CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

NORMA
BRASILEIRA

ABNT NBR ISO/IEC 27001

Terceira edição
23.11.2022

Versão corrigida
31.03.2023

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

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

ICS 35.040; 03.100.70

ISBN 978-85-07-09422-7

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO/IEC 27001:2022
23 páginas

© ISO/IEC 2022 - © ABNT 2022

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

© ISO/IEC 2022
Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT, único representante da ISO no território brasileiro.

© ABNT 2022
Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT.

ABNT
Av. Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 3974-2346
abnt@abnt.org.br
www.abnt.org.br

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Sumário

Página

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabelas

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas pelas partes interessadas no tema objeto da normalização.

Os Documentos Técnicos internacionais adotados são elaborados conforme as regras da ABNT Diretiva 3.

A ABNT chama a atenção para que, apesar de ter sido solicitada manifestação sobre eventuais direitos de patentes durante a Consulta Nacional, estes podem ocorrer e devem ser comunicados à ABNT a qualquer momento (Lei nº 9.279, de 14 de maio de 1996).

Os Documentos Técnicos ABNT, assim como as Normas Internacionais (ISO e IEC), são voluntários e não incluem requisitos contratuais, legais ou estatutários. Os Documentos Técnicos ABNT não substituem Leis, Decretos ou Regulamentos, aos quais os usuários devem atender, tendo precedência sobre qualquer Documento Técnico ABNT.

Ressalta-se que os Documentos Técnicos ABNT podem ser objeto de citação em Regulamentos Técnicos. Nestes casos, os órgãos responsáveis pelos Regulamentos Técnicos podem determinar as datas para exigência dos requisitos de quaisquer Documentos Técnicos ABNT.

A ABNT NBR ISO/IEC 27001 foi elaborada no Comitê Brasileiro de Tecnologias da Informação e Transformação Digital (ABNT/CB-021), pela Comissão de Estudo de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade (CE-021:004.027). O Projeto de Revisão circulou em Consulta Nacional conforme Edital nº 10, de 19.10.2022 a 17.11.2022.

A ABNT NBR ISO/IEC 27001 é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27001:2022, que foi elaborada pelo *Technical Committee Information Technology* (ISO/IEC JTC 1), *Subcommittee Cybersecurity and privacy protection* (SC 27).

A ABNT NBR ISO/IEC 27001:2022 cancela e substitui a ABNT NBR ISO/IEC 27001:2013, a qual foi tecnicamente revisada.

Esta versão corrigida da ABNT NBR ISO/IEC 27001:2022 incorpora a Errata 1, de 31.03.2023.

O Escopo da ABNT NBR ISO/IEC 27001 em inglês é o seguinte:

Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

0 Introdução

0.1 Geral

Este documento foi elaboradopara prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação . A adoção de um sistema de gestão de segurança da informação é uma decisão estratégica para uma organização. O estabelecimento e a implementação do sistema de gestão de segurança da informação de uma organização são influenciados pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais usados e tamanho e estrutura da organização. É esperado que todos estes fatores de influência mudem ao longo do tempo.

O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação pela aplicação de um processo de gestão de riscos, e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

É importante que um sistema de gestão da segurança da informação seja parte de, e esteja integrado com, os processos da organização e a estrutura de administração global, e que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles. É esperado que a implementação de um sistema de gestão de segurança da informação seja planejada de acordo com as necessidades da organização.

Este documento pode ser usado por partes internas e externas para avaliar a capacidade da organização de atender aos seus próprios requisitos de segurança da informação.

A ordem na qual os requisitos são apresentados neste documento não reflete sua importância nem implica na ordem em que devem ser implementados. Os itens listados são numerados apenas para fins de referência.

A ISO/IEC 27000 descreve a visão geral e o vocabulário do sistema de gestão da segurança da informação e referencia a família de normas da de sistema de gestão da segurança da informação (incluindo as ABNT NBR ISO/IEC 27003, ABNT NBR ISO/IEC 27004 e ABNT NBR ISO/IEC 27005), com termos e definições relacionados.

0.2 Compatibilidade com outras normas de sistemas de gestão

Este documento aplica estrutura de alto nível, títulos de subseções idênticos, textos idênticos, termos comuns e definições básicas apresentadas no Anexo SL da ISO/IEC *Directives,* Part 1, *Consolidated ISO Supplement*, desta forma mantendo a compatibilidade com outras normas de sistemas de gestão que adotaram o Anexo SL.

Esta abordagem comum especificada no Anexo SL será útil para aquelas organizações que escolhem operar um único sistema de gestão que atenda aos requisitos de duas ou mais normas de sistemas de gestão.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

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

1 Escopo

Este documento especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Este documento também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. Os requisitos estabelecidos neste documento são genéricos e destinam-se a ser aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza. A exclusão de quaisquer dos requisitos especificados nas Seções 4 a 10 não é aceitável quando a organização busca a conformidade com este documento.

2 Referências normativas

O documento a seguir é citado no texto de tal forma que seu conteúdo, total ou parcial, constitui requisito para este Documento.. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do referido documento (incluindo emendas).

ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

3 Termos e definições

Para os efeitos deste documento, aplicam-se os termos e definições da ISO/IEC 27000.

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

— ISO *Online browsing plataform*: disponível em http://www.iso.org/obp

— IEC *Electropedia*: disponível em http://www.electropedia.org/

4 Contexto da organização

4.1 Entendendo a organização e seu contexto

A organização deve determinar as questões internas e externas que são relevantes para o seu propósito e que afetam sua capacidade de alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação.

NOTA A determinação destas questões refere-se ao estabelecimento do contexto interno e externo da organização apresentado na ABNT ISO 31000:2018, 5.4.1[5].

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

4.2 Entendendo as necessidades e as expectativas das partes interessadas

A organização deve determinar:

a) as partes interessadas que são relevantes para o sistema de gestão da segurança da informação;

b) os requisitos relevantes dessas partes interessadas;

c) quais desses requisitos serão endereçados pelo sistema de gestão da segurança da informação.

NOTA Os requisitos das partes interessadas podem incluir requisitos legais e regulamentares, bem como obrigações contratuais.

4.3 Determinando o escopo do sistema de gestão da segurança da informação

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

Ao determinar este escopo, a organização deve considerar:

a) as questões internas e externas referenciadas em 4.1;

b) os requisitos referenciados em 4.2;

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

O escopo deve estar disponível como informação documentada.

4.4 Sistema de gestão da segurança da informação

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

5 Liderança

5.1 Liderança e comprometimento

A Alta Direção deve demonstrar sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação pelos seguintes meios:

a) assegurando que a política de segurança da informação e os objetivos de segurança da informação estejam estabelecidos e sejam compatíveis com a direção estratégica da organização;

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

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

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

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

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

f) orientando e apoiando pessoas a contribuir para a eficácia do sistema de gestão da segurança da informação;

g) promovendo a melhoria contínua; e

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

NOTA Referência a “negócios” neste documento pode ser interpretada amplamente para significar aquelas atividades que são o propósito principal da existência da organização.

5.2 Política

A Alta Direção deve estabelecer uma política de segurança da informação que:

a) seja apropriada ao propósito da organização;

b) inclua os objetivos de segurança da informação (ver 6.2) ou forneça a estrutura para estabelecer os objetivos de segurança da informação;

c) inclua o comprometimento de satisfazer os requisitos aplicáveis relacionados com a segurança da informação;

d) inclua o comprometimento com a melhoria contínua do sistema de gestão da segurança da informação.

A política da segurança da informação deve:

e) estar disponível como informação documentada;

f) ser comunicada dentro da organização;

g) estar disponível para as partes interessadas, conforme apropriado.

5.3 Papéis, responsabilidades e autoridades organizacionais

A Alta Direção deve assegurar que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídos e comunicados dentro da organização.

A Alta Direção deve atribuir a responsabilidade e autoridade para:

a) assegurar que o sistema de gestão da segurança da informação esteja em conformidade com os requisitos deste documento;

b) relatar sobre o desempenho do sistema de gestão da segurança da informação para a Alta Direção.

NOTA A Alta Direção pode também atribuir responsabilidades e autoridades para relatar sobre o desempenho do sistema de gestão da segurança da informação dentro da organização.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

6 Planejamento

6.1 Ações para abordar riscos e oportunidades

6.1.1 Geral

Ao planejar o sistema de gestão da segurança da informação, a organização deve considerar as questões referenciadas em 4.1 e os requisitos estabelecidos em 4.2, e determinar os riscos e oportunidades que precisam ser abordados para:

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

b) prevenir ou reduzir os efeitos indesejados; e

c) alcançar a melhoria contínua.

A organização deve planejar:

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

e) como

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

   2) avaliar a eficácia destas ações.

6.1.2 Avaliação de riscos de segurança da informação

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

a) estabeleça e mantenha critérios de riscos de segurança da informação que incluam:

   1) critérios de aceitação de riscos; e

   2) critérios para realizar as avaliações de riscos de segurança da informação;

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

c) identifique os riscos de segurança da informação:

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

   2) identificando os proprietários dos riscos.

d) analise os riscos de segurança da informação:

   1) avaliando as consequências potenciais que podem resultar se os riscos identificados em 6.1.2 c) 1) forem materializados;

   2) avaliando a probabilidade realística da ocorrência dos riscos identificados em 6.1.2 c) 1); e

   3) determinando os níveis de risco;

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

e) avalie os riscos de segurança da informação:

1) comparando os resultados da análise de riscos com os critérios de riscos estabelecidos em 6.1.2 a); e

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

A organização deve reter informação documentada sobre o processo de avaliação de riscos da segurança da informação.

6.1.3 Tratamento de riscos da segurança da informação

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

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

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

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

c) comparar os controles determinados em 6.1.3 b) com aqueles do Anexo A e verificar se nenhum controle necessário foi omitido;

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

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

d) elaborar uma Declaração de Aplicabilidade que contenha:

— os controles necessários (ver 6.1.3 b) e c));

— a justificativa para inclusões;

— se os controles necessários são implementados ou não; e

— a justificativa para a exclusão de quaisquer controles do Anexo A.

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

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

A organização deve reter a informação documentada relativa ao processo de tratamento de riscos da segurança da informação.

NOTA 4 O processo de tratamento e a avaliação de riscos da segurança da informação deste documento estão alinhados com os princípios e as diretrizes gerais estabelecidos na ABNT NBR ISO 31000[5].

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

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

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

Os objetivos da segurança da informação devem:

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

b) ser mensuráveis (se praticável);

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

d) ser monitorados;

e) ser comunicados;

f) ser atualizados, conforme apropriado;

g) ser disponibilizados como informação documentada.

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

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

h) o que será feito;

i) quais recursos serão necessários;

j) quem será responsável;

k) quando estará concluído; e

l) como os resultados serão avaliados.

6.3 Planejamento de mudanças

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

7 Apoio

7.1 Recursos

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

7.2 Competência

A organização deve:

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

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

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

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

d) reter informação documentada apropriada como evidência da competência.

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

7.3 Conscientização

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.

7.4 Comunicação

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

a) o que comunicar;

b) quando comunicar;

c) com quem comunicar;

d) como se comunicar.

7.5 Informação documentada

7.5.1 Geral

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

a) informação documentada requerida por este documento; e

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

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

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

2) à complexidade dos processos e suas interações; e

3) à competência das pessoas.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

7.5.2 Criando e atualizando

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

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

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

c) análise crítica e aprovação para pertinência e adequação.

7.5.3 Controle da informação documentada

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

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

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

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

c) distribuição, acesso, recuperação e uso;

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

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

f) retenção e disposição.

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

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

8 Operação

8.1 Planejamento e controle operacionais

A organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos e para implementar as ações determinadas na Seção 6:

— estabelecendo critérios para os processos;

— implementando controles dos processos de acordo com os critérios.

A informação documentada deve ser disponibilizada na abrangência necessária para gerar a confiança de que os processos estão sendo realizados conforme planejado.

A organização deve controlar as mudanças planejadas e analisar criticamente as consequências de mudanças não intencionais, tomando ações para mitigar quaisquer efeitos adversos, conforme necessário.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

A organização deve assegurar que os processos, produtos ou serviços providos externamente que são relevantes para o sistema de gestão da segurança da informação sejam controlados.

8.2 Avaliação de riscos da segurança da informação

A organização deve realizar avaliações de riscos da segurança da informação a intervalos planejados, ou quando mudanças significativas forem propostas ou ocorrerem, levando em conta os critérios estabelecidos em 6.1.2 a).

A organização deve reter informação documentada dos resultados das avaliações de riscos da segurança da informação.

8.3 Tratamento de riscos da segurança da informação

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

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

9 Avaliação de desempenho

9.1 Monitoramento, medição, análise e avaliação

A organização deve determinar:

a) o que precisa ser monitorado e medido, incluindo processos e controles da segurança da informação;

b) os métodos para monitoramento, medição, análise e avaliação, conforme aplicável, para assegurar resultados válidos. Convém que os métodos selecionados produzam resultados comparáveis e reproduzíveis para serem considerados válidos;

c) quando o monitoramento e a medição devem ser realizados;

d) quem deve monitorar e medir;

e) quando os resultados do monitoramento e da medição devem ser analisados e avaliados;

f) quem deve analisar e avaliar estes resultados.

Informação documentada deve ser disponibilizada como evidência dos resultados.

A organização deve avaliar o desempenho da segurança da informação e a eficácia do sistema de gestão da segurança da informação.

9.2 Auditoria interna

9.2.1 Geral

A organização deve conduzir auditorias internas a intervalos planejados para prover informações sobre se o sistema de gestão da segurança da informação:

a) está em conformidade com:

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

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

2) os requisitos deste documento;

b) está efetivamente implementado e mantido.

9.2.2 Programa de auditoria interna

A organização deve planejar, estabelecer, implementar e manter programa(s) de auditoria, incluindo frequência, métodos, responsabilidades, requisitos de planejamento e relato.

Ao estabelecer programa(s) de auditoria interna, a organização deve considerar a importância dos processos pertinentes e os resultados de auditorias anteriores.

A organização deve:

a) definir os critérios e o escopo da auditoria, para cada auditoria;

b) selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria;

c) assegurar que os resultados das auditorias sejam relatados para a gestão pertinente.

Informação documentada deve ser disponibilizada como evidência da implementação do(s) programa(s) de auditoria e dos resultados da auditoria.

9.3 Análise crítica pela Direção

9.3.1 Geral

A Alta Direção deve analisar criticamente o sistema de gestão da segurança da informação da organização em intervalos planejados, para assegurar a sua contínua adequação, pertinência e eficácia.

9.3.2 Entradas da análise crítica pela Direção

A análise crítica pela Direção deve incluir considerações em relação a:

a) situação das ações de análises críticas anteriores pela Direção;

b) mudanças nas questões internas e externas que sejam relevantes para o sistema de gestão da segurança da informação;

c) mudanças nas necessidades e expectativas das partes interessadas que sejam relevantes para o sistema de gestão da segurança da informação

d) *feedback* sobre o desempenho da segurança da informação, incluindo tendências para:

1) não conformidades e ações corretivas;

2) resultados da medição e monitoramento;

3) resultados de auditorias;

4) cumprimento dos objetivos da segurança da informação;

e) *feedback* das partes interessadas;

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

f) resultados da avaliação dos riscos e situação do plano de tratamento de riscos;

g) oportunidades para a melhoria contínua.

9.3.3 Resultados da análise crítica pela Direção

Os resultados da análise crítica pela Direção devem incluir decisões relativas às oportunidades para melhoria contínua e quaisquer necessidades de mudanças do sistema de gestão da segurança da informação.

Informação documentada deve ser disponibilizada como evidência dos resultados das análises críticas pela Direção.

10 Melhoria

10.1 Melhoria contínua

A organização deve melhorar continuamente a pertinência, a adequação e a eficácia do sistema de gestão da segurança da informação.

10.2 Não conformidade e ação corretiva

Quando uma não conformidade ocorre, a organização deve:

a) reagir à não conformidade e, conforme apropriado:

   1) tomar ações para controlá-la e corrigi-la; e

   2) lidar com as consequências;

b) avaliar a necessidade de ações para eliminar as causas de não conformidade, para evitar sua repetição ou ocorrência em outro lugar, por um dos seguintes meios:

   1) analisando criticamente a não conformidade;

   2) determinando as causas da não conformidade; e

   3) determinando se não conformidades similares existem, ou se podem potencialmente ocorrer;

c) implementar quaisquer ações necessárias;

d) analisar criticamente a eficácia de quaisquer ações corretivas tomadas; e

e) realizar mudanças no sistema de gestão da segurança da informação, quando necessário.

As ações corretivas devem ser apropriadas aos efeitos das não conformidades encontradas.

Informação documentada deve estar disponível como evidência de:

f) natureza das não conformidades e quaisquer ações subsequentes tomadas; e

g) resultados de qualquer ação corretiva.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Anexo A
(normativo)

Referência de controles da segurança da informação

Os controles da segurança da informação listados na Tabela A.1 são diretamente derivados e alinhados com aqueles listados na ABNT NBR ISO/IEC 27002:2022[1], Seções 5 a 8, e devem ser usados em alinhamento com 6.1.3.

Tabela A.1 – Controles da segurança da informação (continua)

5	**Controles organizacionais**	
5.1	Políticas de segurança da informação	**Controle** A política de segurança da informação e as políticas específicas por tema devem ser definidas, aprovadas pela direção, publicadas, comunicadas e reconhecidas pelo pessoal pertinente e pelas partes interessadas pertinentes, e analisadas criticamente em intervalos planejados e quando ocorrerem mudanças significativas.
5.2	Papéis e responsabilidades pela segurança da informação	**Controle** Papéis e responsabilidades pela segurança da informação devem ser definidos e alocados de acordo com as necessidades da organização.
5.3	Segregação de funções	**Controle** Funções conflitantes e áreas de responsabilidade conflitantes devem ser segregadas.
5.4	Responsabilidades da direção	**Controle** A direção deve requerer que todo o pessoal aplique a segurança da informação de acordo com a política da segurança da informação estabelecida, com as políticas específicas por tema e com os procedimentos da organização.
5.5	Contato com autoridades	**Controle** A organização deve estabelecer e manter contato com as autoridades relevantes.
5.6	Contato com grupos de interesse especial	**Controle** A organização deve estabelecer e manter contato com grupos de interesse especial ou com outros fóruns de especialistas em segurança e associações profissionais.
5.7	Inteligência de ameaças	**Controle** As informações relacionadas a ameaças à segurança da informação devem ser coletadas e analisadas para produzir inteligência de ameaças.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (continuação)

5	**Controles organizacionais**	
5.8	Segurança da informação no gerenciamento de projetos	**Controle** A segurança da informação deve ser integrada ao gerenciamento de projetos.
5.9	Inventário de informações e outros ativos associados	**Controle** Um inventário de informações e outros ativos associados, incluindo proprietários, deve ser desenvolvido e mantido.
5.10	Uso aceitável de informações e outros ativos associados	**Controle** Regras para o uso aceitável e procedimentos para o manuseio de informações e outros ativos associados devem ser identificados, documentados e implementados.
5.11	Devolução de ativos	**Controle** O pessoal e outras partes interessadas, conforme apropriado, devem devolver todos os ativos da organização em sua posse em mudança ou o encerramento de seu emprego, contratação ou acordo.
5.12	Classificação das informações	**Controle** As informações devem ser classificadas de acordo com as necessidades de segurança da informação da organização, com base na confidencialidade, integridade, disponibilidade e requisitos das partes interessadas relevantes.
5.13	Rotulagem de informações	**Controle** Um conjunto adequado de procedimentos para rotulagem de informações deve ser desenvolvido e implementado de acordo com o esquema de classificação de informações adotado pela organização.
5.14	Transferência de informações	**Controle** Regras, procedimentos ou acordos de transferência de informações devem ser implementados para todos os tipos de recursos de transferência dentro da organização e entre a organização e outras partes.
5.15	Controle de acesso	**Controle** Regras para controlar o acesso físico e lógico às informações e a outros ativos associados devem ser estabelecidas e implementadas com base nos requisitos de segurança da informação e de negócios.
5.16	Gestão de identidade	**Controle** O ciclo de vida completo das identidades deve ser gerenciado.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (continuação)

5	**Controles organizacionais**	
5.17	Informações de autenticação	**Controle** A alocação e a gestão de informações de autenticação devem ser controladas por um processo de gestão, incluindo aconselhar o pessoal sobre o manuseio adequado de informações de autenticação.
5.18	Direitos de acesso	**Controle** Os direitos de acesso às informações e a outros ativos associados devem ser provisionados, analisados criticamente, modificados e removidos de acordo com a política específica por tema e com as regras da organização para o controle de acesso.
5.19	Segurança da informação nas relações com fornecedores	**Controle** Processos e procedimentos devem ser definidos e implementados para gerenciar os riscos da segurança da informação associados com o uso dos produtos ou serviços dos fornecedores.
5.20	Abordagem da segurança da informação nos contratos de fornecedores	**Controle** Requisitos relevantes de segurança da informação devem ser estabelecidos e acordados com cada fornecedor, com base no tipo de relacionamento com o fornecedor.
5.21	Gestão da segurança da informação na cadeia de fornecimento de tecnologia de informação e comunicação (TIC)	**Controle** Processos e procedimentos devem ser definidos e implementados para gerenciar os riscos da segurança da informação associados à cadeia de fornecimento de produtos e serviços de TIC.
5.22	Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores	**Controle** A organização deve monitorar, analisar criticamente, avaliar e gerenciar regularmente a mudança nas práticas da segurança da informação dos fornecedores e na prestação de serviços.
5.23	Segurança da informação para uso de serviços em nuvem	**Controle** Os processos de aquisição, uso, gestão e saída de serviços em nuvem devem ser estabelecidos de acordo com os requisitos da segurança da informação da organização.
5.24	Planejamento e preparação da gestão de incidentes da segurança da informação	**Controle** A organização deve planejar e se preparar para gerenciar incidentes da segurança da informação, definindo, estabelecendo e comunicando processos, papéis e responsabilidades de gestão de incidentes da segurança da informação.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (continuação)

5	**Controles organizacionais**	
5.25	Avaliação e decisão sobre eventos da segurança da informação	**Controle** A organização deve avaliar os eventos da segurança da informação e decidir se categoriza como incidentes da segurança da informação.
5.26	Resposta a incidentes da segurança da informação	**Controle** Os incidentes da segurança da informação devem ser respondidos de acordo com os procedimentos documentados.
5.27	Aprendizado com incidentes de segurança da informação	**Controle** O conhecimento adquirido com incidentes de segurança da informação deve ser usado para fortalecer e melhorar os controles da segurança da informação.
5.28	Coleta de evidências	**Controle** A organização deve estabelecer e implementar procedimentos para identificação, coleta, aquisição e preservação de evidências relacionadas a eventos da segurança da informação.
5.29	Segurança da informação durante a disrupção	**Controle** A organização deve planejar como manter a segurança da informação em um nível apropriado durante a disrupção.
5.30	Prontidão de TIC para continuidade de negócios	**Controle** A prontidão de TIC deve ser planejada, implementada, mantida e testada com base nos objetivos de continuidade de negócios e nos requisitos de continuidade da TIC.
5.31	Requisitos legais, estatutários, regulamentares e contratuais	**Controle** Os requisitos legais, estatutários, regulamentares e contratuais pertinentes à segurança da informação e a abordagem da organização para atender a esses requisitos devem ser identificados, documentados e atualizados.
5.32	Direitos de propriedade intelectual	**Controle** A organização deve implementar procedimentos adequados para proteger os direitos de propriedade intelectual.
5.33	Proteção de registros	**Controle** Os registros devem ser protegidos contra perdas, destruição, falsificação, acesso não autorizado e liberação não autorizada.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (continuação)

5	**Controles organizacionais**	
5.34	Privacidade e proteção de DP	**Controle** A organização deve identificar e atender aos requisitos relativos à preservação da privacidade e à proteção de DP, de acordo com as leis e os regulamentos aplicáveis e requisitos contratuais.
5.35	Análise crítica independente da segurança da informação	**Controle** A abordagem da organização para gerenciar a segurança da informação e sua implementação, incluindo pessoas, processos e tecnologias, devem ser analisadas criticamente, de forma independente a intervalos planejados ou quando ocorrerem mudanças significativas.
5.36	*Compliance* com políticas, regras e normas para segurança da informação	**Controle** O *compliance* com a política de segurança da informação da organização, políticas específicas por tema, regras e normas deve ser analisado criticamente a intervalos regulares.
5.37	Documentação dos procedimentos de operação	**Controle** Os procedimentos de operação dos recursos de processamento das informações devem ser documentados e disponibilizados para o pessoal que necessite deles.
6	**Controles de pessoas**	
6.1	Seleção	**Controle** Verificações de antecedentes de todos os candidatos a serem contratados devem ser realizadas antes de ingressarem na organização e de modo contínuo, de acordo com as leis, os regulamentos e a ética aplicáveis, e devem ser proporcionais aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.
6.2	Termos e condições de contratação	**Controle** Os contratos trabalhistas devem declarar as responsabilidades do pessoal e da organização para a segurança da informação.
6.3	Conscientização, educação e treinamento em segurança da informação	**Controle** O pessoal da organização e partes interessadas relevantes devem receber treinamento, educação e conscientização em segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas específicas por tema e procedimentos, conforme pertinente para as suas funções.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (continuação)

6	**Controles de pessoas**	
6.4	Processo disciplinar	**Controle** Um processo disciplinar deve ser formalizado e comunicado, para tomar ações contra pessoal e outras partes interessadas relevantes que tenham cometido uma violação da política da segurança da informação.
6.5	Responsabilidades após encerramento ou mudança da contratação	**Controle** As responsabilidades e funções de segurança da informação que permaneçam válidas após o encerramento ou a mudança da contratação devem ser definidas, aplicadas e comunicadas ao pessoal e a outras partes interessadas pertinentes.
6.6	Acordos de confidencialidade ou não divulgação	**Controle** Acordos de confidencialidade ou não divulgação que reflitam as necessidades da organização para a proteção das informações devem ser identificados, documentados, analisados criticamente em intervalos regulares e assinados pelo pessoal e por outras partes interessadas pertinentes.
6.7	Trabalho remoto	**Controle** Medidas de segurança devem ser implementadas quando as pessoas estiverem trabalhando remotamente para proteger as informações acessadas, tratadas ou armazenadas fora das instalações da organização.
6.8	Relato de eventos de segurança da informação	**Controle** A organização deve fornecer um mecanismo para que as pessoas relatem eventos da segurança da informação observados ou suspeitos por meio de canais apropriados em tempo hábil.
7	**Controles físicos**	
7.1	Perímetros de segurança física	**Controle** Perímetros de segurança devem ser definidos e usados para proteger áreas que contenham informações e outros ativos associados.
7.2	Entrada física	**Controle** As áreas seguras devem ser protegidas por controles de entrada e pontos de acesso apropriados.
7.3	Segurança de escritórios, salas e instalações	**Controle** Segurança física para escritórios, salas e instalações deve ser projetada e implementada

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (continuação)

7	**Controles físicos**	
7.4	Monitoramento de segurança física	**Controle** As instalações devem ser monitoradas continuamente quanto a acesso físico não autorizado
7.5	Proteção contra ameaças físicas e ambientais	**Controle** Proteção contra ameaças físicas e ambientais, como desastres naturais e outras ameaças físicas intencionais ou não intencionais à infraestrutura, deve ser projetada e implementada.
7.6	Trabalho em áreas seguras	**Controle** Medidas de segurança para trabalhar em áreas seguras devem ser projetadas e implementadas.
7.7	Mesa limpa e tela limpa	**Controle** Regras de mesa limpa para documentos impressos e mídia de armazenamento removível e regras de tela limpa para os recursos de processamento de informações devem ser definidas e adequadamente aplicadas.
7.8	Localização e proteção de equipamentos	**Controle** Os equipamentos devem ser posicionados com segurança e proteção.
7.9	Segurança de ativos fora das instalações da organização	**Controle** Os ativos fora das instalações da organização devem ser protegidos.
7.10	Mídia de armazenamento	**Controle** As mídias de armazenamento devem ser gerenciadas por seu ciclo de vida de aquisição, uso, transporte e descarte, de acordo com o esquema de classificação e com os requisitos de manuseio da organização.
7.11	Serviços de infraestrutura	**Controle** As instalações de processamento de informações devem ser protegidas contra falhas de energia e outras disrupções causadas por falhas nos serviços de infraestrutura.
7.12	Segurança do cabeamento	**Controle** Os cabos que transportam energia ou dados, ou que sustentam serviços de informação, devem ser protegidos contra interceptação, interferência ou danos.
7.13	Manutenção de equipamentos	**Controle** Os equipamentos devem ser mantidos corretamente para assegurar a disponibilidade, integridade e confidencialidade da informação.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (continuação)

7	**Controles físicos**	
7.14	Descarte seguro ou reutilização de equipamentos	**Controle** Os itens dos equipamentos que contenham mídia de armazenamento devem ser verificados para assegurar que quaisquer dados sensíveis e *software* licenciado tenham sido removidos ou sobrescritos com segurança antes do descarte ou reutilização.
8	**Controles tecnológicos**	
8.1	Dispositivos *endpoint* do usuário	**Controle** Informações armazenadas, processadas ou acessíveis por meio de dispositivos *endpoint* do usuário devem ser protegidas.
8.2	Direitos de acessos privilegiados	**Controle** A atribuição e o uso de direitos de acessos privilegiados devem ser restritos e gerenciados
8.3	Restrição de acesso à informação	**Controle** O acesso às informações e a outros ativos associados deve ser restrito de acordo com a política específica por tema sobre controle de acesso.
8.4	Acesso ao código-fonte	**Controle** Os acessos de leitura e escrita ao código-fonte, ferramentas de desenvolvimento e bibliotecas de *software* devem ser adequadamente gerenciados.
8.5	Autenticação segura	**Controle** Tecnologia e procedimentos de autenticação segura devem ser implementados, com base em restrições de acesso à informação e à política específica por tema de controle de acesso.
8.6	Gestão de capacidade	**Controle** O uso dos recursos deve ser monitorado e ajustado de acordo com os requisitos de capacidade atual e esperada.
8.7	Proteção contra *malware*	**Controle** Proteção contra *malware* deve ser implementada e apoiada pela conscientização adequada do usuário.
8.8.	Gestão de vulnerabilidades técnicas	**Controle** Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas; a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (continuação)

8	**Controles tecnológicos**	
8.9	Gestão de configuração	**Controle** As configurações, incluindo configurações de segurança, de *hardware*, *software*, serviços e redes, devem ser estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente.
8.10	Exclusão de informações	**Controle** As informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento devem ser excluídas quando não forem mais necessárias.
8.11	Mascaramento de dados	**Controle** O mascaramento de dados deve ser usado de acordo com a política específica por tema da organização sobre o controle de acesso e outras políticas específicas por tema relacionadas e requisitos do negócio, levando em consideração a legislação aplicável.
8.12	Prevenção de vazamento de dados	**Controle** As medidas de prevenção de vazamento de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que processem, armazenem ou transmitam informações sensíveis.
8.13	*Backup* das informações	**Controle** Cópias de *backup* de informações, *software* e sistemas devem ser mantidas e testadas regularmente de acordo com a política específica por tema acordada sobre *backup*.
8.14	Redundância dos recursos de processamento de informações	**Controle** Recursos de processamento de informações devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade.
8.15	*Log*	**Controle** *Logs* que registrem atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados.
8.16	Atividades de monitoramento	**Controle** As redes, sistemas e aplicações devem ser monitorados quanto a comportamentos anômalos e ações apropriadas devem ser tomadas para avaliar possíveis incidentes de segurança da informação.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (continuação)

8	**Controles tecnológicos**	
8.17	Sincronização do relógio	**Controle** Os relógios dos sistemas de processamento de informações utilizados pela organização devem ser sincronizados com fontes de tempo aprovadas.
8.18	Uso de programas utilitários privilegiados	**Controle** O uso de programas utilitários que possam ser capazes de se sobrepor a controles de sistema e de aplicações deve ser restrito e rigorosamente controlado.
8.19	Instalação de *software* em sistemas operacionais	**Controle** Procedimentos e medidas devem ser implementados para gerenciar com segurança a instalação de *software* em sistemas operacionais.
8.20	Segurança de redes	**Controle** Redes e dispositivos de rede devem ser protegidos, gerenciados e controlados para proteger as informações em sistemas e aplicações.
8.21	Segurança dos serviços de rede	**Controle** Mecanismos de segurança, níveis de serviço e requisitos de serviços de rede devem ser identificados, implementados e monitorados.
8.22	Segregação de redes	**Controle** Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados nas redes da organização.
8.23	Filtragem da *web*	**Controle** O acesso a *websites* externos deve ser gerenciado para reduzir a exposição a conteúdo malicioso.
8.24	Uso de criptografia	**Controle** Regras para o uso efetivo da criptografia, incluindo o gerenciamento de chaves criptográfica devem ser definidas e implementadas.
8.25	Ciclo de vida de desenvolvimento seguro	**Controle** Regras para o desenvolvimento seguro de *software* e sistemas devem ser estabelecidas e aplicadas.
8.26	Requisitos de segurança da aplicação	**Controle** Requisitos de segurança da informação devem ser identificados, especificados e aprovados ao desenvolver ou adquirir aplicações.

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Tabela A.1 (conclusão)

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

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO RIO GRANDE DO SUL – CREA-RS - CNPJ 92.695.790/0001-95

Bibliografia

[1] ABNT NBR ISO/IEC 27002:2022, *Segurança da informação, segurança cibernética e proteção de privacidade - Controles de segurança da informação*

[2] ABNT NBR ISO/IEC 27003, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Orientações*

[3] ABNT NBR ISO/IEC 27004, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Monitoramento, medição, análise e avaliação*

[4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*

[5] ABNT NBR ISO 31000:2018, *Gestão de riscos - Diretrizes*

[6] ISO/IEC Directives - Part 1 and Consolidated ISO Supplement, *Procedure for the technical work – Procedures specific to ISO*

Exemplar para uso exclusivo - Convênio Sistema CONFEA/CREA/MUTUA - ABNT -

© ISO/IEC 2022 - © ABNT 2022 - Todos os direitos reservados

Impresso por: RS - Santana do Livramento - IMPRESSÃO