.



Foi criada na norma ABNT NBR ISO/IEC 27002:2013 uma seção específica para **controles criptográficos (seção 10.1)**, com o objetivo de assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

Seções

Seção	ISO/IEC 27002: 2013
Seção	ISO/IEC 27002: 2005
5	Política de Segurança da Informação
6	Organizando a Segurança da Informação
7	Gerenciamento de Ativos
8	Segurança em Recursos Humanos
9	Segurança Física e do Ambiente
10	Gestão de Operações e Comunicações
11	Controle de Acesso
12	Aquisição, Desenvolvimento e Manutenção de SI
13	Gerenciamento de Incidentes de SI
14	Gerenciamento da Continuidade do Negócio
15	Conformidade
5	Política de Segurança da Informação
6	Organizando a Segurança da Informação
7	Gerenciamento de Ativos
8	Segurança em Recursos Humanos
9	Controle de Acesso
10	Criptografia
11	Segurança Física e do Ambiente
12	Segurança das Operações
13	Comunicação de Segurança
14	Aquisição, Desenvolvimento e Manutenção de SI
15	Relacionamento com Fornecedor
16	Gerenciamento de Incidentes de SI
17	Aspectos da segurança da informação no BCM
18	Conformidade

Conforme visto na tabela seguinte, a norma contém **14 seções** de controles de segurança da informação de um total de **35 objetivos de controles** e **114 controles**.

Letra b.

10.1. CONTROLES CRIPTOGRÁFICOS

Objetivo: Assegurar o **uso efetivo e adequado da criptografia** para proteger a **confidencialidade, autenticidade** e/ou a **integridade** da informação.

Esse objetivo é dividido em **dois controles**:

10.1.1. Política para o Uso de Controles Criptográficos

Controle: convém que seja desenvolvida e implementada uma **política** para o **uso de controles criptográficos** para a proteção da informação.

Diretrizes para implementação. Quando do desenvolvimento de uma política para criptografia, convém que sejam considerados:

- **A abordagem da Direção quanto ao uso de controles criptográficos** em toda a organização, incluindo os princípios gerais sob os quais as informações de negócios sejam protegidas;
- **A identificação do nível requerido de proteção** com base em uma avaliação de risco, levando em consideração o tipo, a força e a qualidade do algoritmo de criptografia requerido;

- O uso de criptografia para a proteção de informações sensíveis transportadas em dispositivos móveis, mídias removíveis ou através de linhas de comunicação;
- A abordagem do gerenciamento de chaves, incluindo métodos para lidar com a proteção das chaves criptográficas e a recuperação de informações cifradas, no caso de chaves perdidas, comprometidas ou danificadas;
- Papéis e responsabilidades, por exemplo, de quem for responsável:
 - pela implementação da política;
 - pelo gerenciamento de chaves, incluindo sua geração.
- Os padrões a serem adotados para a efetiva implementação ao longo de toda a organização (qual solução é usada para quais processos de negócios);
- O impacto do uso de informações cifradas em controles que dependem da inspeção de conteúdos (por exemplo, detecção de *malware*).

Convém que sejam consideradas na implementação da política criptográfica da organização, **as leis ou regulamentações e restrições nacionais** aplicáveis ao uso de técnicas criptográficas, nas diferentes partes do mundo, e das questões relativas ao fluxo transfronteiriças de informações cifradas.

Convém que **controles de criptografia** sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

Controles criptográficos podem ser usados para alcançar diferentes objetivos de segurança, como por exemplo:

- **Confidencialidade**: usando a criptografia da informação para proteger informações sensíveis ou críticas, armazenadas ou transmitidas;
- **Integridade/autenticidade**: usando assinaturas digitais ou códigos de autenticação de mensagens (MAC) para verificar a autenticidade ou integridade de informações sensíveis ou críticas, armazenadas ou transmitidas;
- **Não repúdio**: usando técnicas de criptografia para obter evidência da ocorrência ou não ocorrência de um evento ou ação.
- **Autenticação**: usando técnicas criptográficas para autenticar usuários e outros sistemas que requeiram acesso para transações com usuários de sistemas, entidades e recursos.

Informações adicionais: convém que a tomada de decisão quanto a uma solução de criptografia ser apropriada, seja vista como parte de processos mais amplos de avaliação de riscos e seleção de controles. **Essa avaliação pode, então, ser usada para determinar se um controle criptográfico é apropriado, que tipo de controle convém ser aplicado e para qual propósito e processos de negócio.**

Uma política sobre o uso de controles criptográficos é necessária para maximizar os benefícios, minimizar os riscos do uso de técnicas criptográficas e para evitar o uso incorreto ou inapropriado.

Convém que seja buscada a **opinião de um especialista para identificar os controles criptográficos adequados** para atender os objetivos da Política de Segurança da Informação.

10.1.2. Gerenciamento de Chaves

Controle: convém que uma **política** sobre o **uso, proteção e ciclo de vida das chaves criptográficas**, seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.

Diretrizes para implementação. Convém que a política inclua **requisitos para o gerenciamento de chaves criptográficas** ao longo de todo o seu ciclo de vida incluindo, a geração, armazenagem, arquivo, recuperação, distribuição, retirada e destruição das chaves.

Algoritmos criptográficos, tamanho de chaves e práticas usuais sejam selecionados de acordo com as melhores práticas.

Todas as chaves criptográficas sejam protegidas contra modificação e perda. Adicionalmente, chaves secretas e privadas necessitam de proteção contra o uso ou a divulgação não autorizada.

É recomendável que os **equipamentos utilizados para gerar, armazenar e guardar as chaves sejam fisicamente protegidos**.

Convém que um **sistema de gerenciamento de chaves** seja baseado em um conjunto estabelecido de normas, procedimentos e métodos seguros para:

- **Gerar chaves** para diferentes sistemas criptográficos e diferentes aplicações;
- **Gerar e obter certificados de chaves públicas;**
- **Distribuir chaves** para os usuários devidos, incluindo a forma como as chaves são ativadas, quando recebidas;
- **Armazenar chaves**, incluindo a forma como os usuários autorizados obtêm acesso a elas;
- **Mudar ou atualizar chaves**, incluindo regras quando as chaves são mudadas e como isto deve ser conduzido;
- **Lidar com chaves comprometidas;**
- **Revogar chaves**, incluindo regras de como elas são retiradas ou desativadas, por exemplo, quando chaves tiverem sido comprometidas ou quando um usuário deixa a organização (é recomendável, também neste caso, que as chaves sejam guardadas);
- **Recuperar chaves perdidas ou corrompidas;**
- **Realizar cópias de segurança ou guardar as chaves;**
- **Destruir chaves;**
- **Manter registro e auditoria das atividades relacionadas com o gerenciamento de chaves.**

Para reduzir a possibilidade de comprometimento, convém que as **datas de ativação e desativação de chaves** sejam definidas de forma que possam ser utilizadas apenas por um período de tempo definido na política de gerenciamento de chaves.

Além do gerenciamento seguro de chaves secretas e privadas, convém que a **autenticidade de chaves públicas seja considerada**. Este processo de **autenticação** pode ser conduzido utilizando-se certificados de chaves públicas que são normalmente emitidos por uma **autoridade certificadora**, a qual recomenda-se que seja uma organização reconhecida, com controles adequados e procedimentos implantados com o objetivo de garantir o requerido nível de confiança.

Convém que os **conteúdos dos acordos de nível de serviço ou dos contratos com fornecedores externos de serviços criptográficos**, como por exemplo, com uma autoridade certificadora, **cubra aspectos como responsabilidades, confiabilidade dos serviços e tempos de resposta** para a execução dos serviços contratados.

Informações adicionais: a gestão de chaves criptográficas é essencial para o uso eficaz de técnicas criptográficas.

Técnicas criptográficas podem ser também utilizadas para proteger chaves criptográficas. Pode ser necessário o estabelecimento de procedimentos para o manuseio de solicitações legais para acesso a chaves criptográficas, por exemplo, a disponibilização de informação cifrada pode ser requerida em sua forma decifrada para uso como evidência em um processo judicial.

11. SEGURANÇA FÍSICA E DO AMBIENTE

11. Segurança física e do ambiente.

11.1 Áreas seguras.

- 11.1.1 Perímetro de segurança física.
- 11.1.2 Controles de entrada física.
- 11.1.3 Segurança em escritórios, salas e instalações.
- 11.1.4 Proteção contra ameaças externas e do meio ambiente.
- 11.1.5 Trabalhando em áreas seguras.
- 11.1.6 Áreas de entrega e de carregamento.

11.2 Equipamentos.

- 11.2.1 Escolha do local e proteção do equipamento.
- 11.2.2 Utilidades.
- 11.2.3 Segurança do cabeamento.
- 11.2.4 Manutenção dos equipamentos.
- 11.2.5 Remoção de ativos.
- 11.2.6 Segurança de equipamentos e ativos fora das dependências da organização.
- 11.2.7 Reutilização e alienação segura de equipamentos.
- 11.2.8 Equipamento de usuário sem monitoração.
- 11.2.9 Política de mesa limpa e tela limpa.

Esta Seção possui **dois objetivos**.

11.1. ÁREAS SEGURAS

Objetivo: prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.

Esse objetivo é dividido em **seis controles**:

11.1.1. Perímetro de Segurança Física

Controle: convém que perímetros de segurança sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis.

Diretrizes para implementação:

Convém que as diretrizes seguintes sejam consideradas e implementadas, onde apropriado, para os perímetros de segurança física.

Convém que:

- Os **perímetros de segurança sejam claramente definidos** e que a localização e a capacidade de resistência de cada perímetro dependam dos requisitos de segurança dos ativos existentes no interior do perímetro, e dos resultados da avaliação de riscos;
- Os **perímetros de um edifício ou de um local que contenha as instalações de processamento da informação** sejam **fisicamente sólidos**: o perímetro não deve ter brechas nem pontos onde poderia ocorrer facilmente uma invasão); as **paredes externas do local devem ser de construção robusta** e todas as portas externas sejam adequadamente protegidas contra acesso não autorizado por meio de mecanismos de controle, por exemplo, barras, alarmes, fechaduras etc.; **as portas e janelas sejam trancadas quando estiverem sem monitoração**, e que uma **proteção externa para as janelas** seja considerada, principalmente para as que estiverem situadas no andar térreo;
- Seja implantada uma área de recepção, ou um outro meio para controlar o acesso físico ao local ou ao edifício; o acesso aos locais ou edifícios deve ficar restrito somente ao pessoal autorizado;
- Sejam construídas **barreiras físicas**, onde aplicável, para impedir o acesso físico não autorizado e a contaminação do meio ambiente;
- Todas as **portas corta-fogo do perímetro de segurança sejam providas de alarme, monitoradas e testadas juntamente com as paredes**, para estabelecer o nível de resistência exigido, de acordo com normas regionais, nacionais e internacionais aceitáveis; elas devem funcionar de acordo com os códigos locais de prevenção de incêndios e prevenção de falhas;

**Figura – Portas Corta-Fogo**

- **Sistemas adequados de detecção de intrusos**, de acordo com normas regionais, nacionais e internacionais sejam instalados e testados em intervalos regulares, e cubram todas as portas externas e janelas acessíveis; as áreas *não ocupadas* sejam protegidas por alarmes o tempo todo; também seja dada **proteção a outras áreas**, por exemplo, salas de computadores ou salas de comunicações;
- As instalações de processamento da informação gerenciadas pela organização fiquem **fisicamente separadas** daquelas que são gerenciadas por partes externas.

Informações adicionais: pode-se obter proteção física criando uma ou mais barreiras físicas ao redor das instalações e dos recursos de processamento da informação da organização.

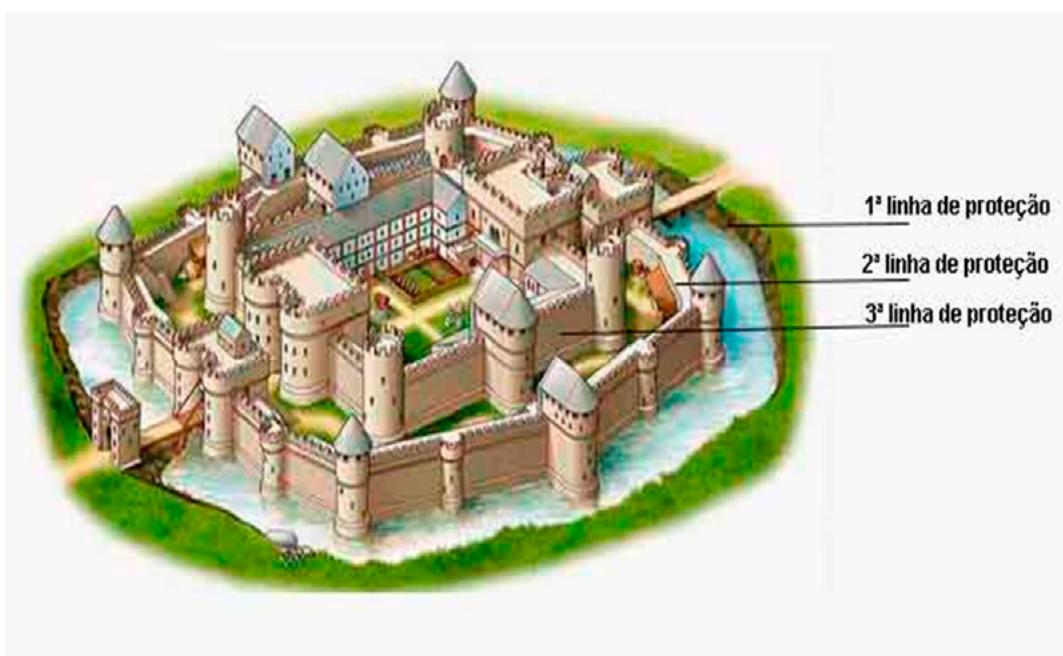


Figura 2 – Perímetros de Segurança Física (GOOGLE, 2016)

O uso de **barreiras múltiplas** proporciona uma proteção adicional, uma vez que neste caso a falha de uma das barreiras não significa que a segurança fique comprometida imediatamente.

Uma área segura pode ser um escritório trancável ou um conjunto de salas rodeado por uma barreira física interna contínua de segurança.

Pode haver necessidade de barreiras e perímetros adicionais para o controle do acesso físico, quando existem áreas com requisitos diferentes de segurança dentro do perímetro de segurança.

Sejam tomadas precauções especiais para a segurança do acesso físico no caso de edifícios que alojam diversas organizações.

A aplicação de controles físicos, especialmente para as áreas seguras sejam adaptadas para as circunstâncias técnicas e econômicas da organização, como definido na avaliação de riscos.

11.1.2. Controles de Entrada Física

Controle: convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.

Diretrizes para implementação:

Diretrizes a serem consideradas - Convém que:

- A **data e hora da entrada e saída de visitantes sejam registradas**, e todos os **visitantes sejam supervisionados**, a não ser que o seu acesso tenha sido previamente aprovado; as permissões de acesso só sejam concedidas para finalidades específicas e autorizadas, e sejam emitidas com instruções sobre os requisitos de segurança da área e os procedimentos de emergência. A identidade dos visitantes seja autenticada por meios apropriados;

- O acesso às áreas em que são processadas ou armazenadas informações sensíveis seja restrito apenas ao pessoal autorizado pela implementação de controles de acesso apropriados, por exemplo, mecanismos de autenticação de dois fatores, como, cartões de controle de acesso e PIN (*personal identification number*);
- Uma trilha de auditoria eletrônica ou um livro de registro físico de todos os acessos seja mantida e monitorada de forma segura;
- Seja exigido que todos os funcionários, fornecedores e partes externas, e todos os visitantes, tenham alguma forma visível de identificação, e que eles avisem imediatamente ao pessoal de segurança, caso encontrem visitantes não acompanhados ou qualquer pessoa que não esteja usando uma identificação visível;
- Às partes externas que realizam serviços de suporte, convém que seja concedido acesso restrito às áreas seguras ou as instalações de processamento da informação sensíveis, somente quando necessário; este acesso seja autorizado e monitorado;
- Os direitos de acesso a áreas seguras sejam revistos e atualizados em intervalos regulares, e revogados quando necessário.

11.1.3. Segurança em Escritórios, Salas e Instalações

Controle: convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.

Diretrizes para implementação. Veja a seguir as diretrizes a serem consideradas para a proteção de escritórios, salas e instalações. Convém que:

- As **instalações-chave** sejam localizadas de maneira a evitar o acesso do público;
- Quando for aplicável, os **edifícios** sejam **discretos** com a menor indicação possível da sua finalidade, sem letreiros evidentes, fora ou dentro do edifício, que identifiquem a presença de atividades de processamento de informações;
- As **instalações** sejam projetadas para evitar que as informações confidenciais ou as atividades sejam visíveis e possam ser ouvidas da parte externa. Convém que proteção eletromagnética também seja considerada, conforme apropriado.
- As **listas de funcionários e guias telefônicos internos**, que identifiquem a localização das instalações que processam informações sensíveis, **não** fiquem facilmente acessíveis a qualquer pessoal não autorizada.

11.1.4. Proteção Contra Ameaças Externas e do Meio-Ambiente

Controle: convém que **sejam** projetadas e aplicadas proteção física contra desastres naturais, ataques maliciosos ou acidentes.

Diretrizes para implementação. Convém que orientações de especialistas sejam obtidas sobre como evitar danos oriundos de:

- Fogo;
- Inundação;

- Terremoto;
- Explosão;
- Manifestações civis;
- Outras formas de desastre natural ou provocado pela natureza.

11.1.5. Trabalhando em Áreas Seguras

Controle: convém que seja **projeto e aplicado procedimentos para o trabalho em áreas seguras.**

Diretrizes para implementação. Veja as diretrizes a serem consideradas - Convém que:

- O pessoal só tenha conhecimento da existência de áreas seguras ou das atividades nelas realizadas, apenas se for necessário;
- Seja evitado o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para prevenir as atividades mal-intencionadas;
- As áreas seguras, não ocupadas, sejam fisicamente trancadas e periodicamente verificadas;
- Não seja permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado.
- As normas para o trabalho em áreas seguras incluem o controle dos funcionários, fornecedores e partes externas que trabalham em tais áreas, cubram todas as atividades nestas áreas.

11.1.6. Áreas de Entrega e de Carregamento

Controle: convém que pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.

Diretrizes para implementação. Diretrizes a serem consideradas - Convém que:

- O acesso a uma área de entrega e carregamento a partir do exterior do prédio fique restrito ao pessoal identificado e autorizado;
- As áreas de entrega e carregamento sejam projetadas de tal maneira que seja possível carregar e descarregar suprimentos sem que os entregadores tenham acesso a outras partes do edifício;
- As portas externas de uma área de entrega e carregamento sejam protegidas enquanto as portas internas estiverem abertas;
- Os materiais entregues sejam inspecionados e examinados para detectar a presença de explosivos, materiais químicos ou outros materiais perigosos, antes de serem transportados da área de entrega e carregamento para o local de utilização;
- Os materiais entregues sejam registrados de acordo com os procedimentos de gerenciamento de ativos, por ocasião da sua entrada no local;

- As remessas entregues sejam segregadas fisicamente das remessas que saem, sempre que possível;
- Os materiais entregues sejam inspecionados para evidenciar alteração indevida.

Caso alguma alteração indevida seja descoberta, ela deve ser imediatamente notificada ao pessoal da segurança.

11.2. EQUIPAMENTO

Objetivo: impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das operações da organização.

Esse objetivo é dividido em nove controles:

11.2.1. Escolha do Local e Proteção do Equipamento

Controle: convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

Diretrizes para implementação. Diretrizes a serem consideradas para a proteção dos equipamentos - Convém que:

- Os equipamentos sejam colocados no local, a fim de minimizar o acesso desnecessário às áreas de trabalho;
- As instalações de processamento da informação que manuseiam dados sensíveis sejam posicionadas cuidadosamente para reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante a sua utilização;
- As instalações de armazenagem sejam protegidas de forma segura para evitar acesso não autorizado;
- Os itens que exigem proteção especial sejam protegidos para reduzir o nível geral de proteção necessário;
- Sejam adotados controles para minimizar o risco de ameaças físicas potenciais e ambientais, tais como furto, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;
- Sejam estabelecidas diretrizes quanto a comer, beber e fumar nas proximidades das instalações de processamento da informação;
- As condições ambientais, como temperatura e umidade, sejam monitoradas para a detecção de condições que possam afetar negativamente as instalações de processamento da informação;

- Todos os edifícios sejam dotados de **proteção contra raios** e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;
- Para equipamentos em ambientes industriais, é recomendado considerar o uso de métodos especiais de proteção, como membranas para teclados;
- Os equipamentos que processam informações sensíveis sejam protegidos, a fim de minimizar o risco de vazamento de informações em decorrência de emanações eletromagnéticas.

11.2.2. Utilidades

Controle: convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

Diretrizes para implementação - Convém que:

- Todas as utilidades (como suprimento de energia elétrica, telecomunicações, suprimento de água, gás, esgoto, calefação/ventilação e ar-condicionado):
 - Estejam em conformidade com as especificações do fabricante do equipamento e com os requisitos legais da localidade;
 - Sejam avaliadas regularmente quanto à sua capacidade para atender ao crescimento do negócio e às interações com outras utilidades;
 - Sejam inspecionadas e testadas regularmente para assegurar o seu adequado funcionamento;
 - Seja alarmada para detectar mau funcionamento, quando necessário;
 - Tenham múltiplas alimentações com rotas físicas diferentes;
- Seja providenciada iluminação e comunicação de **emergência**.

As chaves de emergência (switches) e válvulas para o corte de energia, água, gás ou outras utilidades, sejam localizadas próximo das saídas de emergência ou salas de equipamentos.

Informações adicionais:

Redundância adicional para conectividade em rede pode ser obtida por meio de múltiplas rotas de mais de um provedor de utilidades.

DIRETO DO CONCURSO

002. (CESPE/TJ-CE/ANALISTA JUDICIÁRIO/CIÊNCIAS DA COMPUTAÇÃO/2014) O uso de equipamentos de UPS (*uninterruptible power supply*), considerados fornecedores de energia elétrica secundários, é recomendado, de acordo com a norma ABNT NBR ISO/IEC 27.002, para o controle

a) da segurança em escritórios, salas e instalações.

- b) de trabalho em áreas seguras.
- c) de áreas seguras.
- d) do perímetro de segurança física.
- e) da segurança de equipamentos.



A norma ABNT NBR ISO/IEC 27.002/2013 destaca em 11.2.2 – Utilidades - o seguinte **Controle**:

Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

A proteção, neste caso, pode ser feita com uso de equipamento UPS (*uninterruptible power supply*), para o controle da segurança de equipamentos.

Letra e.

11.2.3. Segurança do Cabeamento

Controle: convém que o **cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos.**

Diretrizes para implementação. Convém que:

- As linhas de energia e de telecomunicações que entram nas instalações de processamento da informação sejam subterrâneas (ou fiquem abaixo do piso) sempre que possível, ou recebam uma proteção alternativa adequada;
- Os cabos de energia sejam segregados dos cabos de comunicações, para evitar interferências;
- Para sistemas sensíveis ou críticos, os seguintes controles adicionais, sejam considerados:
 - Instalação de conduítes blindados e salas ou caixas trancadas em pontos de inspeção e pontos terminais;
 - Utilização de blindagem eletromagnética para a proteção dos cabos;
 - Realização de varreduras técnicas e inspeções físicas para detectar a presença de dispositivos não autorizados conectados aos cabos;
 - Acesso controlado aos painéis de conexões e às salas de cabos.

11.2.4. Manutenção dos Equipamentos

Controle: convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente.

Diretrizes para implementação. Convém que:

- A manutenção dos equipamentos seja realizada nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações;
- A manutenção e os consertos dos equipamentos só sejam realizados por pessoal de manutenção autorizado;
- Sejam mantidos registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas;
- Sejam implementados controles apropriados, na época programada para a manutenção do equipamento, dependendo de a manutenção ser realizada pelo pessoal local ou por pessoal externo à organização; **onde necessário, que informações sensíveis sejam eliminadas do equipamento, ou o pessoal de manutenção seja de absoluta confiança;**
- Sejam atendidas todas as exigências de manutenção estabelecidas nas apólices de seguro;
- Antes de colocar o equipamento em operação, após a sua manutenção, convém que ele seja inspecionado para garantir que o equipamento não foi alterado indevidamente e que não está em mau funcionamento.

11.2.5. Remoção de Ativos

Controle: convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.

Diretrizes para implementação:

- Sejam claramente **identificados os funcionários, fornecedores e partes externas** que tenham autoridade para permitir a remoção de ativos para fora do local;
- Sejam estabelecidos **limites de tempo para a retirada de equipamentos do local**, e a **devolução seja controlada**;
- Sempre que necessário ou apropriado, é recomendado que seja feito um registro da retirada e da devolução de ativos, quando do seu retorno;
- A identidade, atribuição e função de qualquer pessoa que manuseia ou utiliza os ativos estejam documentados, e que esta documentação seja devolvida com o equipamento, a informação ou software.

Informações adicionais: podem ser feitas inspeções aleatórias para detectar a retirada não autorizada de ativos e a existência de equipamentos de gravação não autorizados, armas etc., e impedir sua entrada e saída do local.

Convém que:

- Tais inspeções aleatórias sejam feitas de acordo com a legislação e as normas aplicáveis;
- As pessoas sejam avisadas da realização das inspeções, e elas só possam ser feitas com a devida autorização, levando em conta as exigências legais e regulamentares.

11.2.6. Segurança de Equipamentos e Ativos Fora das Dependências da Organização

Controle: convém que **sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.**

Diretrizes para implementação. Convém que o uso de qualquer equipamento de processamento e armazenamento de informações fora das dependências da organização seja autorizado pela gerência. **Isto se aplica aos próprios equipamentos da organização e aos equipamentos pessoais, usados em nome da organização.**

Convém que as seguintes diretrizes sejam adotadas para proteção de equipamentos usados **fora** das dependências da organização:

- os equipamentos e mídias removidos das dependências da organização não fiquem sem supervisão em lugares públicos;
- sejam observadas a qualquer tempo as instruções do fabricante para a proteção do equipamento, por exemplo, proteção contra a exposição a campos eletromagnéticos intensos;
- os controles para as localidades fora das dependências da organização, como, o trabalho em casa e localidades remotas e temporárias, sejam determinados por uma avaliação de riscos, devendo ser aplicados controles adequados para cada caso, por exemplo, arquivos trancáveis, **política de “mesa limpa”**, controles de acesso a computadores, e comunicação segura com o escritório;
- quando o equipamento fora das dependências da organização é transferido entre diferentes pessoas ou partes externas, convém que seja mantido um registro para definir a **cadeia de custódia** do equipamento, incluindo pelo menos os nomes e organizações daqueles que são responsáveis pelo equipamento.

EVIDÊNCIA ELETRÔNICA				
FORMULÁRIO DE CADEIA DE CUSTÓDIA				
Caso Num.:	Pag.:			
De:				
MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO				
Item: <input type="text"/>	Descrição: <input type="text"/>			
Fabricante: <input type="text"/>	Modelo: <input type="text"/>	Num. de serie: <input type="text"/>		
DETALHES SOBRE A IMAGEM DOS DADOS				
Data/Hora: <input type="text"/>	Criada por: <input type="text"/>	Método usado: <input type="text"/>	Nome da Imagem: <input type="text"/>	Partes: <input type="text"/>
Drive: <input type="text"/>	HASH: <input type="text"/>			
CADEIA DE CUSTÓDIA				
Destino:	Data/Hora:	Origem:	Destino	Motivo:
	Data: <input type="text"/>	Nome/Org.: <input type="text"/>	Nome/Org.: <input type="text"/>	
	Hora: <input type="text"/>	Assinatura: <input type="text"/>	Assinatura: <input type="text"/>	
	Data: <input type="text"/>	Nome/Org.: <input type="text"/>	Nome/Org.: <input type="text"/>	
	Hora: <input type="text"/>	Assinatura: <input type="text"/>	Assinatura: <input type="text"/>	
	Data: <input type="text"/>	Nome/Org.: <input type="text"/>	Nome/Org.: <input type="text"/>	
	Hora: <input type="text"/>	Assinatura: <input type="text"/>	Assinatura: <input type="text"/>	
	Data: <input type="text"/>	Nome/Org.: <input type="text"/>	Nome/Org.: <input type="text"/>	
	Hora: <input type="text"/>	Assinatura: <input type="text"/>	Assinatura: <input type="text"/>	
	Data: <input type="text"/>	Nome/Org.: <input type="text"/>	Nome/Org.: <input type="text"/>	
	Hora: <input type="text"/>	Assinatura: <input type="text"/>	Assinatura: <input type="text"/>	

Figura 3 – Formulário de Cadeia de Custódia (FDTK, 2015)

Os riscos de segurança, por exemplo, de danos, furto ou espionagem, podem variar consideravelmente de um local para outro, e convém que sejam levados em conta para determinar os controles mais apropriados.

Informações adicionais: os equipamentos de armazenagem e processamento de informações incluem todas as formas de computadores pessoais, agendas eletrônicas, telefones celulares, cartões inteligentes, papéis e outros tipos, utilizados no trabalho em casa, ou que são removidos do local normal de trabalho.

Recomenda-se evitar o risco, desencorajando os funcionários de trabalharem fora das instalações da organização, ou restringindo o uso de dispositivos móveis.

11.2.7. Reutilização e Alienação Segura de Equipamentos

Controle: convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre gravados com segurança, antes do descarte ou do seu uso.

Diretrizes para implementação. Convém que:

- Os equipamentos sejam inspecionados para verificar se a mídia está ou não armazenada, antes do descarte ou reutilização;
- As mídias de armazenamento que contém informações confidenciais ou de direitos autorais sejam destruídas fisicamente, ou as informações sejam destruídas, apagadas ou sobre gravadas por meio de técnicas que tornem as informações originais irrecuperáveis, em vez de se usarem as funções-padrão de apagar ou formatar.

Informações adicionais: no caso de dispositivos defeituosos que contenham informações sensíveis, pode ser necessária uma avaliação de riscos para determinar se convém destruir fisicamente o dispositivo em vez de mandá-lo para o conserto ou descartá-lo.

As informações podem ser comprometidas por um descarte feito sem os devidos cuidados ou pela reutilização do equipamento.

Adicionalmente à remoção segura das informações contidas no disco, a encriptação completa do disco reduz o risco de revelação de informação confidencial quando o equipamento é descartado ou reparado considerando que:

- O processo de encriptação é suficientemente robusto e cobre o disco por completo;
- As chaves criptográficas são de um tamanho considerável para resistir um ataque de força bruta;
- As chaves criptográficas são guardadas de forma confidencial (por exemplo, nunca armazenada no mesmo disco).

Técnicas para sobregravar de forma segura as mídias armazenadas, diferem em função da tecnologia usada para armazenar a mídia. Convém que ferramentas usadas para sobregravar sejam analisadas criticamente para assegurar que elas são aplicáveis à tecnologia usada para o armazenamento da mídia.

11.2.8. Equipamento de Usuário Sem Monitoração

Controle: convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.

Diretrizes para implementação. Convém que:

- Todos os usuários estejam cientes dos requisitos de segurança da informação e procedimentos para proteger equipamentos desacompanhados, assim como suas responsabilidades por implementar estas proteções;

- Os usuários sejam informados para:
 - Encerrar as sessões ativas, a menos que elas possam ser protegidas por meio de um mecanismo de bloqueio;
 - Efetuar a desconexão de serviços de rede ou aplicações, quando não for mais necessário;
 - Proteger os computadores ou dispositivos móveis contra uso não autorizado através de tecla de bloqueio ou outro controle equivalente.

11.2.9. Política de Mesa Limpa e Tela Limpa

Controle: convém que seja adotada uma **política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.**

Diretrizes para implementação. Convém que uma política de mesa limpa e tela protegida leve em consideração a classificação da informação, requisitos contratuais e legais, e o risco correspondente e aspectos culturais da organização.

As seguintes diretrizes sejam consideradas - Convém que:

- As informações do negócio sensíveis ou críticas sejam guardadas em lugar seguro (ide-almente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando o escritório está desocupado;
- Os computadores e terminais sejam mantidos desligados ou protegidos com **mecanismo de travamento de tela e teclados controlados por senha, token ou mecanismo de autenticação similar quando sem monitoração e protegida por tecla de bloqueio, senhas ou outros controles, quando não usados;**
- Sejam evitados o uso não autorizado de fotocopiadoras e outra tecnologia de reprodução;
- Os documentos que contêm informação sensível ou classificada sejam removidos de impressoras imediatamente.

Informações adicionais: uma política de mesa limpa e tela protegida reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho. Cofres e outras formas de recursos de armazenamento seguro também podem proteger informações armazenadas contra desastres como incêndio, terremotos, enchentes ou explosão.

Considerar o uso de impressoras com função de código PIN, permitindo dessa forma que os requerentes sejam os únicos que podem pegar suas impressões, e apenas quando estiverem próximas às impressoras.

Contribuindo para a segurança da sua organização (seja responsável!)

Mesa limpa e tela limpa:



"BARRY IS A FINE EXAMPLE OF THE SUCCESS OF OUR CLEAR DESK POLICY"

"Barry é um bom exemplo do sucesso da nossa política de mesa limpa"

Figura 4 – Mesa Limpa e Tela Limpa (Fonte: CAIS/RNP)

12. SEGURANÇA NAS OPERAÇÕES

12. Segurança nas operações.

12.1. Responsabilidades e procedimentos operacionais.

12.1.1. Documentação dos procedimentos de operação.

12.1.2. Gestão de mudanças.

12.1.3. Gestão de capacidade.

12.1.4. Separação dos ambientes de desenvolvimento, teste e produção.

12.2. Proteção contra malware.

12.2.1. Controles contra malware.

12.3. Cópias de Segurança.

12.3.1. Cópias de segurança das informações.

12.4. Registros e monitoramento.

12.4.1. Registros de eventos.

12.4.2. Proteção das informações dos registros de eventos (logs).

12.4.3. Registros de eventos (log) de administrador e operador.

12.4.4. Sincronização dos relógios.

12.5. Controle de software operacional.

12.5.1. Instalação de software nos sistemas operacionais.

12.6. Gestão de vulnerabilidades técnicas.

12.6.1. Gestão de vulnerabilidades técnicas.

12.6.2. Restrições quanto à instalação de software.

12.7. Considerações quanto à auditoria de sistemas da informação.

12.7.1. Controles de auditoria de sistemas de informação.

Esta Seção é dividida em **sete objetivos**.

12.1. RESPONSABILIDADES E PROCEDIMENTOS OPERACIONAIS

Objetivo: garantir a operação segura e correta dos recursos de processamento da informação.

Esse objetivo possui **quatro controles**:

12.1.1. Documentação dos Procedimentos de Operação

Controle: convém que os procedimentos de operação sejam documentados e disponibilizados para todos os usuários que necessitem deles.

12.1.2. Gestão de Mudanças

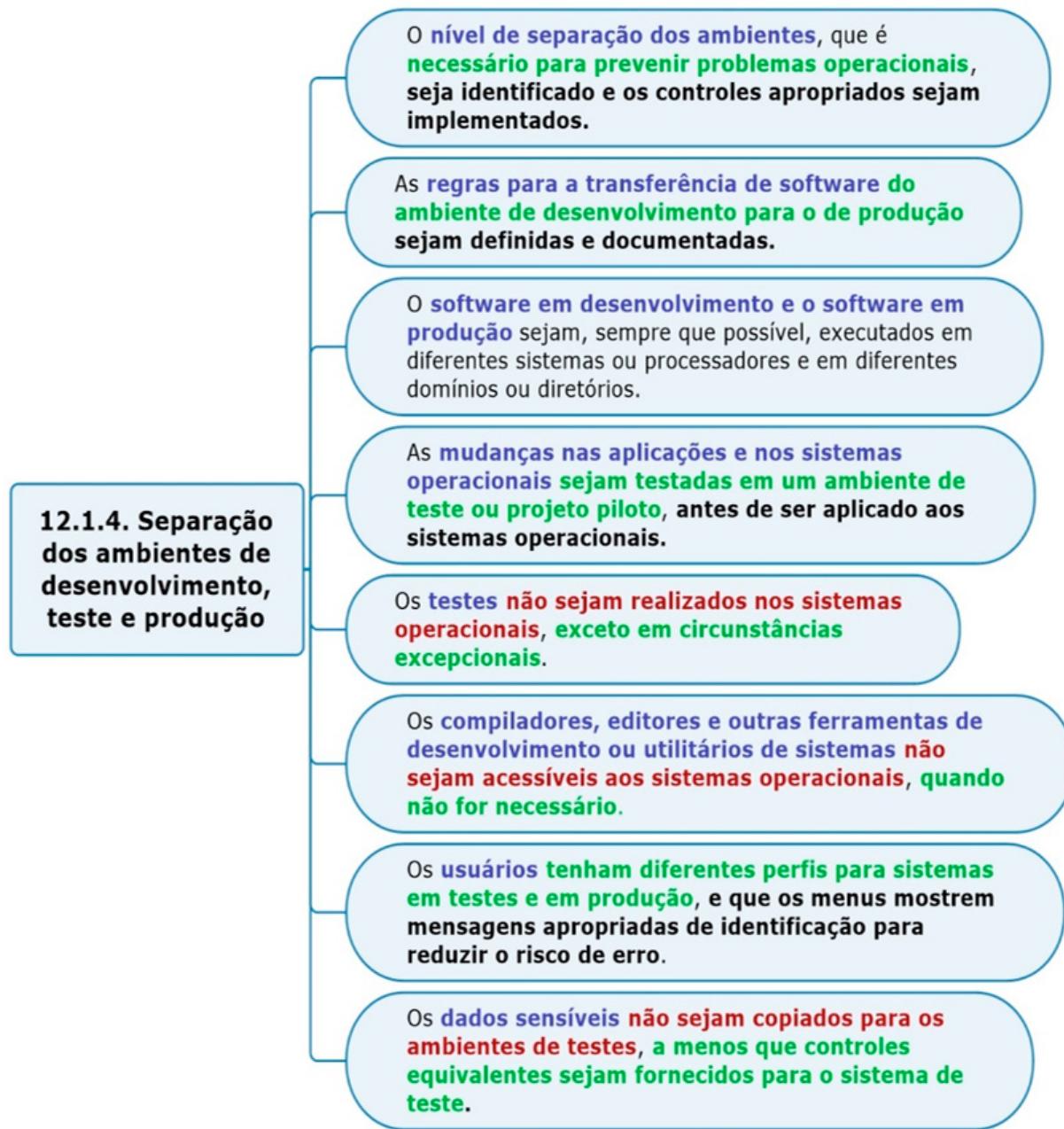
Controle: convém que mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas.

12.1.3. Gestão de capacidade

Controle: convém que a utilização dos recursos seja monitorada e ajustada, e que as projeções sejam feitas para a necessidade de capacidade futura para garantir o desempenho requerido do sistema.

12.1.4. Separação dos Ambientes de Desenvolvimento, Teste e Produção

Controle: convém que **ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.**



DIRETO DO CONCURSO

003. (FCC/TJ-MA/ANALISTA DE SISTEMAS/DESENVOLVIMENTO/2019) A norma ABNT NBR ISO/IEC 27002:2013 tem uma seção que trata da segurança de operações, cujo objetivo é garantir a operação segura e correta dos recursos de processamento da informação. Nesta seção, no que tange ao desenvolvimento, teste e produção de software, recomenda-se que

- a) softwares em desenvolvimento e softwares em produção sejam sempre executados no mesmo sistema, processador, domínio ou diretório.
- b) ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

- c) compiladores, editores e outras ferramentas de desenvolvimento sejam completamente acessíveis aos sistemas operacionais.
- d) usuários tenham um único perfil para sistemas de testes e em produção, para garantir que todos os aspectos desejados sejam testados.
- e) dados sensíveis sejam copiados e utilizados nos ambientes de teste, independente dos controles, para obter maior precisão nos resultados dos testes.



- a) Errada. De acordo com a norma ABNT NBR ISO/IEC 27002:2013 (p. 50), convém que **o software em desenvolvimento e o software em produção sejam, sempre que possível, executados em diferentes sistemas ou processadores e em diferentes domínios ou diretórios**.
- b) Certa. De acordo com a norma ABNT NBR ISO/IEC 27002:2013 (pág. 50), convém que **ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção**
- c) Errada. De acordo com a norma ABNT NBR ISO/IEC 27002:2013 (p. 51), convém que os compiladores, editores e outras ferramentas de desenvolvimento ou utilitários de sistemas **não** sejam acessíveis aos sistemas operacionais, quando não for necessário.
- d) Errada. De acordo com a norma ABNT NBR ISO/IEC 27002:2013 (p. 51), convém que usuários tenham **diferentes perfis** para sistemas em testes e em produção, e que os menus mostrem mensagens apropriadas de identificação para reduzir o risco de erro. Utilizar o mesmo perfil para os 2 casos seria uma grande vulnerabilidade de segurança.
- e) Errada. Segundo a norma ABNT NBR ISO/IEC 27002:2013 (p. 51), convém que dados sensíveis (como por exemplo, dados de cartão de crédito, senhas) **não** sejam copiados e utilizados nos ambientes de teste, a menos que controles equivalentes sejam fornecidos para o sistema de teste.

Letra b.

12.2. PROTEÇÃO CONTRA MALWARE

Objetivo: assegurar que as informações e os recursos de processamento da informação estão protegidos contra malware.

Esse objetivo possui **um único controle**.

12.2.1. Controles Contra Malware

Controle: convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário.

12.3. CÓPIAS DE SEGURANÇA

Objetivo: proteger contra perda de dados.

Esse objetivo possui **um único controle**.

12.3.1. Cópias de Segurança das Informações

Controle: convém que cópias de segurança das informações, dos softwares e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

12.4. REGISTROS E MONITORAMENTO

Objetivo: registrar eventos e gerar evidências.

Esse objetivo possui **quatro controles**:

12.4.1. Registros de Eventos

Controle: convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.

12.4.2. Proteção das Informações dos Registros de Eventos (Logs)

Controle: convém que as informações dos registros de eventos (log) e os seus recursos sejam protegidos contra acesso não autorizado e adulteração.

12.4.3. Registros de Eventos (Log) de Administrador e Operador

Controle: convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares.

12.4.4. Sincronização dos Relógios

Controle: convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa.

12.5. CONTROLE DE SOFTWARE OPERACIONAL

Objetivo: assegurar a integridade dos sistemas operacionais.

Esse objetivo possui **um único** controle.

12.5.1. Instalação de Software nos Sistemas Operacionais

Controle: convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados.

12.6. GESTÃO DE VULNERABILIDADES TÉCNICAS

Objetivo: prevenir a exploração de vulnerabilidade técnicas.

Esse objetivo possui **dois controles**:

12.6.1. Gestão de Vulnerabilidades Técnicas

Controle: convém que as informações sobre vulnerabilidades técnicas dos sistemas de informação em uso sejam obtidas em tempo hábil; convém que a exposição da organização a estas vulnerabilidades seja avaliada e que sejam tomadas as medidas apropriadas para lidar com os riscos associados.

12.6.2. Restrições quanto à Instalação de Software

Controle: convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários.

12.7. CONSIDERAÇÕES QUANTO À AUDITORIA DE SISTEMAS DA INFORMAÇÃO

Objetivo: minimizar o impacto das atividades de auditoria nos sistemas operacionais.

Esse objetivo possui **um único controle**.

12.7.1. Controles de Auditoria de Sistemas de Informação

Controle: convém que as atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.

13. SEGURANÇA NAS COMUNICAÇÕES

13. Segurança nas comunicações.

13.1. Gerenciamento da segurança em redes.

13.1.1. Controles de redes.

13.1.2. Segurança dos serviços de rede.

13.1.3. Segregação de redes.

13.2. Transferência de informação.

13.2.1. Políticas e procedimentos para transferência de informações.

13.2.2. Acordos para transferência de informações.

13.2.3. Mensagens eletrônicas.

13.2.4. Acordos de confidencialidade e não divulgação.

Esta Seção é dividida em **dois objetivos**.

13.1. GERENCIAMENTO DA SEGURANÇA EM REDES

Objetivo: assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam.

Esse objetivo é dividido em **três controles**:

13.1.1. Controles de Redes

Controle: convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

13.1.2. Segurança dos Serviços de Rede

Controle: convém que mecanismos de segurança, níveis de serviços e requisitos de gerenciamento de todos os serviços de rede sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.

13.1.3. Segregação de Redes

Controle: convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.

13.2. TRANSFERÊNCIA DE INFORMAÇÃO

Objetivo: manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

Esse objetivo é dividido em **quatro controles**:

13.2.1. Políticas e Procedimentos para Transferência de Informações

Controle: convém que políticas, procedimentos e controles de transferências formais sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.

13.2.2. Acordos para Transferência de Informações

Controle: convém que sejam estabelecidos acordos para transferência segura de informações do negócio entre a organização e as partes externas.

13.2.3. Mensagens Eletrônicas

Controle: convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.

13.2.4. Acordos de Confidencialidade e Não Divulgação

Controle: convém que os requisitos para confidencialidade ou acordos de não divulgação que refletem as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente.

14. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

14. Aquisição, desenvolvimento e manutenção de sistemas.

14.1. Requisitos de Segurança de sistemas de informação.

14.1.1. Análise e especificação dos requisitos de SI.

14.1.2. Serviços de aplicação seguros em redes públicas.

14.1.3. Protegendo as transações nos aplicativos de serviços.

14.2. Segurança em processos de desenvolvimento e de suporte.

14.2.1. Política de desenvolvimento seguro.

14.2.2. Procedimentos para controle de mudanças de sistemas.

14.2.3. Análise crítica técnica das aplicações após mudanças nas plataformas operacionais.

14.2.4. Restrições sobre mudanças em pacotes de software.

14.2.5. Princípios para projetar sistemas seguros.

14.2.6. Ambiente seguro para desenvolvimento.

14.2.7. Desenvolvimento terceirizado.

14.2.8. Teste de segurança do sistema.

14.2.9. Teste de aceitação de sistemas.

14.3 Dados para teste.

14.3.1. Proteção dos dados para teste.

Esta Seção é dividida em **três objetivos**.

14.1. REQUISITOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Objetivo: garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviço sobre as redes públicas.

Esse objetivo é dividido em **três controles**.

14.1.1. Análise e Especificação dos Requisitos de SI

Controle: convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

14.1.2. Serviços de Aplicação Seguros em Redes Públicas

Controle: convém que as informações envolvidas nos serviços de aplicação que transitam sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.

14.1.3. Protegendo as Transações nos Aplicativos de Serviços

Controle: convém que informações envolvidas em transações nos aplicativos de serviços sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada.

14.2. SEGURANÇA EM PROCESSOS DE DESENVOLVIMENTO E DE SUPORTE

Objetivo: garantir que a segurança da informação esteja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.

Esse objetivo é dividido em **nove controles**:

14.2.1. Política de Desenvolvimento Seguro

Controle: convém que **regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização**.

14.2.2. Procedimentos para Controle de Mudanças de Sistemas

Controle: convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças.

14.2.3. Análise Crítica Técnica das Aplicações após Mudanças nas Plataformas Operacionais

Controle: quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para garantir que não haverá qualquer impacto adverso na operação da organização ou na segurança.

14.2.4. Restrições sobre Mudanças em Pacotes de Software

Controle: convém que modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas.

14.2.5. Princípios para Projetar Sistemas Seguros

Controle: convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.

14.2.6. Ambiente Seguro para Desenvolvimento

Controle: convém que as organizações estabeleçam e protejam adequadamente ambientes seguros de desenvolvimento, para os esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema.

14.2.7. Desenvolvimento Terceirizado

Controle: convém que a organização supervise e monitore as atividades de desenvolvimento de sistemas terceirizado.

14.2.8. Teste de Segurança do Sistema

Controle: convém que os testes das funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas.

14.2.9. Teste de Aceitação de Sistemas

Controle: convém que programas de testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões.

14.3. DADOS PARA TESTE

Objetivo: assegurar a proteção dos dados usados para teste.

Esse objetivo possui um único controle.

14.3.1. Proteção dos Dados para Teste

Controle: convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados.

15. RELACIONAMENTO NA CADEIA DE SUPRIMENTO

15. Relacionamento na cadeia de suprimento.

15.1. SI na cadeira de suprimento.

15.1.1. Política de SI no relacionamento com os fornecedores.

- 15.1.2. Identificando SI nos acordos com fornecedores.
- 15.1.3. Cadeia de suprimento na tecnologia da informação e comunicação.

15.2. Gerenciamento da entrega do serviço do fornecedor.

- 15.2.1. Monitoramento e análise crítica de serviços com fornecedores.
- 15.2.2. Gerenciamento de mudanças para serviços com fornecedores.

Esta Seção é dividida em **dois objetivos**.

15.1. SI NA CADEIRA DE SUPRIMENTO

Objetivo:

Garantir a proteção dos ativos da organização que são acessados pelos fornecedores.

Esse objetivo é dividido em **três controles**:

15.1.1. Política de SI no Relacionamento com os Fornecedores

Controle: convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor e documentados.

15.1.2. Identificando SI nos Acordos com Fornecedores

Controle: convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização.

15.1.3. Cadeia de Suprimento na Tecnologia da Informação e Comunicação

Controle: convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados à cadeia de produtos e serviços de tecnologia da informação e comunicação.

15.2. GERENCIAMENTO DA ENTREGA DO SERVIÇO DO FORNECEDOR

Objetivo: manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

Esse objetivo é dividido em **dois controles**:

15.2.1. Monitoramento e Análise Crítica de Serviços com Fornecedores

Controle: convém que as organizações monitorem, analisem criticamente e auditem, a intervalos regulares, a entrega dos serviços executados pelos fornecedores.

15.2.2. Gerenciamento de Mudanças para Serviços com Fornecedores

Controle: convém que mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, sejam gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos, e a reavaliação dos riscos.

16. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

16. Gestão de incidentes de SI.

16.1. Gestão de incidentes de SI e melhorias.

16.1.1. Responsabilidades e procedimentos.

16.1.2. Notificação de eventos de segurança da informação.

16.1.3. Notificando fragilidades de segurança da informação.

16.1.4. Avaliação e decisão dos eventos de segurança da informação.

16.1.5. Resposta aos incidentes de segurança da informação.

16.1.6. Aprendendo com os incidentes de segurança da informação.

16.1.7. Coleta de evidências.

Esta Seção é dividida em um único objetivo.

16.1. GESTÃO DE INCIDENTES DE SI E MELHORIAS

Objetivo: assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo comunicação sobre fragilidades e eventos de segurança da informação.

Esse objetivo é dividido em sete controles:

16.1.1. Responsabilidades e Procedimentos

Controle: convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.

16.1.2. Notificação de Eventos de Segurança da Informação

Controle: convém que os **eventos de segurança da informação sejam relatados por meio dos canais de gestão, o mais rapidamente possível**.

16.1.3. Notificando Fragilidades de Segurança da Informação

Controle: convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização sejam instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.

16.1.4. Avaliação e Decisão dos Eventos de Segurança da Informação

Controle: convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.

16.1.5. Resposta aos Incidentes de Segurança da Informação

Controle: convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados.

16.1.6. Aprendendo com os Incidentes de Segurança da Informação

Controle: convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.

16.1.7. Coleta de Evidências

Controle: convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.

17. ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DA CONTINUIDADE DO NEGÓCIO

17. Aspectos da SI na gestão da continuidade do negócio.

17.1 Continuidade da SI.

17.1.1 Planejando a continuidade da SI.

17.1.2 Implementando a continuidade da SI.

17.1.3 Verificação, análise crítica e avaliação da continuidade da SI.

17.2 Redundâncias.

17.2.1 Disponibilidade dos recursos de processamento da informação.

Esta Seção é dividida em **dois objetivos**.

17.1. CONTINUIDADE DA SEGURANÇA DA INFORMAÇÃO (SI)

Objetivo: convém que a continuidade da segurança da informação seja considerada nos sistemas de gestão da continuidade do negócio da organização.

Esse objetivo é dividido em **três controles**.

17.1.1. Planejando a Continuidade da Segurança da Informação

Controle: convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

Diretrizes para implementação: convém que uma organização avalie se a continuidade da segurança da informação está contida dentro do processo de gestão da continuidade do negócio ou no processo de gestão de recuperação de desastre. Requisitos de segurança da informação podem ser determinados quando do planejamento da continuidade do negócio e da recuperação de desastre.

Na ausência de um planejamento formal de continuidade do negócio e de recuperação de desastre, convém que a gestão da segurança da informação assuma que os requisitos de segurança da informação permanecem os mesmos, em situações adversas, comparadas com as condições de operação normal. Alternativamente, uma organização pode realizar uma análise de impacto do negócio relativa aos aspectos de segurança da informação, para determinar os requisitos de segurança da informação que são aplicáveis nas situações adversas.

Informações adicionais: para reduzir o tempo e o esforço de uma análise de impacto do negócio adicional, da segurança da informação, é recomendado capturar os aspectos da segurança da informação no gerenciamento da continuidade normal dos negócios ou na análise do impacto ao negócio no gerenciamento da recuperação de um desastre. Isto implica que os requisitos de continuidade da segurança da informação estão explicitamente contemplados na gestão da continuidade do negócio ou nos processos de gerenciamento da recuperação de desastre.

17.1.2. Implementando a Continuidade da Segurança da Informação

Controle: convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.

Diretrizes para implementação. Convém que uma organização se assegure de que:

- Uma **estrutura de gerenciamento adequada está implementada** para mitigar e responder a um evento de interrupção, usando pessoal com a necessária autoridade, experiência e competência;
- O **pessoal de resposta a incidente** com a necessária responsabilidade, autoridade e competência para gerenciar um incidente e garantir a segurança da informação, está designado;
- **Planos documentados, procedimentos de recuperação e resposta** estejam desenvolvidos e aprovados, detalhando como a organização irá gerenciar um evento de interrupção e como manterá a sua segurança da informação em um nível predeterminado, com base nos objetivos de continuidade da segurança da informação aprovado pela direção.

Em função dos requisitos de continuidade de segurança da informação, convém que a organização estabeleça, documente, implemente e mantenha:

- **Controles de segurança da informação** dentro dos processos de recuperação de desastre ou de continuidade do negócio, procedimentos e ferramentas e sistemas de suporte;
- **Processos, procedimentos e mudança** de implementação para manter os controles de segurança da informação existentes durante uma situação adversa;
- **Controles compensatórios** para os controles de segurança da informação que não possam ser mantidos durante uma situação adversa.

Informações adicionais. Dentro do contexto da continuidade do negócio ou da recuperação de desastre, procedimentos e processos específicos podem ser necessários, que sejam definidos. Convém que informações que sejam tratadas nestes processos e procedimentos ou em sistemas de informação dedicados para apoiá-los, sejam protegidas. Desta forma, convém que a organização envolva especialistas em segurança da informação, quando do estabelecimento, implementação e manutenção dos procedimentos e processos de recuperação de desastres ou da continuidade dos negócios.

Convém que os controles de segurança da informação a serem implementados continuem a operar durante uma condição de situação adversa. Se os controles de segurança não são capazes de manter a informação segura, convém que outros controles sejam estabelecidos, implementados e mantidos para garantir um nível aceitável da segurança da informação.

17.1.3. Verificação, Análise Crítica e Avaliação da Continuidade da Segurança da Informação

Controle: convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.

Diretrizes para implementação: mudanças organizacionais, técnicas, de procedimentos e processos, quando em um contexto operacional ou de continuidade, podem conduzir a mudanças nos requisitos de continuidade da segurança da informação. Em tais casos, convém que a continuidade dos processos, procedimentos e controles para segurança da informação sejam analisados criticamente com base nesses requisitos alterados.

Convém que a organização verifique a sua continuidade da gestão da segurança da informação através de:

- Testes e verificação da funcionalidade dos processos, procedimentos e controles da continuidade da segurança da informação para garantir que eles são consistentes com os objetivos da continuidade da segurança da informação;
- Testes e verificação do conhecimento e rotina para operar os procedimentos, processos e controles de continuidade da segurança da informação de modo a assegurar que o seu desempenho esteja consistente com os objetivos da continuidade da segurança da informação;

- Análise crítica quanto à validade e eficácia dos controles de continuidade da segurança da informação, quando aos sistemas de informação, processos de segurança da informação, procedimentos e controles ou gestão da continuidade do negócio/gestão de recuperação de desastre e soluções de mudança.

Informações adicionais: a verificação dos controles da continuidade da segurança da informação é diferente das verificações e testes da segurança da informação normal.

Convém que sejam realizados fora do âmbito dos testes de mudanças.

Quando possível é recomendável integrar a verificação dos controles da continuidade da segurança da informação, com os testes de recuperação de desastre ou da continuidade dos negócios da organização.

17.2. REDUNDÂNCIAS

Objetivo: assegurar a disponibilidade dos recursos de processamento da informação.

Esse objetivo é dividido em um único controle.

17.2.1. Disponibilidade dos Recursos de Processamento da Informação

Controle: convém que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.

Diretrizes para implementação: convém que a organização identifique os requisitos do negócio quanto à disponibilidade de sistemas de informação. Quando a disponibilidade não puder ser assegurada usando a arquitetura de sistemas existentes, componentes redundantes ou arquiteturas sejam considerados.

Onde aplicável, convém que sistemas de informação redundantes sejam testados para assegurar que a transferência de um componente para outro componente, quando existe falha do primeiro componente, este funciona conforme esperado.

Informações adicionais: a implementação de redundâncias pode introduzir riscos à integridade ou confidencialidade da informação e dos sistemas de informação, os quais precisam ser considerados quando do projeto dos sistemas de informação.

18. CONFORMIDADE

18. Conformidade.

18.1. Conformidade com requisitos legais e contratuais.

18.1.1. Identificação da legislação aplicável e de requisitos contratuais.

18.1.2. Direitos de propriedade intelectual.

18.1.3. Proteção de registros.

18.1.4. Proteção e privacidade de informações de identificação pessoal.

18.1.5. Regulamentação de controles de criptografia.

18.2. Análise crítica da segurança da informação.

18.2.1. Análise crítica independente da segurança da informação.

18.2.2. Conformidade com as políticas e procedimentos de SI.

18.2.3. Análise crítica da conformidade técnica.

Esta Seção possui **dois objetivos**.

18.1. CONFORMIDADE COM REQUISITOS LEGAIS E CONTRATUAIS

Objetivo: evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança. Esse objetivo é dividido em **cinco controles**:

18.1.1. Identificação da Legislação Aplicável e de Requisitos Contratuais

Controle: convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes e o enfoque da organização para atender a esses requisitos sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.

18.1.2. Direitos de Propriedade Intelectual

Controle: convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados aos direitos de propriedade intelectual, e sobre o uso de produtos de softwares.

18.1.3. Proteção de Registros

Controle: convém que registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

18.1.4. Proteção e Privacidade de Informações de Identificação Pessoal

Controle: convém que a privacidade e a proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.

18.1.5. Regulamentação de Controles de Criptografia

Controle: convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

18.2. ANÁLISE CRÍTICA DA SEGURANÇA DA INFORMAÇÃO

Objetivo: assegurar que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização.

Esse objetivo é dividido em **três controles**:

18.2.1. Análise Crítica Independente da Segurança da Informação

Controle: convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivo dos controles, controles, políticas, processo e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.

18.2.2. Conformidade com as Políticas e Procedimentos de SI

Controle: convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.

18.2.3. Análise Crítica da Conformidade Técnica

Controle: convém que os sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.

RESUMO

A norma que será aqui destacada!

ABNT NBR ISO/IEC 27002:2013

Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Controles de Segurança da Informação



Norma ISO/IEC 27002

... é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação.

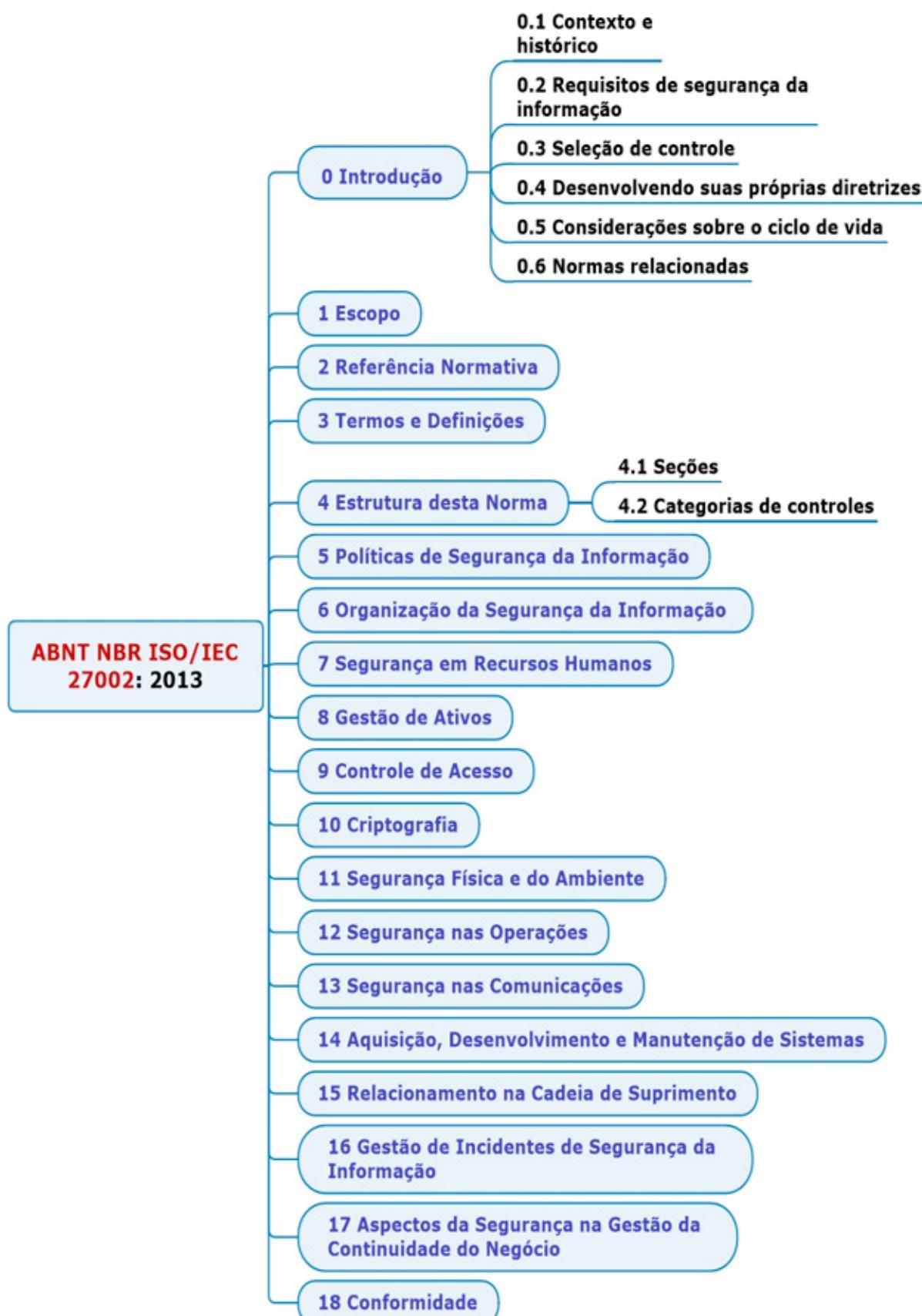


Figura. Seções da norma ABNT NBR ISO IEC 27002:2013

Fonte: Quintão (2020)

QUESTÕES COMENTADAS EM AULA

001. (FGV/TCE-SE/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/SEGURANÇA DA INFORMAÇÃO/2015) Com relação à norma ISO/IEC 27002:2013, está correto afirmar que:

- a) ela indica a necessidade do uso do ciclo PDCA nos processos da organização;
- b) a revisão de 2013 criou uma seção específica para controles criptográficos;
- c) não é mais necessário o gerenciamento de ativos, cuja cláusula foi suprimida na revisão de 2013;
- d) organizações agora podem ser certificadas na última revisão (2013) da ISO 27002;
- e) ela tem foco no gerenciamento de risco na segurança da informação.

002. (CESPE/TJ-CE/ANALISTA JUDICIÁRIO/CIÊNCIAS DA COMPUTAÇÃO/2014) O uso de equipamentos de UPS (uninterruptible power supply), considerados fornecedores de energia elétrica secundários, é recomendado, de acordo com a norma ABNT NBR ISO/IEC 27.002, para o controle

- a) da segurança em escritórios, salas e instalações.
- b) de trabalho em áreas seguras.
- c) de áreas seguras.
- d) do perímetro de segurança física.
- e) da segurança de equipamentos.

003. (FCC/TJ-MA/ANALISTA DE SISTEMAS/DESENVOLVIMENTO/2019) A norma ABNT NBR ISO/IEC 27002:2013 tem uma seção que trata da segurança de operações, cujo objetivo é garantir a operação segura e correta dos recursos de processamento da informação. Nesta seção, no que tange ao desenvolvimento, teste e produção de software, recomenda-se que

- a) softwares em desenvolvimento e softwares em produção sejam sempre executados no mesmo sistema, processador, domínio ou diretório.
- b) ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.
- c) compiladores, editores e outras ferramentas de desenvolvimento sejam completamente acessíveis aos sistemas operacionais.
- d) usuários tenham um único perfil para sistemas de testes e em produção, para garantir que todos os aspectos desejados sejam testados.
- e) dados sensíveis sejam copiados e utilizados nos ambientes de teste, independente dos controles, para obter maior precisão nos resultados dos testes.

QUESTÕES DE CONCURSO

004. (CESPE/CGE-CE/AUDITOR DE CONTROLE INTERNO/TECNOLOGIA DA INFORMAÇÃO/2019) Em uma organização em que se processam dados pessoais sensíveis, existe a preocupação com o manuseio dos dados pelos empregados, para que não aconteçam vazamentos de dados e exposição indevida de pessoas. Segundo a NBR ISO/IEC 27002, para assegurar que as referidas informações pessoais recebam o nível adequado de proteção, deve-se utilizar como controle

- a) o descarte de mídias.
- b) o uso aceitável de ativos.
- c) o gerenciamento de chaves.
- d) o provisionamento para acesso de usuário.
- e) a classificação da informação.



Conforme vimos na seção **Gestão de Ativos** da NBR ISO/IEC 27002, para **assegurar que a informação receba um nível adequado de proteção**, de acordo com a sua importância para a organização, o **controle** a ser utilizado é o de **Classificação da Informação**, que faz parte da seção **Gestão de Ativos**. Veja mais:

8.2.1. Classificação da Informação

Controle

Convém que **a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada**.

Letra e.

005. (CESPE/ABIN/OFICIAL TÉCNICO DE INTELIGÊNCIA/ÁREA 8/2018) Acerca de segurança da informação, julgue o item a seguir, com base na norma ABNT NBR ISO/IEC 27002:2013. As bibliotecas das fontes dos programas de uma organização devem ser mantidas no mesmo ambiente computacional do sistema operacional, com o objetivo de facilitar atividades de auditoria.



Convém, de acordo com a norma ABNT NBR ISO/IEC 27002:2013, que **seja evitado manter as bibliotecas de programa-fonte no mesmo ambiente dos sistemas operacionais**.

Errado.

006. (CESPE/TRE-TO/TÉCNICO JUDICIÁRIO/PROGRAMAÇÃO DE SISTEMAS/2017) Segundo a norma ABNT NBR ISO/IEC 27002:2013, a segurança da informação deve ser apoiada por políticas de tópicos específicos, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro

da organização. A partir dessas informações, assinale a opção que apresenta um exemplo de política com tópico específico considerado pela referida norma.

- a) desenvolvimento de software**
- b) segurança institucional**
- c) ética concorrencial**
- d) gestão de riscos**
- e) controles criptográficos**



Segundo a ABNT NBR ISO/IEC 27002 (2013, p.3), são identificadas como políticas com tópicos específicos:

- controle de acesso (ver Seção 9);
- classificação e tratamento da informação (ver 8.2);
- segurança física e do ambiente (ver Seção 11);
- *backup* (ver 12.3);
- transferência da informação (ver 13.2);
- proteção contra *malware* (ver 12.2);
- gerenciamento de vulnerabilidades técnicas (ver 12.6.1);
- **controles criptográficos** (ver Seção 10);
- segurança nas comunicações (ver Seção 13);
- proteção e privacidade da informação de identificação pessoal (ver 18.1.4);
- relacionamento na cadeia de suprimento (ver Seção 15);
- tópicos orientados aos usuários finais, como uso aceitável dos ativos (ver 8.1.3), mesa limpa e tela limpa (ver 11.2.9), etc.

Letra e.

007. (CESPE/TRT-7^a REGIÃO/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2017) A classificação da informação assegura um nível adequado de proteção à informação. De acordo com a ABNT NBR ISO/IEC 27002, uma ação a ser considerada no tratamento de ativos é

- a) registrar as mídias removíveis com informações consideradas confidenciais.**
- b) manter registro formal dos destinatários de ativos autorizados.**
- c) definir uma relação de portadores autorizados.**
- d) avaliar os impactos da violação da confidencialidade de ativos.**

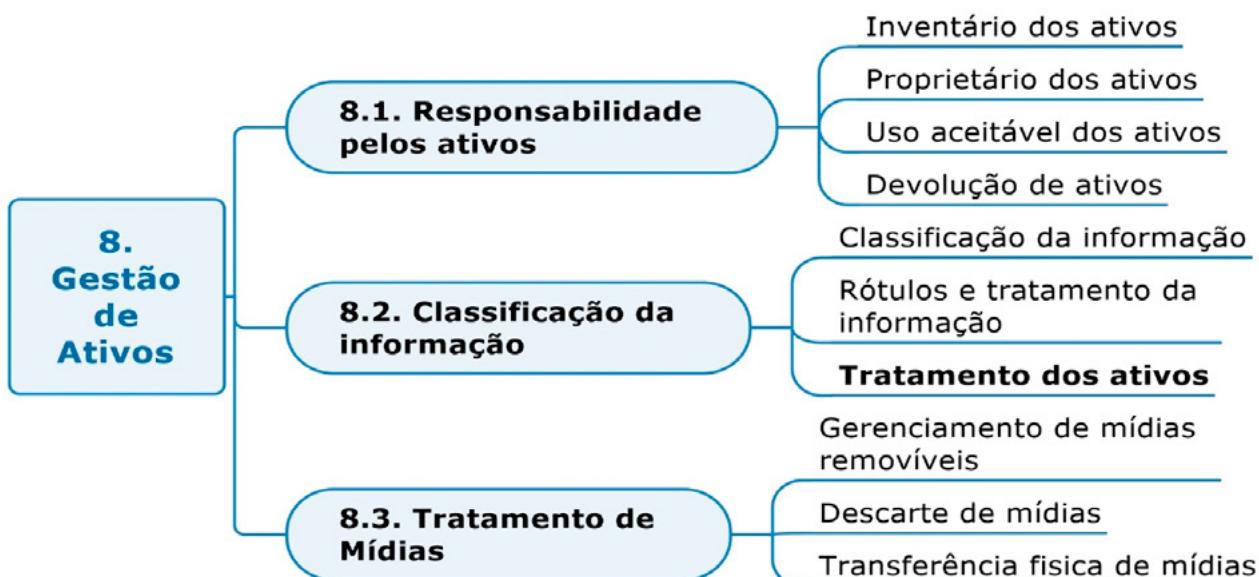


- a) Errada. Pertence à subseção **Gerenciamento de mídias removíveis**.**
- b) Certa. **Tratamento dos ativos** (item 8.2.3) é subseção de **Classificação da informação** (item 8.2), a qual é subseção da seção **Gestão de ativos** (item 8).**

De acordo com a ABNT NBR ISO/IEC 27002, sobre **tratamento de ativos**, convém considerar:

- que **procedimentos** sejam **estabelecidos** para o **tratamento, processamento, armazenamento** e a **transmissão** da informação, de acordo com a sua **classificação**;
- **restrições** de acesso;
- **manutenção de um registro formal dos destinatários de ativos autorizados**;
- **armazenamento** dos ativos de TI de acordo com as especificações dos **fabricantes**;
- **identificação eficaz de todas as cópias das mídias**, para chamar a atenção dos destinatários autorizados;
- que **acordos** com outras organizações **contemplem procedimento para identificar a classificação de informações** compartilhadas e interpretar os rótulos de classificação de outras organizações.

Conforme visto, uma ação a ser considerada no tratamento de ativos é **manter registro formal dos destinatários de ativos autorizados (letra B)**.



Controle de 8.2.3.

Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela organização.

c) Errada. Definir uma relação de portadores autorizados pertence à subseção **Transferência física de mídias**.

d) Errada. Não é contemplado na norma.

Letra b.

008. (CESPE/TRE-BA/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS/2017) De acordo com a ABNT NBR ISO/IEC 27002 – norma de referência para a escolha de controles no processo de implementação de sistemas de gestão da segurança da informação –, o primeiro objetivo de resposta a incidente de segurança da informação é

a) qualificar técnicos locais para o trabalho de identificar, coletar e preservar as informações.

- b) realizar o devido processo administrativo disciplinar para a apuração do fato.
- c) listar as lições aprendidas para a divulgação entre os integrantes da organização.
- d) voltar ao nível de segurança normal e, então, iniciar a recuperação.
- e) suspender as atividades até que os fatos relacionados ao incidente sejam apurados.



A seção **16. Gestão de incidentes de Segurança da Informação** da ABNT NBR ISO/IEC 27002, subseção **16.1.5. Resposta aos incidentes de Segurança da Informação** destaca que o primeiro objetivo de resposta a incidente é “voltar ao nível de segurança normal” e então iniciar a recuperação necessária. Conforme visto, a letra D é a resposta!

A letra (e) não foi contemplada na norma. As letras (a), (b) e (c) retratam atividades a serem realizadas em outro contexto.

Letra d.

009. (CESPE/SE-DF/ANALISTA DE GESTÃO EDUCACIONAL/TECNOLOGIA DA INFORMAÇÃO/2017) Relativamente a segurança da informação, julgue o item subsequente.

De acordo com a NBR ISO 27002, a política de controle de acesso deve tratar do controle de acesso lógico, enquanto a política de segurança física e do ambiente deve tratar do controle de acesso físico.



Na seção **9. Controle de Acesso**, da ABNT NBR ISO/IEC 27002, subseção **9.1.1. Política de Controle de Acesso**, a norma trata como diretriz que os **controles de acesso lógico e físico sejam tratados de forma conjunta**.

Errado.

010. (FAURGS/BANRISUL/SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO/2018)

Em relação à Política de Segurança da Informação (PSI), a norma ISO ABNT NBR ISO/IEC 27002:2013 recomenda

- a) o alinhamento da PSI da organização com a PSI dos órgãos de controle externo da organização.
- b) que seja um documento único, detalhado e autocontido, facilitando a divulgação e aumentando sua aplicabilidade.
- c) uma revisão com periodicidade mínima de um ano, visando assegurar a sua contínua pertinência, adequação e eficácia.
- d) que o Gestor de TI tenha autonomia para alterar e publicar a PSI.
- e) que sejam contemplados requisitos oriundos de regulamentações, legislação e contratos.



- a) Errada. Não há esse direcionamento na norma.
- b) Errada. Conforme destaca a norma ISO ABNT NBR ISO/IEC 27002 (2013, p. 4), políticas de segurança da informação podem ser **emitidas em um único documento**, “política de segurança da informação” **ou como um conjunto de documentos individuais, relacionados**.
- c) Errada. A norma não destaca periodicidade mínima. As políticas de segurança da informação devem ser analisadas criticamente a **intervalos planejados ou quando mudanças significativas ocorrerem**, para assegurar a sua contínua pertinência, adequação e eficácia.
- d) Errada. A alta direção é responsável por estabelecer, implantar, atualizar e comunicar as políticas de segurança da informação.
- e) Certa. A norma ISO ABNT NBR ISO/IEC 27002 (2013, p.2), no item 5.1.1, recomenda que as políticas de segurança da informação contemplam requisitos oriundos de: regulamentações, legislação e contratos, bem como de estratégia do negócio e do ambiente de ameaça da segurança da informação, atual e futuro.

Letra e.

011. (CESPE/TCE-MG/ANALISTA DE CONTROLE EXTERNO/CIÊNCIA DA COMPUTAÇÃO/2018) A NBR ISO/IEC 27001 foi preparada para prover requisitos que estabeleçam um sistema de gestão de segurança da informação (SGSI), ao passo que a ISO/IEC 27002 foi projetada para organizações que usem a norma como uma referência para selecionar controles no processo de implementação do SGSI.

Em relação a essas normas, assinale a opção correta.

- a) De acordo com a NBR ISO/IEC 27002, a informação sobre logs deve ser acessível a todos, de forma a ofertar a maior transparência possível aos gestores da organização, excluídas as atividades de administrador de sistemas, que não precisam ser controladas sob o princípio da tutela da confidencialidade.
- b) Determinar os riscos e as oportunidades que necessitam ser considerados pelo sistema faz parte da NBR ISO/IEC 27001, mas o tratamento dos riscos limita-se à NBR ISO/IEC 27002.
- c) De acordo com a NBR ISO/IEC 27001, o SGSI não aborda controles afetos a processos terceirizados, uma vez que os fornecedores são tratados como parte de controles, logo concorrentes à NBR ISO/IEC 27002.
- d) A NBR ISO/IEC 27001 trata de auditoria interna no SGSI, com intervalos planejados conduzidos pela organização; já a NBR ISO/IEC 27002 trata de atividades e requisitos de auditoria que envolvem a verificação dos sistemas operacionais, com o objetivo de minimizar interrupções nos processos de negócio.
- e) Um dos controles da NBR ISO/IEC 27002 afetos à segurança dos sistemas diz respeito à implantação de criptografia assimétrica nos sistemas relevantes, com fulcro a proteger a informação tendo como base que cada um desses sistemas deve possuir sua própria referência de fonte de tempo para isolá-los em caso de ataques.



- a) Errada. Conforme cita o item 12.4.2 da NBR ISO/IEC 27002, convém que as informações dos registros de eventos (log) e os seus recursos **sejam protegidos contra acesso não autorizado e adulteração**. Conforme 12.4.13 **convém também que as atividades dos administradores e operadores do sistema sejam registradas** e os **registros (logs) protegidos** e analisados criticamente, a intervalos regulares.
- b) Errada. **O tratamento dos riscos aplica-se tanto à NBR ISO/IEC 27002 quanto à NBR ISO/IEC 27001.**
- c) Errada. **Tanto a NBR ISO/IEC 27002 quanto a NBR ISO/IEC 27001 tratam de processos terceirizados.** O subitem 8.1 da NBR ISO/IEC 27001 destaca que a organização deve assegurar **que os processos terceirizados estão determinados e são controlados**.
- d) Certa. Ambas as normas tratam de auditorias. De acordo com a NBR ISO/IEC 27001, o SGSI é melhorado através de auditorias internas e análises críticas da direção. Quanto à NBR ISO/IEC 27002, no que diz respeito à controles de auditoria de sistemas de informação (item 12.7.1), temos o seguinte texto na referida norma:
- Controle:** convém que as atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.
- e) Errada. Não existe na **NBR ISO/IEC 27002 um** controle que mencione especificamente a *implantação de criptografia assimétrica*. Quanto à referência de fonte de tempo, em 12.4.4, a referida norma destaca: convém que os relógios de todos os sistemas de processamento de informações relevantes sejam sincronizados com uma fonte de tempo precisa.

Portanto, a resposta é a letra **d**.

Letra d.

012. (CESPE/EBSERH/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/2018) Julgue o próximo item, a respeito da segurança da informação.

De acordo com a norma ISO 27002, é conveniente que, na política de segurança da informação, seja incluída atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação.



Sobre a seção 5.1.1 da norma ISO 27002, intitulada **políticas para Segurança da Informação (SI)**, convém que:

- contemplam **requisitos oriundos da estratégia do negócio; de regulamentações, legislação e contratos; do ambiente de ameaça da SI**, atual e futuro;
- contenham **declarações** relativas a:
- **definição da SI, objetivos e princípios** para orientar todas as atividades relativas à SI;

- atribuição de **responsabilidades** para os **papéis** definidos;
- **processos** para o **tratamento dos desvios** e exceções.
- a Política de Segurança da Informação seja apoiada por **políticas de tópicos específicos**;
- estas **políticas sejam comunicadas** aos funcionários e partes externas.

Certo.

013. (CESPE/STJ/TÉCNICO JUDICIÁRIO/SUPORTE TÉCNICO/2018) Julgue o item seguinte, a respeito de DevOps e das disposições constantes da NBR ISO/IEC 27002.

Os controles da segurança da informação elencados na NBR ISO/IEC 27002 englobam as ações realizadas na gestão de projetos específicos da área de segurança da informação, as quais, porém, não lidam com controles que visem proteger a informação processada em sítios de teletrabalho.



O uso do Teletrabalho (ou trabalho remoto) está contemplado no item “6. Organização da segurança da informação”, da norma **NBR ISO/IEC 27002**. Vamos ao que está explicitado na referida norma:

6.2.2. Trabalho remoto

Controle

Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em **locais de trabalho remoto**.

Diretrizes para implementação

Convém que a organização que permita a atividade de **trabalho remoto** publique uma política que defina as condições e restrições para o uso do **trabalho remoto**.

Conforme visto, o item está errado.

Errado.

014. (CESPE/ABIN/OFICIAL TÉCNICO DE INTELIGÊNCIA - ÁREA 8/2018) Acerca de segurança da informação, julgue o item a seguir, com base na norma ABNT NBR ISO/IEC 27002:2013. Quando uma mídia removível não for mais necessária e vier a ser retirada da organização, recomenda-se que o conteúdo magnético seja deletado.



Segundo a norma ABNT NBR ISO/IEC 27002 (2013), sobre **gerenciamento de mídias removíveis**, convém que: quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável seja destruído, caso venha a ser retirado da organização.

Observe que o termo correto é “destruído”, ao invés de deletado como consta no enunciado.

Atenção aqui!

Errado.

015. (CESPE/ABIN/OFICIAL TÉCNICO DE INTELIGÊNCIA/ÁREA 8/2018) Acerca de segurança da informação, julgue o item a seguir, com base na norma ABNT NBR ISO/IEC 27002:2013. Uma das premissas do controle de acesso na segurança da informação é a implementação da regra de que tudo é proibido, a menos que seja expressamente permitido.



A norma **ABNT NBR ISO/IEC 27002:2013** recomenda, em seu tópico 9.1.1 Política de controle de acesso, que sejam tomados cuidados na especificação de regras de controle de acesso quando se considerar o seguinte: a) estabelecer regra baseada na premissa de que “**Tudo é proibido a menos que expressamente permitido**” em lugar da regra mais fraca que “Tudo é permitido, a menos que expressamente proibido”.

Certo.

016. (CESPE/ABIN/OFICIAL TÉCNICO DE INTELIGÊNCIA/ÁREA 8/2018) Acerca de segurança da informação, julgue o item a seguir, com base na norma ABNT NBR ISO/IEC 27002:2013. As informações já armazenadas no histórico de acesso não devem ser mais editadas, servindo para coleta e retenção de evidências para auditoria.



A norma **ABNT NBR ISO/IEC 27002:2013** recomenda, em **12.4.2 - Proteção das informações dos registros de eventos (logs)**, que as informações dos registros de eventos (*log*) e os seus recursos sejam protegidos contra acesso não autorizado e adulteração, (...) devendo ser guardados como parte da política de retenção de registros ou devido aos requisitos para a coleta e retenção de evidência.

Certo.

017. (FCC/TCE-CE/TÉCNICO DE CONTROLE EXTERNO/AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO/2015) A Norma NBR ISO/IEC 27002:2013 possui 14 sessões de controles de segurança da informação, dentre elas,

- a)** Gestão de Riscos de Segurança da Informação.
- b)** Métricas de Sistemas de Gestão de Segurança da Informação.
- c)** Gestão da Segurança da Informação em Organizações da Administração Pública.
- d)** Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio.
- e)** Técnicas para Governança da Segurança da Informação.



Seções da ABNT NBR ISO/IEC 27002: 2013 que Contém Controles

- 5 Políticas de Segurança da Informação
- 6 Organização da Segurança da Informação
- 7 Segurança em Recursos Humanos
- 8 Gestão de Ativos
- 9 Controle de Acesso
- 10 Criptografia
- 11 Segurança Física e do Ambiente
- 12 Segurança nas Operações
- 13 Segurança nas Comunicações
- 14 Aquisição, Desenvolvimento e Manutenção de Sistemas
- 15 Relacionamento na Cadeia de Suprimento
- 16 Gestão de Incidentes de Segurança da Informação
- 17 Aspectos da Segurança na Gestão da Continuidade do Negócio
- 18 Conformidade

Letra d.

018. (CESPE/MEC/GESTÃO/GERENTE DE SEGURANÇA/2015) Julgue os próximos itens, de acordo com a norma NBR ISO/IEC 27002:2013, que estabelece diretrizes para práticas de gestão de segurança da informação.

As fontes principais de requisitos de segurança da informação são avaliação de riscos para a organização, legislação vigente e conjuntos particulares de princípios, objetivos e requisitos do negócio.



De acordo com a norma NBR ISO/IEC 27002:2013, existem **três fontes principais de requisitos de segurança da informação**. São elas:

- a **avaliação de riscos para a organização**, levando-se em conta os objetivos e as estratégias globais de negócio da organização;
- a **legislação vigente**, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural;

- os **conjuntos particulares de princípios, objetivos e os requisitos do negócio** para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.

Certo.

019. (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.

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 à proteção física dos ativos.



Nesse contexto, os equipamentos devem ser examinados antes da manutenção, para **assegurar que as informações sensíveis sejam eliminadas do equipamento, ou o pessoal de manutenção seja de absoluta confiança**. Tal controle está ligado à **segurança física** (que busca proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos).

Certo.

020. (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.

Errado.

021. (CESPE/MEC/ADMINISTRADOR DE DADOS/2015) Considerando as normas ISO/IEC 27001, ISO/IEC 27002 e IN MPOG n.º 04/2014, julgue o item subsequente.

Durante o processo de correção das provas do ENEM, deve-se implementar a separação dos recursos de desenvolvimento, mas não os de teste e de produção.



A norma **ABNT NBR ISO/IEC 27002:2013** recomenda, em **12.1.4 – Separação dos ambientes de desenvolvimento, teste e produção**, que “convém que **ambientes de desenvolvimento, teste**

e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção”.

Errado.

022. (CESPE/TJ-CE/ANALISTA JUDICIÁRIO/CIÊNCIAS COMPUTAÇÃO/2014) Constitui diretriz de implementação de controles contra códigos maliciosos, conforme a norma ABNT NBR ISO/IEC 27.002:

- a)** estabelecer controles criptográficos para serviços de tecnologia da informação que exijam autenticação.
- b)** aplicar mecanismos apropriados de registro e monitoração para habilitar a gravação das ações relevantes de segurança.
- c)** destruir o conteúdo de qualquer meio magnético, ainda que reutilizável, que não seja mais necessário, ou seja, retirado da organização.
- d)** conduzir análises críticas regulares dos softwares e dados dos sistemas que suportam processos críticos de negócio.
- e)** ativar medidas técnicas disponíveis nos sistemas específicos para garantir que o código móvel esteja sendo administrado.



A seção **12.2 - Proteção contra malware** da norma **ABNT NBR ISO/IEC 27002:2013** destaca controles associados a essas ameaças. A referida norma recomenda, em **12.2.1 – Controles contra malware - que diversos controles sejam considerados, como o listado na letra D dessa questão**. De acordo com a norma recomenda-se “**f)** conduzir análises críticas regulares dos softwares e dados dos sistemas que suportam processos críticos de negócio.

Letra d.

023. (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.



A organização deve conduzir **auditorias internas** a intervalos planejados para prover informações sobre o quanto o SGSI:

- Está em conformidade com:
 - os próprios requisitos da organização para o seu sistema de gestão de segurança da informação;
 - os requisitos da Norma ABNT NBR ISO/IEC 27001;
- 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:

- avaliar a necessidade de ações para eliminar as causas de não conformidade;
- realizar mudanças no SGSI, quando necessárias, dentre outras.

Certo.

024. (CESPE/MEC/GESTÃO/GERENTE DE SEGURANÇA/2015) Julgue os próximos itens, de acordo com a norma NBR ISO/IEC 27002:2013, que estabelece diretrizes para práticas de gestão de segurança da informação.

A definição de uma política de segurança da informação e o estabelecimento da abordagem para gerenciar os objetivos de segurança da informação devem ser aprovados no mais alto nível da organização.



Isso mesmo, conforme destaca a seguinte diretriz: “convém que, no mais **alto nível da organização**, seja **definida uma política de segurança da informação**, que seja aprovada pela direção e **estabeleça a abordagem da organização** para gerenciar os objetivos de segurança da informação (Seção 5.1.1 da ABNT NBR ISO/IEC 27002:2013).

Certo.

025. (CESPE/MEC/GESTÃO/GERENTE DE SEGURANÇA/2015) Julgue os próximos itens, de acordo com a norma NBR ISO/IEC 27002:2013, que estabelece diretrizes para práticas de gestão de segurança da informação.

A estrutura organizacional e as funções de software e hardware não figuram como objetos da referida norma.



A norma ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da Informação), em sua seção introdutória, destaca que a segurança da informação é alcançada pela implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, **estruturas organizacionais e funções de software e hardware**. Esses controles (que figuram como objetos da referida norma) precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos (ABNT, 2005).

Errado.

026. (CESPE/MEC/TÉCNICO DE NÍVEL SUPERIOR/ADMINISTRADOR DE REDE/2015) Julgue os seguintes itens, de acordo com o que estabelecem as normas ISO/IEC 27001 e ISO/IEC 27002.

De acordo com a norma ISO/IEC 27002, os controles implementados para a proteção das informações de log devem levar em consideração a capacidade de armazenamento da mídia utilizada para esse fim.



Conforme destaca a seção 12.4.2 da norma ISO/IEC 27002:2013, os controles implementados para a proteção das informações de log devem levar em consideração a capacidade de armazenamento da mídia utilizada para essa finalidade, uma vez que, se ela for excedida, resultará em falhas no registro de eventos ou sobreposição do registro de evento anterior.

Certo.

027. (FCC/TRE-CE/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS/2012) Em relação à norma ISO/IEC 27002, considere:

I – Para definição de uma estratégia de continuidade de negócios deve-se ter como meta o tempo esperado de recuperação, que, por sua vez, é derivado dos períodos máximos toleráveis de interrupção.

II – Os requisitos para controles de segurança de novos sistemas de informação ou melhorias em sistemas existentes devem constar nas especificações de requisitos de negócios dos sistemas.

III – Convém que os registros (log) de auditoria incluam, quando relevantes, os registros das tentativas de acesso ao sistema aceitas e rejeitadas.

IV – Entre os objetivos de controle de manuseio de mídias inclui-se o controle de descarte de mídias, sendo previstas, nessas normas, diretrizes de implementação para o descarte de forma segura e protegida.

Está correto o que se afirma em:

- a) I, II e III, apenas.
- b) I, II e IV, apenas.
- c) I, III e IV, apenas.
- d) II, III e IV, apenas.
- e) I, II, III e IV.



Todas as assertivas estão corretas. Uma boa fonte e estudo para vocês!

Sobre os **registros (log) de eventos**, convém que incluam:

- identificação dos usuários (**ID**);
- **atividades** do sistema;
- **datas, horários e detalhes de eventos-chave**;
- identidade/**localização** do dispositivo/sistema;

- registros das **tentativas de acesso** ao sistema ou a outros recursos de dados, **aceitos e rejeitados**;
- **alterações** na **configuração** do sistema;
- uso de **privilégios**;
- uso de aplicações e **utilitários** do sistema;
- **endereços e protocolos de rede**;
- **alarmes** provocados pelo sistema de controle de acesso;
- ativação e desativação dos **sistemas de proteção**;
- registros de **transações executadas**.

Letra e.

028. (CESGRANRIO/PETROBRAS/ANALISTA DE SISTEMAS JÚNIOR - PROCESSOS DE NEGÓCIOS/2010) De acordo com a NBR/ISO 27002, Segurança da Informação é a proteção da informação de vários tipos de ameaças para

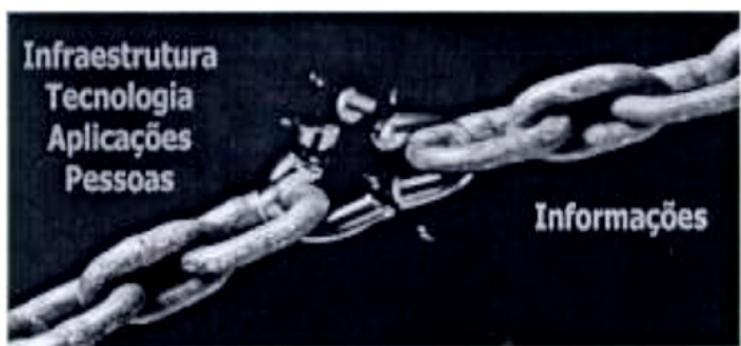
- a) garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.
- b) garantir a continuidade do negócio, minimizar as vulnerabilidades dos ativos de segurança, maximizar o retorno sobre os investimentos e as oportunidades de negócio.
- c) garantir a continuidade do negócio, facilitar o controle de acesso, maximizar o retorno sobre os investimentos e maximizar a disponibilidade dos sistemas de segurança.
- d) facilitar o controle de acesso, minimizar o risco ao negócio, maximizar a disponibilidade dos sistemas de segurança e as oportunidades de negócio.
- e) minimizar as vulnerabilidades dos ativos de segurança, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e a disponibilidade dos sistemas de segurança.



Segurança da informação é o processo de proteger a informação de diversos tipos de ameaças externas e internas para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação não deve ser tratada como um fator isolado e tecnológico apenas, mas sim como a **gestão inteligente da informação em todos os ambientes, desde o ambiente tecnológico passando pelas aplicações, infraestrutura e as pessoas**. Soluções pontuais isoladas não resolvem toda a problemática associada à segurança da informação. Segurança se faz em pedaços, porém todos eles integrados, como se fossem uma corrente.

Segurança se faz protegendo todos os elos da corrente, ou seja, todos os ativos (físicos, tecnológicos e humanos) que compõem seu negócio. Afinal, o poder de proteção da corrente está diretamente associado ao elo mais fraco!



Letra a.

029. (FUNDATÉC/TECNOLOGIA DA INFORMAÇÃO/PROCERGS/SEGURANÇA DA INFORMAÇÃO/2012) Segundo a norma NBR ISO/IEC 27002, o termo ‘segurança da informação’ pode ser definido como a preservação de três propriedades essenciais (ou principais), além de ser possível a adição de outras. As três consideradas principais são:

- a) Autenticidade, confidencialidade e integridade.
- b) Autenticidade, integridade e não repúdio.
- c) Confidencialidade, disponibilidade e integridade.
- d) Confidencialidade, integridade e não repúdio.
- e) Integridade, não repúdio e responsabilidade.



São princípios (ou pilares) básicos da segurança da informação:

Princípio	Conceito	Objetivo
Confidencialidade	<i>Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.</i>	Proteger contra o acesso não autorizado, mesmo para dados em trânsito.
Integridade	<i>Propriedade de salvaguarda da exatidão e completeza de ativos.</i>	Proteger informação contra modificação sem permissão; garantir a fidedignidade das informações.
Disponibilidade	<i>Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.</i>	Proteger contra indisponibilidade dos serviços (ou degradação); garantir aos usuários com autorização, o acesso aos dados.

Letra c.

GABARITO

- | | | |
|-------|-------|-------|
| 1. b | 11. d | 21. E |
| 2. e | 12. C | 22. d |
| 3. b | 13. E | 23. C |
| 4. e | 14. E | 24. C |
| 5. E | 15. C | 25. E |
| 6. e | 16. C | 26. C |
| 7. b | 17. d | 27. e |
| 8. d | 18. C | 28. a |
| 9. E | 19. C | 29. c |
| 10. e | 20. E | |

REFERÊNCIAS

Quintão, Patrícia L. **Notas de aula. Tecnologia da Informação.** 2020.

ABNT NBR ISO/IEC 27002. Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação. Rio de Janeiro, 2013.

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, 3^a. edição e 1001 questões comentadas de informática (Cespe/UnB), 2^a. edição, pela Editora Gen/Método.

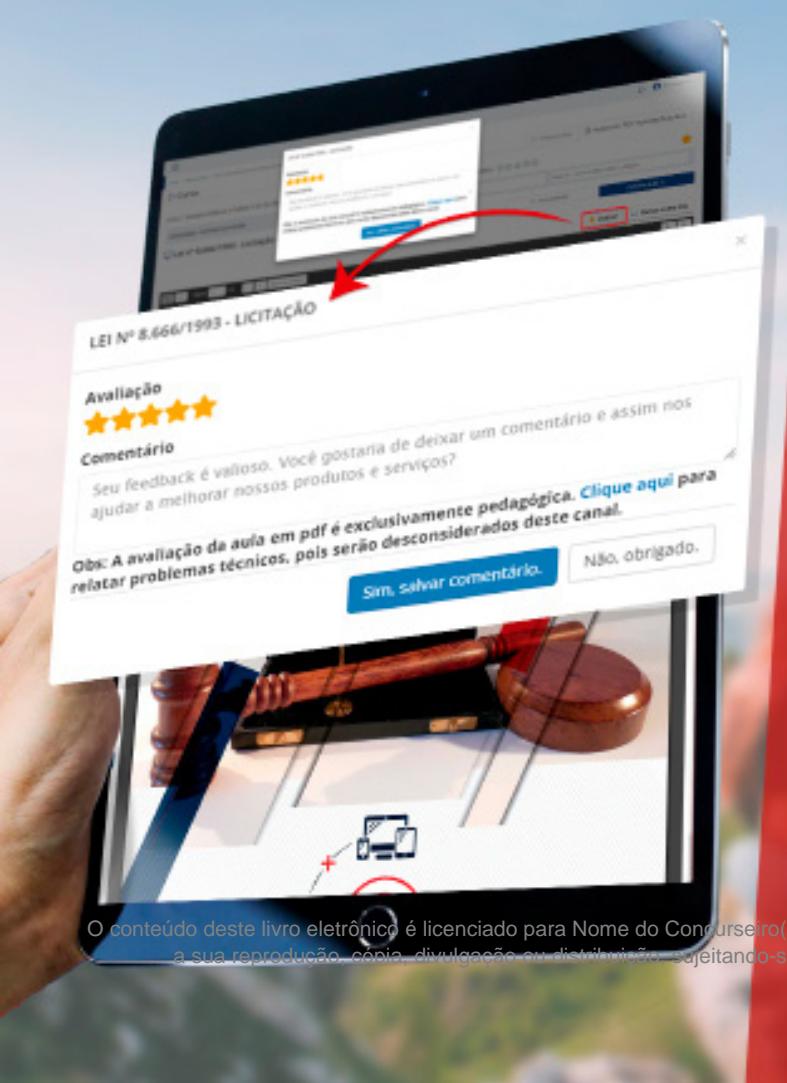
Foi aprovada nos seguintes concursos: Analista Legislativo, na especialidade de Administração de Rede, na Assembleia Legislativa do Estado de MG; Professora titular do Departamento de Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia; Professora substituta do DCC da UFJF; Analista 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 2^a Região RJ/ES, etc.

@coachpatriciaquintao

/profapatriciaquintao

@plquintao

t.me/coachpatriciaquintao



NÃO SE ESQUEÇA DE AVALIAR ESTA AULA!

SUA OPINIÃO É MUITO IMPORTANTE
PARA MELHORARMOS AINDA MAIS
NOSSOS MATERIAIS.

ESPERAMOS QUE TENHA GOSTADO
DESTA AULA!

PARA AVALIAR, BASTA CLICAR EM LER
A AULA E, DEPOIS, EM AVALIAR AULA.

AVALIAR 