



ASSOCIAÇÃO
BRASILEIRA
DE NORMAS
TÉCNICAS

NORMA BRASILEIRA ABNT NBR ISO/IEC 27001:2022

ABNT/CB-021

Publicada em 31.03.2023

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

ERRATA 1

Página v, Prefácio Nacional, 7º parágrafo

Substituir “ISO/IEC FDIS 27001:2022” por “ISO/IEC 27001:2022”

Página v, Prefácio Nacional, 8º parágrafo

Substituir “ABNT NBR ISO/IEC:2023” por “ABNT NBR ISO/IEC 27001:2013”

Página 1, Seção 3, 2º parágrafo

Substituir por:

A ISO e a IEC mantêm bases de dados terminológicos para uso na normalização nos seguintes endereços:

- ISO *Online browsing platform*: disponível em <http://www.iso.org/obp>
- IEC *Electropedia*: disponível em <http://www.electropedia.org/>

Página 3, Subseção 5.2, alínea c)

Remover vírgula entre “aplicáveis” e “relacionados”

Página 4, Subseção 6.1.1, alínea a)

Substituir “pode alcançar” por “possa alcançar”

Página 4, Subseção 6.1.2, alínea a), 1)

Substituir “aceitação do risco” por “aceitação de riscos”

Ref.: ABNT NBR ISO/IEC 27001:2022/Er1:2023

ABNT NBR ISO/IEC 27001:2022/Er1:2023

Página 4, Subseção 6.1.2, alínea b)

Substituir “avaliações de riscos de segurança da informação produzam” por “avaliações de riscos de segurança da informação repetidas produzam”

Página 5, Subseção 6.1.3, 1º parágrafo, alínea c), Nota 2

Substituir “são instruídos a” por “são “direcionados ao”

Página 6, Subseção 6.2, alínea b)

Substituir “(quando aplicável)” por “(se praticável)”

Página 6, Subseção 6.3, parágrafo único

Substituir “determinar as necessidades para as mudanças” por “determina necessidade para mudanças”

Página 7, Subseção 7.2, alínea b)

Substituir “essas pessoas são” por “essas pessoas sejam”

Página 7, Subseção 7.2, NOTA, 2ª linha

Substituir “ou a contratação de pessoas competentes” por “ou empregar ou contratar pessoas competentes”

Página 7, Subseção 7.3

Substituir por:

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

- a) da política da segurança da informação;
- b) da sua contribuição para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e
- c) das implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

Página 8, Subseção 7.5.2, parágrafo único, 1ª linha

Substituir “apropriada” por “apropriados(as)”

Página 8, Subseção 7.5.3, 3º parágrafo, 3ª linha

Substituir “como apropriada e controlada” por “como apropriado, e controlada”

Página 8, 7.5.3, NOTA, 1ª linha

Substituir “O acesso implica em uma decisão quanto à permissão para apenas ler” por “O acesso pode implicar em uma decisão quanto à permissão para apenas ver”

Página 8, Subseção 8.1, 3º Parágrafo, 2ª linha

Substituir “mudanças não previstas” por “mudanças não intencionais”

Página 9, Subseção 8.1, 4º parágrafo, 1ª linha

Substituir “produtos ou serviços terceirizados” por “produtos ou serviços providos externamente”

Página 9, Subseção 9.1, alínea a)

Substituir “incluindo controles e processos” por “incluindo processos e controles”

Página 9, Subseção 9.1, alínea b), 3ª linha

Substituir “a serem considerados válidos” por “para serem considerados válidos”

Página 12, Tabela A.1, 3ª linha “5.3 Segregação de funções”, 3ª coluna “Controle”

Substituir “Funções conflitantes e áreas de responsabilidade” por “Funções conflitantes e áreas de responsabilidade conflitantes”

Página 13, Tabela A.1, 4ª linha “5.11 Devolução de ativos”, 3ª coluna “Controle”

Substituir “após a mudança ou o encerramento da contratação ou acordo” por “em mudança ou o encerramento de seu emprego, contratação ou acordo”

Página 14, Tabela A.1, 1ª linha “5.17 Informações de autenticação”, 3ª coluna “Controle”

Substituir “uma gestão de processo” por “um processo de gestão”

Página 14, Tabela A.1, 2ª linha “5.18 Direitos de acesso”, 3ª coluna “Controle”

Substituir “política de tema específico” por “política específica por tema”

Página 14, Tabela A.1, 3ª linha “5.19 Segurança da informação nas relações com fornecedores”, 3ª coluna “Controle”

Substituir “para gerenciar a segurança da informação e os riscos associados” por “para gerenciar os riscos da segurança da informação associados”

ABNT NBR ISO/IEC 27001:2022/Er1:2023

Página 14, Tabela A.1, 5ª linha “5.21 Gestão da segurança da informação na cadeia de fornecimento de TC”, 2ª coluna

Substituir por:

Gestão da segurança da informação na cadeia de fornecimento de tecnologia de informação e comunicação (TIC)

Página 15, Tabela A.1, 7ª linha “5.31 Requisitos legais, estatutários, regulamentares e contratuais”, 3ª coluna “Controle”

Substituir “à abordagem” por “a abordagem”

Página 16, Tabela A.1, 2ª linha “5.35 Análise crítica independente da segurança da informação”, 3ª coluna “Controle”

Substituir “deve ser analisada criticamente, de forma independente, a intervalos planejados” por “devem ser analisadas criticamente, de forma independente a intervalos planejados”

Página 16, Tabela A.1, 3ª linha “5.36 Compliance com políticas, regras e normas para segurança da informação”, 3ª coluna “Controle”

Substituir “O *compliance* da política de segurança da informação da organização, políticas, regras e normas de temas específicos” por “O *compliance* com a política de segurança da informação da organização, políticas específicas por tema, regras e normas”

Página 16, Tabela A.1, 4ª linha “5.37 Documentação dos procedimentos de operação”, 3ª coluna “Controle”

Substituir “recursos de tratamento da informação” por “recursos de processamento das informações”

Página 16, Tabela A.1, última linha “6.3 Conscientização, educação e treinamento em segurança da informação”, 3ª coluna “Controle”

Substituir “políticas e procedimentos específicas por tema, pertinentes” por “políticas específicas por tema e procedimentos, conforme pertinente”

Página 18, Tabela A.1, 1ª linha “7.4 Monitoramento em segurança física”, 3ª coluna “Controle”

Substituir “para acesso” por “quanto a acesso”

Página 18, Tabela A.1, 4ª linha “7.7 Mesa limpa e tela limpa”, 3ª coluna “Controle”

Substituir “os recursos de tratamento das informações” por “os recursos de processamento de informações”

Página 18, Tabela A.1, 8ª linha “7.11 Serviços de infraestrutura”, 3ª coluna “Controle”

Substituir “instalações de tratamento de informações” por “instalações de processamento de informações”

Página 19, Tabela A.1, 1ª linha “7.14 Descarte seguro ou reutilização de equipamentos”, 3ª coluna “Controle”

Substituir “para assegurar que quaisquer dados confidenciais e *software* licenciado tenham sido removidos ou substituídos” por “para assegurar que quaisquer dados sensíveis e *software* licenciado tenham sido removidos ou sobrescritos”

Página 19, Tabela A.1, 3ª linha “8.1 Dispositivos endpoint do usuário”, 3ª coluna “Controle”

Substituir “As informações armazenadas, tratadas ou acessíveis” por “Informações armazenadas, processadas ou acessíveis”

Página 19, Tabela A.1, 6ª linha “8.5 Autenticação segura”, 3ª coluna “Controle”

Substituir “Tecnologia e procedimentos de autenticação seguros” por “Tecnologia e procedimentos de autenticação segura”

Página 19, Tabela A.1, 7ª linha “8.6 Gestão de capacidade”, 3ª coluna “Controle”

Substituir “de acordo com os requisitos atuais e esperados de capacidade” por “de acordo com os requisitos de capacidade atual e esperada”

Página 20, Tabela A.1, 3ª linha “8.11 Mascaramento de dados”, 3ª coluna “Controle”

Substituir “outros requisitos específicos por tema relacionados e requisitos de negócios” por “outras políticas específicas por tema relacionadas e requisitos do negócio”

Página 20, Tabela A.1, 4ª linha “8.12 Prevenção de vazamento de dados”, 3ª coluna “Controle”

Substituir “dispositivos que tratem” por “dispositivos que processem”

Página 20, Tabela A.1, 6ª linha “8.14 Redundância dos recursos de tratamento da informação”, 2ª coluna

Substituir por:

Redundância dos recursos de processamento de informações

ABNT NBR ISO/IEC 27001:2022/Er1:2023

Página 20, Tabela A.1, 6ª linha “8.14 Redundância dos recursos de tratamento da informação”, 2ª coluna, 3ª coluna “Controle”

Substituir “Os recursos de tratamento de informações” por “Recursos de processamento de informações”

Página 20, Tabela A.1, 7ª linha “8.16 Atividades de monitoramento”, 3ª coluna “Controle”

Substituir “por comportamentos anômalos e por ações apropriadas, tomadas” por “quanto a comportamentos anômalos e ações apropriadas devem ser tomadas”

Página 21, Tabela A.1, 1ª linha “8.17 Sincronização do relógio”, 3ª coluna “Controle”

Substituir “Os relógios dos sistemas de tratamento” por “Os relógios dos sistemas de processamento”

Página 21, Tabela A.1, 2ª linha 8.18 Uso de programas utilitários privilegiados”, 3ª coluna “Controle”

Substituir “capazes de substituir os controles de sistema e as aplicações” por “capazes de se sobrepor a controles de sistema e de aplicações”

Página 21, Tabela A.1, 7ª linha “8.23 Filtragem da web”, 3ª coluna “Controle”

Substituir “acesso a sites” por “acesso a websites”

Página 22, Tabela A.1, 1ª linha “8.27 Princípios de arquitetura e engenharia de sistemas seguros”, 3ª coluna “Controle”

Substituir “Princípios de engenharia de sistemas” por “Princípios para engenharia de sistemas”