NORMA
BRASILEIRA

ABNT NBR ISO/IEC 27701

Primeira edição
25.11.2019

Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes

Security techniques — Extension to ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for privacy information management — Requirements and guidelines

ICS 35.030

ISBN 978-85-07-08355-9

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO/IEC 27701:2019
82 páginas

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

Sumário

Página

Prefácio Nacional viii
Introdução ix
0.1 Geral ix
0.2 Compatibilidade com outras normas de sistema de gestão ix
1 Escopo 1
2 Referências normativas 1
3 Termos, definições e abreviaturas 1
4 Geral 2
4.1 Estrutura deste documento 2
4.2 Aplicação dos requisitos da ABNT NBR ISO/IEC 27001:2013 3
4.3 Aplicação das diretrizes da ABNT NBR ISO/IEC 27002:2013 4
4.4 Cliente 5
5 Requisitos específicos de um SGPI relacionados à ABNT NBR ISO/IEC 27001 5
5.1 Geral 5
5.2 Contexto da organização 5
5.2.1 Entendendo a organização e seu contexto 5
5.2.2 Entendendo as necessidades e as expectativas das partes interessadas 6
5.2.3 Determinando o escopo do sistema de gestão da segurança da informação 6
5.2.4 Sistema de gestão da segurança da informação 6
5.3 Liderança 7
5.3.1 Liderança e comprometimento 7
5.3.2 Política 7
5.3.3 Autoridades, responsabilidades e papéis organizacionais 7
5.4 Planejamento 7
5.4.1 Ações para contemplar riscos e oportunidades 7
5.4.2 Objetivos de segurança da informação e planejamento para alcançá-los 8
5.5 Apoio 8
5.5.1 Recursos 8
5.5.2 Competência 8
5.5.3 Conscientização 9
5.5.4 Comunicação 9
5.5.5 Informação documentada 9
5.6 Operação 9
5.6.1 Planejamento e controle operacional 9
5.6.2 Avaliação de riscos de segurança da informação 9
5.6.3 Tratamento de riscos de segurança da informação 9
5.7 Avaliação de desempenho 9
5.7.1 Monitoramento, medição, análise e avaliação 9
5.7.2 Auditoria interna 9
5.7.3 Análise crítica pela Direção 10
5.8 Melhoria 10

5.8.1 Não conformidade e ação corretiva 10
5.8.2 Melhoria contínua 10
6 Diretrizes específicas de SGPI relacionadas à ABNT NBR ISO/IEC 27002 10
6.1 Geral 10
6.2 Políticas de segurança da informação 10
6.2.1 Orientação da Direção para segurança da informação 10
6.3 Organização da segurança da informação 11
6.3.1 Organização interna 11
6.3.2 Dispositivos móveis e trabalho remoto 12
6.4 Segurança em recursos humanos 12
6.4.1 Antes da contratação 12
6.4.2 Durante a contratação 13
6.4.3 Encerramento e mudança da contratação 13
6.5 Gestão de ativos 13
6.5.1 Responsabilidade pelos ativos 13
6.5.2 Classificação da informação 14
6.5.3 Tratamento de mídias 14
6.6 Controle de acesso 15
6.6.1 Requisitos do negócio para controle de acesso 15
6.6.2 Gerenciamento de acesso do usuário 16
6.6.3 Responsabilidades dos usuários 17
6.6.4 Controle de acesso ao sistema e à aplicação 17
6.7 Criptografia 18
6.7.1 Controles criptográficos 18
6.8 Segurança física e do ambiente 18
6.8.1 Áreas seguras 18
6.8.2 Equipamentos 19
6.9 Segurança nas operações 20
6.9.1 Responsabilidades e procedimentos operacionais 20
6.9.2 Proteção contra códigos maliciosos 20
6.9.3 Cópias de segurança 21
6.9.4 Registros e monitoramento 22
6.9.5 Controle de *software* operacional 23
6.9.6 Gestão de vulnerabilidades técnicas 23
6.9.7 Considerações quanto à auditoria de sistemas de informação 23
6.10 Segurança nas comunicações 23
6.10.1 Gerenciamento da segurança em redes 23
6.10.2 Transferência de informação 24
6.11 Aquisição, desenvolvimento e manutenção de sistemas 24
6.11.1 Requisitos de segurança de sistemas de informação 24
6.11.2 Segurança em processos de desenvolvimento e de suporte 25
6.11.3 Dados para teste 27
6.12 Relacionamento na cadeia de suprimento 27

6.12.1 Segurança da informação na cadeia de suprimento 27
6.12.2 Gerenciamento da entrega do serviço do fornecedor 28
6.13 Gestão de incidentes de segurança da informação 28
6.13.1 Gestão de incidentes de segurança da informação e melhorias 28
6.14 Aspectos da segurança da informação na gestão da continuidade do negócio 31
6.14.1 Continuidade da segurança da informação 31
6.14.2 Redundâncias 31
6.15 Compliance 31
6.15.1 Compliance com requisitos legais e contratuais 31
6.15.2 Análise crítica da segurança da informação 32
7 Diretrizes adicionais da ABNT NBR ISO/IEC 27002 para controladores de DP 33
7.1 Geral 33
7.2 Condições para coleta e tratamento 33
7.2.1 Identificação e documentação do propósito 33
7.2.2 Identificação de bases legais 34
7.2.3 Determinando quando e como o consentimento deve ser obtido 34
7.2.4 Obtendo e registrando o consentimento 35
7.2.5 Avaliação de impacto de privacidade 35
7.2.6 Contratos com operadores de DP 36
7.2.7 Controlador conjunto de DP 36
7.2.8 Registros relativos ao tratamento de DP 37
7.3 Obrigações dos titulares de DP 38
7.3.1 Determinando e cumprindo as obrigações para os titulares de DP 38
7.3.2 Determinando as informações para os titulares de DP 38
7.3.3 Fornecendo informações aos titulares de DP 39
7.3.4 Fornecendo mecanismos para modificar ou cancelar o consentimento 39
7.3.5 Fornecendo mecanismos para negar o consentimento ao tratamento de DP 40
7.3.6 Acesso, correção e/ou exclusão 41
7.3.7 Obrigações dos controladores de DP para informar aos terceiros 41
7.3.8 Fornecendo cópia do DP tratado 42
7.3.9 Tratamento de solicitações 42
7.3.10 Tomada de decisão automatizada 43
7.4 Privacy by Design e *Privacy by Default 43*
7.4.1 Limite de coleta 43
7.4.2 Limite de tratamento 43
7.4.3 Precisão e qualidade 44
7.4.4 Objetivos de minimização de DP 44
7.4.5 Anonimização e exclusão de DP ao final do tratamento 45
7.4.6 Arquivos temporários 45
7.4.7 Retenção 46
7.4.8 Descarte 46
7.4.9 Controle de transmissão de DP 46
7.5 Compartilhamento, transferência e divulgação de DP 46

7.5.1 Identificando as bases para a transferência de DP entre jurisdições 47
7.5.2 Países e organizações internacionais para os quais os DP podem ser transferidos 47
7.5.3 Registros de transferência de DP 47
7.5.4 Registro de divulgação de DP para terceiros 48
8 Diretrizes adicionais da ABNT NBR ISO/IEC 27002 para os operadores de DP 48
8.1 Geral 48
8.2 Condições para coleta e tratamento 48
8.2.1 Acordos com o cliente 48
8.2.2 Propósitos da organização 49
8.2.3 Uso de *marketing* e propaganda 49
8.2.4 Violando instruções 49
8.2.5 Obrigações do cliente 50
8.2.6 Registros relativos ao tratamento de DP 50
8.3 Obrigações para os titulares de DP 50
8.3.1 Obrigações para os titulares de DP 50
***8.4* *Privacy by design* e *privacy by default* 51**
8.4.1 Arquivos temporários 51
8.4.2 Retorno, transferência ou descarte de DP 51
8.4.3 Controles de transmissão de DP 52
8.5 Compartilhamento, transferência e divulgação de DP 52
8.5.1 Bases para a transferência de DP entre jurisdições 52
8.5.2 Países e organizações internacionais para os quais DP podem ser transferidos 53
8.5.3 Registros de DP divulgados para terceiros 53
8.5.4 Notificação de solicitações de divulgação de DP 54
8.5.5 Divulgações legalmente obrigatórias de DP 54
8.5.6 Divulgação de subcontratados usados para tratar DP 54
8.5.7 Contratação de um subcontratado para tratar DP 55
8.5.8 Mudança de subcontratado para tratar DP 55
Anexo A (normativo) **SGPI – Referências específicas de controles e objetivos de controle (Controladores de DP) 56**
Anexo B (normativo) **SGPI – Referências específicas de controles e objetivos de controle (Operadores de DP) 61**
Anexo C (informativo) **Mapeamento com a ISO/IEC 29100 ..... 64**
Anexo D (informativo) **Mapeamento com o *General Data Protection Regulation* 67**
Anexo E (informativo) **Mapeamento das ABNT NBR ISO/IEC 27018 e ISO/IEC 29151 ..... 71**
Anexo F (informativo) **Como aplicar a ABNT NBR ISO/IEC 27701 com as ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 ..... 75**
F.1 Como usar este documento 75
F.2 Exemplo de extensão de normas de segurança 76
Anexo N/A (informativo) **Mapeamento da ABNT NBR ISO/IEC 27701 com a LGPD 78**
Bibliografia 82

Tabelas

Tabela 1 – Localização dos requisitos específicos de SGPI e outras informações para a implementação dos controles da ABNT NBR ISO/IEC 27001:2013 3
Tabela 2 – Localização das diretrizes específicas de SGPI e outras informações para a implementação dos controles da ABNT NBR ISO/IEC 27002:2013 4
Tabela A.1 – Controles e objetivos de controle 56
Tabela B.1 – Controles e objetivos de controle 61
Tabela C.1 – Mapeamento dos controles para os controladores de DP e a ISO/IEC 29100 64
Tabela C.2 – Mapeamento dos controles para os operadores de DP e a ISO/IEC 29100 66
Tabela D.1 – Mapeamento da estrutura da ABNT NBR ISO/IEC 27701 com os artigos do GDPR 67
Tabela E.1 – Mapeamento da ABNT NBR ISO/IEC 27701 com as ABNT NBR ISO/IEC 27018 e ISO/IEC 29151 71
Tabela F.1 – Mapeamento da extensão do termo segurança da informação por privacidade ... 75
Tabela N/A.1 – Mapeamento da estrutura da ABNT NBR ISO/IEC 27701 com os artigos da LGPD 78

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 ABNT 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 27701 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-021), pela Comissão de Estudo de Técnicas de Segurança (CE-021:000.027). O Projeto circulou em Consulta Nacional conforme Edital nº 10, de 04.10.2019 a 07.11.2019.

A ABNT NBR ISO/IEC 27701 é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27701:2019, que foi elaborada pelo *Technical Committee Information Technology* (ISO/IEC JTC 1), *Subcommittee Information security, cybersecurity and privacy protection* (SC 27).

O Escopo da ABNT NBR ISO/IEC 27701 em inglês é o seguinte:

Scope

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for privacy management within the context of the organization.

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII.

Introdução

0.1 Geral

Quase todas as organizações tratam de dados pessoais (DP). Além disso, a quantidade e os tipos de DP tratados estão aumentando, assim como o número de situações em que uma organização precisa cooperar com outras organizações em relação ao tratamento de DP. A proteção da privacidade no contexto do tratamento de DP é uma necessidade da sociedade, bem como um tópico de legislação e/ou regulamentação dedicada em todo o mundo.

O Sistema de Gestão de Segurança da Informação (SGSI), definido na ABNT NBR ISO/IEC 27001, é projetado para permitir a adição de requisitos específicos setoriais, sem a necessidade de desenvolver um novo Sistema de Gestão. As Normas de Sistemas de Gestão ISO, incluindo as específicas por setor, são projetadas para poderem ser implementadas separadamente ou como um Sistema de Gestão combinado.

Os requisitos e diretrizes para a proteção de DP variam de acordo com o contexto da organização, em particular onde existe legislação e/ou regulamentação nacional. A ABNT NBR ISO/IEC 27001 requer que este contexto seja compreendido e levado em consideração. Este documento inclui o mapeamento para:

— a estrutura de privacidade e os princípios estabelecidos na ISO/IEC 29100;

— a ABNT NBR ISO/IEC 27018;

— a ISO/IEC 29151; e

— o Regulamento Geral de Proteção de Dados da UE.

No entanto, estes podem precisar ser interpretados para levar em consideração a legislação e/ou a regulamentação local.

Este documento pode ser usado por controladores de DP (incluindo aqueles que são controladores conjunto de DP) e operadores de DP (incluindo aqueles que usam operadores de DP subcontratados e aqueles que tratam DP ao atuar como subcontratados de operadores de DP).

Uma organização que cumpra os requisitos deste documento irá gerar evidências documentais de como lida com o tratamento de DP. Estas evidências podem ser usadas para facilitar acordos com parceiros de negócios nos quais o tratamento de DP é mutuamente relevante. Estas evidências também podem ajudar no relacionamento com outras partes interessadas. O uso deste documento em conjunto com a ABNT NBR ISO/IEC 27001 pode, se desejado, fornecer verificação independente destas evidências.

Este documento foi desenvolvido inicialmente como ISO/IEC 27552.

0.2 Compatibilidade com outras normas de sistema de gestão

Este documento aplica a estrutura desenvolvida pela ISO para melhorar o alinhamento entre as suas Normas de Sistemas de Gestão.

Este documento permite que uma organização alinhe ou integre seu SGPI aos requisitos de outras Normas de Sistemas de Gestão.

Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes

1 Escopo

Este documento especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização.

Este documento especifica os requisitos relacionados ao SGPI e fornece as diretrizes para os controladores de DP e operadores de DP que têm responsabilidade e responsabilização com o tratamento de DP.

Este documento é aplicável a todos os tipos e tamanhos de organizações, incluindo as companhias públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que são controladoras de DP e/ou que são operadoras de DP.

NOTA BRASILEIRA O motivo para a tradução do termo “personally identifiable information (PII)” por dados pessoais (DP) é o uso corrente da expressão dados pessoais no Brasil e sua adoção pela lei brasileira que trata de privacidade e proteção de dados pessoais (Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD).

2 Referências normativas

Os documentos a seguir são citados no texto de tal forma que seus conteúdos, totais ou parciais, constituem requisitos 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*

ABNT NBR ISO/IEC 27001:2013, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos*

ABNT NBR ISO/IEC 27002:2013, *Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação*

ISO/IEC 29100, *Information technology – Security techniques – Privacy Framework*

3 Termos, definições e abreviaturas

Para os efeitos deste documento, aplicam-se os termos e definições das ISO/IEC 27000 e ISO/IEC 29100.

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

— ISO *Online browsing platform*: disponível em https://www.iso.org/obp

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

3.1
controlador conjunto de DP
controlador de DP que determina os propósitos e formas do tratamento de DP, junto com um ou mais controladores de DP

3.2
sistema de gestão da privacidade da informação
SGPI
sistema de gestão da segurança da informação que considera a proteção da privacidade como potencialmente afetada pelo tratamento de DP

4 Geral

4.1 Estrutura deste documento

Este é um documento específico do setor relacionado às ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013.

Este documento tem foco nos requisitos específicos de um SGPI. O compliance com este documento está baseado na aderência a estes requisitos e aos requisitos da ABNT NBR ISO/IEC 27001:2013. Este documento amplia os requisitos da ABNT NBR ISO/IEC 27001:2013, levando em consideração a proteção da privacidade dos titulares de DP que possam ser potencialmente afetados pelo tratamento de DP, em complemento à segurança da informação. Para um melhor entendimento, diretrizes para implementação e outras informações relacionadas aos requisitos estão incluídas.

A Seção 5 apresenta os requisitos específicos de um SGPI e outras informações relacionadas aos requisitos de segurança da informação da ABNT NBR ISO/IEC 27001, apropriados para uma organização que atue como um controlador de DP ou como um operador de DP.

NOTA BRASILEIRA O motivo para a tradução do termo “PII processor” por “operador de DP” é o uso corrente da expressão operador de DP no Brasil e sua adoção pela lei brasileira que trata de privacidade e proteção de dados pessoais (Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD).

NOTA 1 Como complementação, a Seção 5 contém uma subseção para cada uma das seções da ABNT NBR ISO/IEC 27001:2013 que contém requisitos, mesmo no caso onde não existam requisitos específicos de SGPI ou outras informações.

A Seção 6 apresenta as diretrizes específicas de um SGPI e outras informações relacionadas aos controles de segurança da informação contidos na ABNT NBR ISO/IEC 27002 e diretrizes específicas de um SGPI para uma organização que esteja atuando como um controlador de DP ou como um operador de DP.

NOTA 2 Como complemento, a Seção 6 contém uma subseção para cada uma das seções que apresentam os objetivos ou os controles da ABNT NBR ISO/IEC 27002:2013, mesmo nos casos onde não existam diretrizes específicas de um SGPI ou outra informação.

A Seção 7 apresenta as diretrizes adicionais da ABNT NBR ISO/IEC 27002 para os controladores de DP, e a Seção 8 fornece as diretrizes adicionais contidas na ABNT NBR ISO/IEC 27002 para os operadores de DP.

O Anexo A apresenta os controles e objetivos de controles específicos de um SGPI para uma organização que atue como um controlador de DP (independentemente se ela usa ou não um operador de DP, e se está atuando ou não em conjunto com outro controlador de DP).

O Anexo B apresenta os controles e objetivos de controles específicos para uma organização que atue como um operador de DP (independentemente se ela subcontrata ou não o tratamento de DP para um outro operador de DP, e incluindo aqueles tratamentos de DP como subcontratados para os operadores de DP).

O Anexo C apresenta um mapeamento com a ISO/IEC 29100.

O Anexo D apresenta um mapeamento dos controles deste documento com o Regulamento da União Europeia sobre a Proteção de Dados.

O Anexo E apresenta um mapeamento com a ABNT NBR ISO/IEC 27018 e com a ISO/IEC 29151.

O Anexo F explica como as ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 são estendidas à proteção da privacidade, quando do tratamento de DP.

4.2 Aplicação dos requisitos da ABNT NBR ISO/IEC 27001:2013

A Tabela 1 apresenta a posição dos requisitos específicos de um SGPI neste documento, em relação à ABNT NBR ISO/IEC 27001.

Tabela 1 – Localização dos requisitos específicos de SGPI e outras informações para a implementação dos controles da ABNT NBR ISO/IEC 27001:2013

Seção da ABNT NBR ISO/IEC 27001:2013	Título	Subseção neste documento	Comentários
4	Contexto da organização	5.2	Requisitos adicionais
5	Liderança	5.3	Sem requisitos específicos de SGPI
6	Planejamento	5.4	Requisitos adicionais
7	Apoio	5.5	Sem requisitos específicos de SGPI
8	Operação	5.6	Sem requisitos específicos de SGPI
9	Avaliação de desempenho	5.7	Sem requisitos específicos de SGPI
10	Melhoria	5.8	Sem requisitos específicos de SGPI

NOTA A interpretação estendida de “segurança da informação”, de acordo com 5.1, sempre se aplica, mesmo quando não existem requisitos específicos de SGPI.

4.3 Aplicação das diretrizes da ABNT NBR ISO/IEC 27002:2013

A Tabela 2 apresenta a posição das diretrizes específicas de SGPI neste documento, em relação à ABNT NBR ISO/IEC 27002.

Tabela 2 – Localização das diretrizes específicas de SGPI e outras informações para a implementação dos controles da ABNT NBR ISO/IEC 27002:2013

Seção da ABNT NBR ISO/IEC 27002:2013	Título	Subseção neste documento	Comentários
5	Políticas de segurança da informação	6.2	Diretrizes adicionais
6	Organização da segurança da informação	6.3	Diretrizes adicionais
7	Segurança em recursos humanos	6.4	Diretrizes adicionais
8	Gestão de ativos	6.5	Diretrizes adicionais
9	Controle de acesso	6.6	Diretrizes adicionais
10	Criptografia	6.7	Diretrizes adicionais
11	Segurança física e do ambiente	6.8	Diretrizes adicionais
12	Segurança nas operações	6.9	Diretrizes adicionais
13	Segurança nas comunicações	6.10	Diretrizes adicionais
14	Aquisição, desenvolvimento e manutenção de sistemas	6.11	Diretrizes adicionais
15	Relacionamento na cadeia de suprimento	6.12	Diretrizes adicionais
16	Gestão de incidentes de segurança da informação	6.13	Diretrizes adicionais
17	Aspectos da segurança da informação na gestão da continuidade do negócio	6.14	Sem diretrizes adicionais para o SGPI
18	*Compliance*	6.15	Diretrizes adicionais

NOTA A interpretação estendida de “segurança da informação”, de acordo com 6.1, sempre se aplica, mesmo quando não existem diretrizes específicas de SGPI.

NOTA BRASILEIRA Neste documento, o termo *“Compliance”* foi mantido em inglês, apesar de na ABNT NBR ISO/IEC 27002:2013 ter sido traduzido como “Conformidade”, considerando o entendimento de que o termo *compliance* é mais abrangente e será então adotado na próxima revisão da ABNT NBR ISO/IEC 27002.

4.4 Cliente

Dependendo do papel da organização (ver 5.2.1), “cliente” pode ser entendido como:

a) uma organização que tenha um contrato com um controlador de DP (por exemplo, o cliente do controlador de DP);

NOTA 1 Isto pode ser o caso de uma organização que seja um controlador conjunto de DP.

NOTA 2 Uma pessoa individual em uma relação comercial com uma organização é referenciada como “titular de DP” neste documento.

b) um controlador de DP que tenha um contrato com um operador de DP (por exemplo, o cliente do operador de DP); ou

c) um operador de DP que tenha um contrato com um subcontratado para realizar o tratamento de DP (por exemplo, o cliente do suboperador de DP subcontratado).

NOTA 3 Onde “cliente” é mencionado na Seção 6, as provisões relacionadas podem ser aplicáveis nos contextos a), b) ou c).

NOTA 4 Onde “cliente” é mencionado na Seção 7 e no Anexo A, as provisões relacionadas são aplicáveis no contexto a).

NOTA 5 Onde “cliente” é mencionado na Seção 8 e no Anexo B, as provisões relacionadas são aplicáveis nos contextos b) e/ou c).

5 Requisitos específicos de um SGPI relacionados à ABNT NBR ISO/IEC 27001

5.1 Geral

Os requisitos da ABNT NBR ISO/IEC 27001:2013 mencionando “segurança da informação” devem ser estendidos para a proteção de privacidade, caso esta seja potencialmente afetada pelo tratamento de DP.

NOTA Na prática, onde “segurança da informação” é usado na ABNT NBR ISO/IEC 27001:2013, considerar “segurança da informação e privacidade” (ver Anexo F).

5.2 Contexto da organização

5.2.1 Entendendo a organização e seu contexto

Um requisito adicional à ABNT NBR ISO/IEC 27001:2013, 4.1, é:

A organização deve determinar o seu papel como um controlador de DP (incluindo a condição de controlador conjunto de DP) e/ou como um operador de DP.

A organização deve determinar os fatores externos e internos que são pertinentes para o seu contexto e que afetam a sua capacidade de alcançar os resultados pretendidos do seu SGPI. Por exemplo, isto pode incluir:

— legislação de privacidade, se aplicável;

— legislação de privacidade aplicável;

— decisões judiciais aplicáveis;

— contexto organizacional, governança, políticas e procedimentos aplicáveis;

— decisões administrativas aplicáveis;

— requisitos contratuais aplicáveis.

Onde a organização atua em ambos os papéis (por exemplo, como um controlador de DP e como um operador de DP), papéis separados devem ser determinados, cada qual estando sujeito a um conjunto separado de controles.

NOTA O papel da organização pode ser diferente para cada situação do tratamento de DP, uma vez que isto depende de quem determina os propósitos e meios de tratamento.

5.2.2 Entendendo as necessidades e as expectativas das partes interessadas

Um requisito adicional à ABNT NBR ISO/IEC 27001:2013, 4.2, é:

A organização deve incluir entre as suas partes interessadas (ver ABNT NBR ISO/IEC 27001:2013, 4.2), aquelas partes que têm interesses ou responsabilidades associados ao tratamento de DP, incluindo os titulares de DP.

NOTA 1 Outras partes interessadas podem incluir clientes (ver 4.4), autoridades supervisoras, outros controladores de DP, operadores de DP e seus subcontratados.

NOTA 2 Requisitos pertinentes para o tratamento de DP podem ser determinados por requisitos legais e regulatórios, por obrigações contratuais e por objetivos autodeterminados pela própria organização. Os princípios de privacidade definidos na ISO/IEC 29100 fornecem diretrizes relativas ao tratamento de DP.

NOTA 3 Como um elemento para demonstrar *compliance* com as obrigações da organização, algumas partes interessadas podem ter a expectativa de que a organização esteja em conformidade com normas específicas, como o Sistema de Gestão especificado neste documento, e/ou qualquer conjunto relevante de especificações. Estas partes podem solicitar uma auditoria de conformidade com estas normas, de forma independente.

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

Um requisito adicional à ABNT NBR ISO/IEC 27001:2013, 4.3, é:

Ao determinar o escopo do SGPI, a organização deve incluir o tratamento de DP.

NOTA A determinação do escopo do SGPI pode requerer uma revisão do escopo do sistema de gestão da segurança da informação, por causa da interpretação estendida de “segurança da informação”, de acordo com 5.1.

5.2.4 Sistema de gestão da segurança da informação

Um requisito adicional à ABNT NBR ISO/IEC 27001:2013, 4.4, é:

A organização deve estabelecer, implementar, manter e melhorar continuamente um SGPI de acordo com os requisitos da ABNT NBR ISO/IEC 27001:2013, Seções 4 a 10, estendidos pelos requisitos da Seção 5.

5.3 Liderança

5.3.1 Liderança e comprometimento

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 5.1, junto com a interpretação especificada em 5.1, se aplicam.

5.3.2 Política

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 5.2, junto com a interpretação especificada em 5.1, se aplicam.

5.3.3 Autoridades, responsabilidades e papéis organizacionais

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 5.3, junto com a interpretação especificada em 5.1, se aplicam.

5.4 Planejamento

5.4.1 Ações para contemplar riscos e oportunidades

5.4.1.1 Geral

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 6.1.1, junto com a interpretação especificada em 5.1, se aplicam.

5.4.1.2 Avaliação de riscos de segurança da informação

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 6.1.2, se aplicam, com as seguintes extensões:

A ABNT NBR ISO/IEC 27001:2013, 6.1.2 c) 1), é estendida como a seguir:

A organização deve aplicar o processo de avaliação de riscos de segurança da informação para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade, dentro do escopo do SGPI.

A organização deve aplicar o processo de avaliação de riscos de privacidade para identificar os riscos relativos ao tratamento de DP, dentro do escopo do SGPI.

A organização deve assegurar ao longo de todos os processos de avaliação de riscos que a relação entre a segurança da informação e a proteção de DP seja adequadamente gerenciada.

NOTA A organização pode aplicar um processo integrado de avaliação de riscos de privacidade e de segurança da informação, ou dois processos separados para a segurança da informação e os riscos relativos ao tratamento de DP.

A ABNT NBR ISO/IEC 27001:2013, 6.1.2 d) 1), é estendida como a seguir:

A organização deve avaliar as consequências potenciais para a organização e os titulares de DP que possam resultar, caso sejam materializados os riscos identificados na ABNT NBR ISO/IEC 27001:2013, 6.1.2 c), como estendido acima.

5.4.1.3 Tratamento dos riscos de segurança da informação

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 6.1.3, se aplicam, com os seguintes acréscimos:

A ABNT NBR ISO/IEC 27001:2013, 6.1.3 c), é estendida como a seguir:

Os controles determinados na ABNT NBR ISO/IEC 27001:2013, 6.1.3 b), devem ser comparados com os controles do Anexo A e/ou Anexo B, e com a ABNT NBR ISO/IEC 27001:2013, Anexo A, para verificar que nenhum controle necessário tenha sido omitido.

Ao avaliar a aplicabilidade dos objetivos de controle e dos controles da ABNT NBR ISO/IEC 27001:2013, Anexo A, para o tratamento dos riscos, os objetivos de controles e os controles devem ser considerados no contexto de ambos os riscos de segurança da informação, bem como os riscos relativos ao tratamento de DP, incluindo os riscos dos titulares de DP.

A ABNT NBR ISO/IEC 27001:2013, 6.1.3 d), é estendida como a seguir:

Produzir uma Declaração de Aplicabilidade que contenha:

— os controles necessários (ver ABNT NBR ISO/IEC 27001:2013, 6.1.3 b) e c));

— a justificativa para as suas inclusões;

— se os controles necessários estão implementados ou não; e

— a justificativa para excluir qualquer um dos controles do Anexo A e/ou do Anexo B, como também da ABNT NBR ISO/IEC 27001:2013, Anexo A, de acordo com a determinação da organização sobre os seus papéis (ver 5.2.1).

Nem todos os objetivos de controles e controles listados nos anexos precisam ser incluídos na implementação de um SGPI. A justificativa para exclusão pode considerar onde os controles não são considerados necessários pela avaliação de riscos, e onde eles não são requeridos pela (ou estão sujeitos sob exceções) legislação e/ou regulamentação, incluindo aquelas aplicáveis ao titular de DP.

5.4.2 Objetivos de segurança da informação e planejamento para alcançá-los

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 6.2, junto com a interpretação especificada em 5.1, se aplicam.

5.5 Apoio

5.5.1 Recursos

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 7.1, junto com a interpretação especificada em 5.1, se aplicam.

5.5.2 Competência

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 7.2, junto com a interpretação especificada em 5.1, se aplicam.

5.5.3 Conscientização

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 7.3, junto com a interpretação especificada em 5.1, se aplicam.

5.5.4 Comunicação

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 7.4, junto com a interpretação especificada em 5.1, se aplicam.

5.5.5 Informação documentada

5.5.5.1 Geral

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 7.5.1, junto com a interpretação especificada em 5.1, se aplicam.

5.5.5.2 Criando e atualizando

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 7.5.2, junto com a interpretação especificada em 5.1, se aplicam.

5.5.5.3 Controle da informação documentada

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 7.5.3, junto com a interpretação especificada em 5.1, se aplicam.

5.6 Operação

5.6.1 Planejamento e controle operacional

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 8.1, junto com a interpretação especificada em 5.1, se aplicam.

5.6.2 Avaliação de riscos de segurança da informação

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 8.2, junto com a interpretação especificada em 5.1, se aplicam.

5.6.3 Tratamento de riscos de segurança da informação

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 8.3, junto com a interpretação especificada em 5.1, se aplicam.

5.7 Avaliação de desempenho

5.7.1 Monitoramento, medição, análise e avaliação

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 9.1, junto com a interpretação especificada em 5.1, se aplicam.

5.7.2 Auditoria interna

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 9.2, junto com a interpretação especificada em 5.1, se aplicam.

5.7.3 Análise crítica pela Direção

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 9.3, junto com a interpretação especificada em 5.1, se aplicam.

5.8 Melhoria

5.8.1 Não conformidade e ação corretiva

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 10.1, junto com a interpretação especificada em 5.1, se aplicam.

5.8.2 Melhoria contínua

Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 10.2, junto com a interpretação especificada em 5.1, se aplicam.

6 Diretrizes específicas de SGPI relacionadas à ABNT NBR ISO/IEC 27002

6.1 Geral

Convém que as diretrizes da ABNT NBR ISO/IEC 27002:2013 que mencionam “segurança da informação” sejam estendidas para a proteção de privacidade, se potencialmente afetadas pelo tratamento de DP.

NOTA 1 Na prática, onde na ABNT NBR ISO/IEC 27002:2013 é usado “segurança da informação”, considerar “segurança da informação e privacidade” (ver Anexo F).

Convém que todos os objetivos de controle e os controles sejam considerados no contexto de ambos os riscos, tanto para segurança da informação como para os riscos de privacidade relacionados ao tratamento de DP.

NOTA 2 A menos que estabelecido de outra forma, por provisões específicas, na Seção 6, ou determinado pela organização de acordo com as jurisdições aplicáveis, as mesmas diretrizes se aplicam aos controladores de DP e aos operadores de DP.

6.2 Políticas de segurança da informação

6.2.1 Orientação da Direção para segurança da informação

6.2.1.1 Políticas para segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 5.1.1, bem como as seguintes diretrizes adicionais, se aplicam:

As diretrizes adicionais para a implementação do controle 5.1.1, Políticas para segurança da informação, da ABNT NBR ISO/IEC 27002:2013, são:

Seja para o desenvolvimento de políticas de privacidade separadas, ou para o acréscimo de políticas de segurança da informação, convém que a organização produza uma declaração quanto ao apoio e comprometimento para alcançar *compliance* com as regulamentações e legislações de proteção de DP aplicáveis, e com termos contratuais acordados entre a organização e seus parceiros, subcontratados e seus terceiros aplicáveis (clientes, fornecedores etc.), para os quais convém que se especifiquem claramente as responsabilidades entre eles.

Outras informações adicionais para o controle 5.1.1, Políticas para segurança da informação, da ABNT NBR ISO/IEC 27002:2013 são:

Para qualquer organização que trate DP, seja um controlador de DP ou um operador de DP, convém que seja considerada a regulamentação e/ou legislação de proteção de DP aplicável, durante o desenvolvimento e a manutenção de políticas de segurança da informação.

6.2.1.2 Análise crítica das políticas para segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 5.1.2, se aplicam.

6.3 Organização da segurança da informação

6.3.1 Organização interna

6.3.1.1 Responsabilidades e papéis da segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 6.1.1, e as seguintes diretrizes adicionais, se aplicam.

As diretrizes adicionais para a implementação do controle 6.1.1, Responsabilidades e papéis da segurança da informação, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização designe um ponto de contato para ser usado pelo cliente, em relação ao tratamento de DP. Quando a organização é um controlador de DP, designar um ponto de contato para os titulares de DP relacionados ao tratamento de seus próprios DP (ver 7.3.2).

Convém que a organização indique uma ou mais pessoas responsáveis pelo desenvolvimento, implementação, manutenção e monitoramento de um programa amplo de privacidade e governança da organização, para assegurar *compliance* com todas as leis e regulamentações aplicáveis, relacionadas ao tratamento de DP.

Convém que a pessoa responsável, quando apropriado:

— seja independente e reporte diretamente para o nível gerencial apropriado da organização, para assegurar uma efetiva gestão de riscos de privacidade;

— esteja envolvida na gestão de todas as questões que estejam relacionadas ao tratamento de DP;

— seja um especialista na legislação, na regulamentação e na prática de proteção de dados;

— atue como um ponto de contato junto às autoridades de supervisão;

— informe à Alta Direção e aos empregados da organização sobre as suas obrigações em relação ao tratamento de DP;

— forneça orientações em relação às avaliações de impacto de privacidade conduzidas pela organização.

NOTA Esta pessoa é chamada de "*Data Protection Officer*" em algumas jurisdições, as quais estabelecem em que momento tal posição é necessária, juntamente com a sua posição e papéis. Esta posição pode ser ocupada por um membro da organização ou terceirizado.

NOTA BRASILEIRA	Na legislação brasileira, esta pessoa é chamada de Encarregado de Proteção de Dados.

6.3.1.2 Segregação de funções

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 6.1.2, se aplicam.

6.3.1.3 Contato com autoridades

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 6.1.3, se aplicam.

6.3.1.4 Contato com grupos especiais

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 6.1.4, se aplicam.

6.3.1.5 Segurança da informação no gerenciamento de projetos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 6.1.5, se aplicam.

6.3.2 Dispositivos móveis e trabalho remoto

6.3.2.1 Política para o uso de dispositivo móvel

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 6.2.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para a implementação do controle 6.2.1, Dispositivos móveis e trabalho remoto, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização assegure que o uso de dispositivos móveis não conduza a um comprometimento de DP.

6.3.2.2 Trabalho remoto

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 6.2.2, se aplicam.

6.4 Segurança em recursos humanos

6.4.1 Antes da contratação

6.4.1.1 Seleção

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 7.1.1, se aplicam.

6.4.1.2 Termos e condições de contratação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 7.1.2, se aplicam.

6.4.2 Durante a contratação

6.4.2.1 Responsabilidades da Direção

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 7.2.1, se aplicam.

6.4.2.2 Conscientização, educação e treinamento em segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 7.2.2, e as seguintes diretrizes adicionais, se aplicam.

As diretrizes adicionais para a implementação do controle 7.2.2, Conscientização, educação e treinamento em segurança da informação, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que medidas sejam implementadas, incluindo a conscientização sobre notificação de incidentes, para assegurar que membros relevantes estejam cientes das possíveis consequências para a organização (por exemplo, consequências legais, perda de negócios e dano reputacional ou da marca), para os membros da organização (por exemplo, consequências disciplinares) e para o titular de DP (por exemplo, consequências físicas, materiais e emocionais) da violação de privacidade ou de regras de segurança e procedimentos, especialmente aqueles relacionados ao manuseio de DP.

NOTA Tais medidas podem incluir o uso de treinamento periódico apropriado para as pessoas que têm acesso a DP.

6.4.2.3 Procedimentos disciplinares

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 7.2.3, se aplicam.

6.4.3 Encerramento e mudança da contratação

6.4.3.1 Responsabilidades pelo encerramento ou mudança da contratação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 7.3.1, se aplicam.

6.5 Gestão de ativos

6.5.1 Responsabilidade pelos ativos

6.5.1.1 Inventário dos ativos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.1.1, se aplicam.

6.5.1.2 Proprietário dos ativos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.1.2, se aplicam.

6.5.1.3 Uso aceitável dos ativos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.1.3, se aplicam.

6.5.1.4 Devolução de ativos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.1.4, se aplicam.

6.5.2 Classificação da informação

6.5.2.1 Classificação da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.2.1, e as seguintes diretrizes adicionais, se aplicam.

As diretrizes adicionais para a implementação do controle 8.2.1, Classificação da informação, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que o sistema de classificação da informação da organização considere explicitamente DP como parte do esquema que ela implementa. Considerar DP dentro de todo o sistema de classificação é importante para entender qual DP a organização trata (por exemplo, tipo, categorias especiais), onde tal DP é armazenado e os sistemas pelos quais ele pode fluir.

6.5.2.2 Rótulos e tratamento da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.2.2, e as seguintes diretrizes adicionais, se aplicam.

As diretrizes adicionais para a implementação do controle 8.2.2, Rótulos e tratamento da informação, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização assegure que as pessoas sob o seu controle estejam conscientes da definição de DP e saibam como reconhecer uma informação que é DP.

NOTA BRASILEIRA Convém que a organização que trata DP sensíveis ou DP de crianças e adolescentes conscientizem seus colaboradores sobre a necessidade de cuidados específicos quando do tratamento destes DP, de acordo com a LGPD.

6.5.2.3 Tratamento dos ativos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.2.3, se aplicam.

6.5.3 Tratamento de mídias

6.5.3.1 Gerenciamento de mídias removíveis

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.3.1, e as seguintes diretrizes adicionais, se aplicam.

As diretrizes adicionais para a implementação do controle 8.3.1, Gerenciamento de mídias removíveis, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização documente qualquer uso de mídia removível e/ou de dispositivos para o armazenamento de DP. Convém que, quando possível, a organização use mídias físicas removíveis e/ou dispositivos que permitam a criptografia, quando do armazenamento de DP. Convém que mídias

não criptografadas sejam usadas somente quando for inevitável, e em situações onde a mídia e/ou os dispositivos não criptografados forem usados, convém que a organização implemente procedimentos e controles compensatórios (por exemplo, embalagens invioláveis) para tratar os riscos ao DP.

Outras informações adicionais para o controle 8.3.1, Gerenciamento de mídias removíveis, da ABNT NBR ISO/IEC 27002:2013, são:

Mídia removível que é levada para fora do ambiente físico da organização está propensa à perda, dano e acesso inapropriado. Criptografar a mídia removível aumenta o nível de proteção para o DP, o que leva à redução dos riscos de privacidade e de segurança, caso a mídia removível seja comprometida.

6.5.3.2 Descarte de mídias

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.3.2, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 8.3.2, Descarte de mídias, da ABNT NBR ISO/IEC 27002:2013, são:

Onde mídias removíveis que armazenam DP forem descartadas, convém que procedimentos de descarte seguros sejam incluídos na informação documentada e implementados para assegurar que DP armazenados previamente não sejam acessíveis.

6.5.3.3 Transferência física de mídias

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.3.3, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 8.3.3, Transferência física de mídias, da ABNT NBR ISO/IEC 27002:2013, são:

Quando mídias físicas são usadas para transferência da informação, convém que um sistema seja implementado para registrar as entradas e saídas das mídias físicas contendo DP, incluindo o tipo de mídia física, o receptor/remetente autorizado, a data e o horário, e o número da mídia física. Quando possível, convém que medidas adicionais, como criptografia, sejam implementadas para assegurar que os dados somente possam ser acessados no ponto de destino e não durante o transporte.

Convém que a organização submeta a mídia física contendo DP a um procedimento de autorização antes de deixar as suas instalações e que assegure que o DP não seja acessível para qualquer outra pessoa que não o pessoal autorizado.

NOTA Uma medida possível para assegurar que a mídia física contendo DP que esteja deixando as instalações da organização não seja acessível de um modo geral é criptografar o DP relacionado e restringir a capacidade de decriptação apenas às pessoas autorizadas.

6.6 Controle de acesso

6.6.1 Requisitos do negócio para controle de acesso

6.6.1.1 Política de controle de acesso

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.1.1, se aplicam.

6.6.1.2 Acesso às redes e aos serviços de rede

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.1.2, se aplicam.

6.6.2 Gerenciamento de acesso do usuário

6.6.2.1 Registro e cancelamento de usuário

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.2.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 9.2.1, Registro e cancelamento de usuário, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que procedimentos para registro e cancelamento de usuários que administrem ou operem sistemas e serviços que tratam DP considerem a situação onde o controle de acesso do usuário para aqueles usuários esteja comprometido, como a corrupção ou o comprometimento de senhas ou outros registros de dados de usuários (por exemplo, como um resultado de uma divulgação inadvertida).

Convém que a organização não reemita aos usuários qualquer *login* expirado ou desativado dos sistemas e serviços que tratam DP.

No caso em que a organização fornece o tratamento de DP como um serviço, o cliente pode ser responsável por alguns ou todos os aspectos do gerenciamento do ID do usuário. Convém que estes casos sejam incluídos na informação documentada.

Algumas jurisdições impõem requisitos específicos em relação à frequência de verificação de credenciais de autenticação não usadas, relativas aos sistemas que tratam DP. Convém que as organizações que operam nestas jurisdições considerem o *compliance* com estes requisitos.

6.6.2.2 Provisionamento para acesso de usuário

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.2.2, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 9.2.2, Provisionamento para acesso de usuário, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização mantenha um registro preciso e atualizado dos perfis dos usuários criados para os usuários que tenham sido autorizados a acessar o sistema de informação e os DP neles contidos. Este perfil compreende um conjunto de dados sobre aquele usuário, incluindo o ID de usuário, necessário para implementar os controles técnicos identificados que fornecem acesso autorizado.

A implementação dos ID individuais de acesso do usuário permite que sistemas configurados identifiquem adequadamente quem acessou DP e quais acréscimos, exclusões ou mudanças eles fizeram. Da mesma forma que a organização é protegida, os usuários são também protegidos, uma vez que eles podem identificar o que foi tratado e o que não foi tratado.

No caso em que a organização fornece tratamento de DP como um serviço, o cliente pode ser responsável por alguns ou todos os aspectos de gerenciamento de acesso. Onde apropriado, convém que a organização forneça aos clientes os meios para realizar o gerenciamento de acesso, como fornecer direitos administrativos para gerenciar ou encerrar o acesso. Convém que estes casos sejam incluídos na informação documentada.

6.6.2.3 Gerenciamento de direitos de acesso privilegiado

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.2.3, se aplicam.

6.6.2.4 Gerenciamento da informação de autenticação secreta de usuários

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.2.4, se aplicam.

6.6.2.5 Análise crítica dos direitos de acesso de usuário

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.2.5, se aplicam.

6.6.2.6 Retirada ou ajuste dos direitos de acesso

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.2.6, se aplicam.

6.6.3 Responsabilidades dos usuários

6.6.3.1 Uso da informação de autenticação secreta

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.3.1, se aplicam.

6.6.4 Controle de acesso ao sistema e à aplicação

6.6.4.1 Restrição de acesso à informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.4.1, se aplicam.

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

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.4.2, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 9.4.2, Procedimentos seguros de entrada no sistema (*log-on*), da ABNT NBR ISO/IEC 27002:2013, são:

Onde requerido pelo cliente, convém que a organização forneça a capacidade para os procedimentos seguros de entrada para quaisquer contas de usuários sob o controle do cliente.

6.6.4.3 Sistema de gerenciamento de senha

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.4.3, se aplicam.

6.6.4.4 Uso de programas utilitários privilegiados

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.4.4, se aplicam.

6.6.4.5 Controle de acesso ao código-fonte de programas

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 9.4.5, se aplicam.

6.7 Criptografia

6.7.1 Controles criptográficos

6.7.1.1 Política para o uso de controles criptográficos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 10.1.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 10.1.1, Política para o uso de controles criptográficos, da ABNT NBR ISO/IEC 27002:2013, são:

Algumas jurisdições podem requerer o uso de criptografia para proteger tipos específicos de DP, como dados sobre saúde, números de registros de residência, números de passaportes e números de licença de motorista.

Convém que a organização forneça informações para o cliente em relação às circunstâncias em que ela usa a criptografia para proteger os DP que ela trata. Convém que a organização também forneça informações para o cliente sobre quaisquer capacidades que ela fornece, que possam atender ao cliente, aplicando sua própria proteção de criptografia.

6.7.1.2 Gerenciamento de chaves

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 10.1.2, se aplicam.

6.8 Segurança física e do ambiente

6.8.1 Áreas seguras

6.8.1.1 Perímetro de segurança física

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.1.1, se aplicam.

6.8.1.2 Controles de entrada física

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.1.2, se aplicam.

6.8.1.3 Segurança em escritórios, salas e instalações

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.1.3, se aplicam.

6.8.1.4 Proteção contra ameaças externas e do meio ambiente

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.1.4, se aplicam.

6.8.1.5 Trabalhando em áreas seguras

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.1.5, se aplicam.

6.8.1.6 Áreas de entrega e de carregamento

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.1.6, se aplicam.

6.8.2 Equipamentos

6.8.2.1 Localização e proteção do equipamento

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.2.1, se aplicam.

6.8.2.2 Utilidades

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.2.2, se aplicam.

6.8.2.3 Segurança do cabeamento

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.2.3, se aplicam.

6.8.2.4 Manutenção dos equipamentos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.2.4, se aplicam.

6.8.2.5 Remoção de ativos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.2.5, se aplicam.

6.8.2.6 Segurança de equipamentos e ativos fora das dependências da organização

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.2.6, se aplicam.

6.8.2.7 Reutilização ou descarte seguro de equipamentos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.2.7, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 11.2.7, Reutilização ou descarte seguro de equipamentos, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização assegure que, quando um espaço de armazenamento é realocado, qualquer DP previamente guardado naquele espaço de armazenamento não seja acessível.

Quando for excluído um DP mantido em um sistema de informação, questões de desempenho podem significar que a exclusão explícita daquele DP é impraticável. Isto cria o risco de que um outro usuário possa acessar o DP. Convém que tal risco seja evitado por meio do uso de medidas técnicas específicas.

Para a reutilização ou descarte seguro, convém que os equipamentos contendo mídias de armazenamento que possivelmente possam armazenar DP sejam tratados como efetivamente contendo DP.

6.8.2.8 Equipamento de usuário sem monitoração

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.2.8, se aplicam.

6.8.2.9 Política de mesa limpa e tela limpa

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 11.2.9, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 11.2.9, Política de mesa limpa e tela limpa, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização restrinja a criação de material físico que inclua DP ao mínimo necessário para atender ao propósito do tratamento identificado.

6.9 Segurança nas operações

6.9.1 Responsabilidades e procedimentos operacionais

6.9.1.1 Documentação dos procedimentos de operação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.1.1, se aplicam.

6.9.1.2 Gestão de mudanças

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.1.2, se aplicam.

6.9.1.3 Gestão de capacidade

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.1.3, se aplicam.

6.9.1.4 Separação dos ambientes de desenvolvimento, teste e de produção

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.1.4, se aplicam.

6.9.2 Proteção contra códigos maliciosos

6.9.2.1 Controles contra códigos maliciosos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.2.1, se aplicam.

6.9.3 Cópias de segurança

6.9.3.1 Cópias de segurança das informações

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.3.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 12.3.1, Cópias de segurança das informações, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização tenha uma política que considere os requisitos para cópia de segurança, recuperação e restauração de DP (que pode ser parte de uma política de cópias de segurança das informações globais), bem como quaisquer requisitos adicionais (por exemplo, requisitos legais e/ou contratuais) para a eliminação de DP contido nas informações mantidas para os requisitos de cópias de segurança.

As responsabilidades específicas de DP nesta questão podem depender do cliente. Convém que a organização assegure que o cliente tenha sido informado dos limites do serviço em relação à cópia de segurança.

Onde a organização explicitamente fornece serviços de cópias de segurança e recuperação para os clientes, convém que a organização forneça a eles informações claras sobre as suas capacidades quanto à cópia de segurança e recuperação de DP.

Algumas jurisdições impõem requisitos específicos relacionados à frequência de cópias de segurança de DP, à peridiocidade de análises críticas e de testes de cópias de segurança, ou quanto aos procedimentos para recuperação de DP. Convém que as organizações que operam nestas jurisdições demonstrem *compliance* com estes requisitos.

Podem ocorrer situações onde o DP precisa ser recuperado, talvez devido ao mau funcionamento do sistema, a um ataque ou a um desastre. Quando o DP é restaurado (normalmente de uma cópia de segurança), os processos necessários precisam estar implementados para assegurar que o DP seja restaurado em uma condição onde a integridade do DP possa ser assegurada, e/ou onde a imprecisão e/ou informação incompleta de DP sejam identificadas e os processos implementados para resolvê-los (o que pode envolver o titular de DP).

Convém que a organização tenha um procedimento e um registro do trabalho de restauração do DP. Como um mínimo, convém que o registro do trabalho de restauração do DP contenha:

— o nome da pessoa responsável pela restauração;

— uma descrição do DP restaurado.

Algumas jurisdições determinam o conteúdo dos *logs* dos esforços de restauração dos DP. Convém que as organizações sejam capazes de documentar o *compliance* com quaisquer requisitos específicos aplicados àquela jurisdição, para a restauração do conteúdo dos *logs*. Convém que as conclusões de tais deliberações sejam incluídas em uma informação documentada.

O uso de subcontratados para armazenar réplicas ou cópias de segurança das informações de DP tratados está coberto neste documento pelos controles aplicados ao tratamento de DP subcontratado (ver 6.5.3.3, 6.12.1.2). Onde ocorre a transferência de mídias físicas relativas a cópias de segurança em restauração, isto também é coberto neste documento pelos controles (6.10.2.1).

6.9.4 Registros e monitoramento

6.9.4.1 Registros de eventos (*logs)*

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.4.1, e as seguintes diretrizes adicionais se aplicam:

As diretrizes adicionais para implementação do controle 12.4.1, Registros de eventos, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que um processo seja implementado para analisar criticamente os registros de eventos (*logs)* usando processos contínuos de alerta e monitoramento automatizados, ou também manualmente, onde convém que tal análise crítica seja desempenhada em uma periodicidade especificada e documentada, visando identificar irregularidades e propor esforços de remediação.

Quando possível, convém que os registros de eventos (*logs)* gravem o acesso ao DP, incluindo por quem, quando, qual titular de DP foi acessado e quais mudanças (se houver alguma) foram feitas (adições, modificações ou exclusões), como um resultado do evento.

Onde múltiplos provedores de serviços estão envolvidos no fornecimento dos serviços, pode haver papéis variados ou compartilhados na implementação desta diretriz. Convém que estes papéis sejam claramente definidos e incluídos na informação documentada, e convém que um acordo sobre qualquer acesso ao *log* entre os provedores seja considerado.

As diretrizes para implementação de operadores de DP são:

Convém que a organização determine um critério em relação a quando e como as informações de *log* podem se tornar disponíveis ou usáveis pelo cliente. Convém que estes critérios estejam disponíveis para o cliente.

Onde a organização permite que os seus clientes acessem os registros de *log* controlados pela organização, convém que a organização implemente controles apropriados para assegurar que o cliente possa apenas acessar os registros que estão relacionados às atividades daquele cliente, que não possa acessar quaisquer registros de *log* os quais estejam relacionados às atividades de outros clientes e que não possa alterar os *logs* de modo algum.

6.9.4.2 Proteção das informações dos registros de eventos (*logs*)

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.4.2, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 12.4.2, Proteção das informações dos registros de eventos (*logs*), da ABNT NBR ISO/IEC 27002:2013, são:

As informações dos registros de eventos (*logs*) para, por exemplo, diagnósticos operacionais e monitoramento da segurança podem conter DP. Convém que medidas como controle de acesso (ver ABNT NBR ISO/IEC 27002:2013, 9.2.3) sejam implementadas para assegurar que as informações de eventos sejam somente usadas conforme pretendido.

Convém que um procedimento, preferencialmente automatizado, seja implementado para assegurar que as informações de eventos sejam excluídas ou anonimizadas como especificado na programação de retenção (ver 7.4.7).

6.9.4.3 Registros de eventos (*log*) de administrador e operador

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.4.3, se aplicam.

6.9.4.4 Sincronização dos relógios

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.4.4, se aplicam.

6.9.5 Controle de *software* operacional

6.9.5.1 Instalação de *software* nos sistemas operacionais

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.5.1, se aplicam.

6.9.6 Gestão de vulnerabilidades técnicas

6.9.6.1 Gestão de vulnerabilidades técnicas

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.6.1, se aplicam.

6.9.6.2 Restrições quanto à instalação de *software*

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.6.2, se aplicam.

6.9.7 Considerações quanto à auditoria de sistemas de informação

6.9.7.1 Controles de auditoria de sistemas de informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 12.7.1, se aplicam.

6.10 Segurança nas comunicações

6.10.1 Gerenciamento da segurança em redes

6.10.1.1 Controles de redes

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 13.1.1, se aplicam.

6.10.1.2 Segurança dos serviços de rede

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 13.1.2, se aplicam.

6.10.1.3 Segregação de redes

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 13.1.3, se aplicam.

6.10.2 Transferência de informação

6.10.2.1 Políticas e procedimentos para transferência de informações

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 13.2.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 13.2.1, políticas e procedimentos para transferência de informações, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização considere procedimentos para assegurar que regras relativas ao tratamento de DP são mandatórias por todo o sistema e fora dele, onde aplicável.

6.10.2.2 Acordos para transferência de informações

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 13.2.2, se aplicam.

6.10.2.3 Mensagens eletrônicas

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 13.2.3, se aplicam.

6.10.2.4 Acordos de confidencialidade e não divulgação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 13.2.4, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 13.2.4, Acordos de confidencialidade e não divulgação, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização assegure que os indivíduos que operam sob seu controle com acesso aos DP estejam sujeitos a um acordo obrigatório de confidencialidade. Convém que o acordo de confidencialidade seja ele parte de um contrato ou, de forma separada, especifique por quanto tempo convém que as obrigações sejam cumpridas.

Quando a organização é um operador de DP, um acordo de confidencialidade independente da forma entre a organização, seus empregados e seus agentes assegura que os empregados e os agentes estejam em *compliance* com as políticas e procedimentos que tratam da proteção e do tratamento dos dados.

6.11 Aquisição, desenvolvimento e manutenção de sistemas

6.11.1 Requisitos de segurança de sistemas de informação

6.11.1.1 Análise e especificação dos requisitos de segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.1.1, se aplicam.

6.11.1.2 Serviços de aplicação seguros em redes públicas

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.1.2, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 14.1.2, Serviços de aplicação seguros em redes públicas, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização assegure que os DP transmitidos por redes de transmissão de dados não confiáveis estejam criptografados para a transmissão.

Redes não confiáveis podem incluir a *internet* pública e outras instalações fora do controle operacional da organização.

NOTA Em alguns casos (por exemplo, na troca de *e-mail*), as características inerentes de um sistema de rede de transmissão de dados não confiáveis podem requerer que alguns dados de tráfego ou cabeçalho sejam expostos para uma transmissão eficaz.

6.11.1.3 Protegendo as transações nos aplicativos de serviços

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.1.3, se aplicam.

6.11.2 Segurança em processos de desenvolvimento e de suporte

6.11.2.1 Política de desenvolvimento seguro

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.2.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 14.2.1, Política de desenvolvimento seguro, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que políticas para o projeto e desenvolvimento de sistemas incluam diretrizes para as necessidades de tratamento de DP da organização, com base nas obrigações dos titulares do DP e/ou qualquer legislação aplicável e/ou regulamentação e os tipos de tratamentos realizados pela organização. As Seções 7 e 8 fornecem considerações de controles para o tratamento de DP, que podem ser úteis no desenvolvimento de políticas para privacidade no projeto de sistemas.

Convém que as políticas que contribuem para a *privacy by design* e *privacy by default* considerem os seguintes aspectos:

a) diretrizes sobre proteção de DP e implementação de princípios de privacidade (ver ISO/IEC 29100) no ciclo de vida de desenvolvimento do *software*;

b) requisitos de proteção e privacidade de DP na etapa de *design* do *software*, o que pode ser baseado no resultado de uma avaliação de riscos de privacidade e/ou na avaliação do impacto da privacidade (ver 7.2.5);

c) pontos de controle para proteção de DP dentro dos marcos (*milestones*) do projeto;

d) conhecimento requerido de privacidade e proteção de DP;

e) por regra, minimização do tratamento de DP.

6.11.2.2 Procedimentos para controle de mudanças de sistemas

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.2.2, se aplicam.

6.11.2.3 Análise crítica técnica das aplicações após mudanças nas plataformas operacionais

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.2.3, se aplicam.

6.11.2.4 Restrições sobre mudanças em pacotes de *software*

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.2.4, se aplicam.

6.11.2.5 Princípios para projetar sistemas seguros

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.2.5, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 14.2.5, Princípios para projetar sistemas seguros, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que os sistemas e/ou componentes relativos ao tratamento de DP sejam projetados seguindo os princípios de *privacy by design* e *privacy by default*, e para antecipar e facilitar a implementação de controles pertinentes (como descrito nas Seções 7 e 8 para, respectivamente, os controladores de DP e operadores de DP), em particular quando a coleta e o tratamento de DP naqueles sistemas estiverem limitados ao que é necessário para os propósitos identificados do tratamento de DP (ver 7.2).

Por exemplo, convém que uma organização que trate DP assegure que, com base na jurisdição relevante, ela descarte o DP após um período especificado. Convém que o sistema que opera aquele DP seja projetado de modo a facilitar este requisito de exclusão.

6.11.2.6 Ambiente seguro para desenvolvimento

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.2.6, se aplicam.

6.11.2.7 Desenvolvimento terceirizado

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.2.7, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 14.2.7, Desenvolvimento terceirizado, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que os mesmos princípios (ver 6.11.2.5) de *privacy by design* e *privacy by default* sejam aplicados, se pertinente, para sistema de informação terceirizado.

6.11.2.8 Teste de segurança do sistema

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.2.8, se aplicam.

6.11.2.9 Teste de aceitação de sistemas

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.2.9, se aplicam.

6.11.3 Dados para teste

6.11.3.1 Proteção dos dados para teste

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 14.3.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 14.3.1, Proteção dos dados para teste, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que o DP não seja usado para propósitos de testes; convém que seja usado um DP falso ou sintético. Onde o uso de DP para propósitos de teste não puder ser evitado, convém que sejam implementadas medidas técnicas e organizacionais equivalentes a aquelas usadas no ambiente de produção, para minimizar os riscos. Onde tais medidas equivalentes não forem possíveis, convém que uma avaliação de riscos seja realizada e utilizada para informar a seleção de controles apropriados de mitigação.

6.12 Relacionamento na cadeia de suprimento

6.12.1 Segurança da informação na cadeia de suprimento

6.12.1.1 Política de segurança da informação no relacionamento com os fornecedores

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 15.1.1, se aplicam.

6.12.1.2 Identificando segurança da informação nos acordos com fornecedores

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 15.1.2, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 15.1.2, Identificando segurança da informação nos acordos com fornecedores, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização especifique nos acordos com fornecedores se o DP é tratado e as medidas mínimas técnicas e organizacionais que o fornecedor precisa atender para que a organização cumpra com as suas as obrigações de proteção de DP e segurança da informação (ver 7.2.6 e 8.2.1).

Convém que acordos com fornecedores estabeleçam claramente as responsabilidades entre a organização, seus parceiros, seus fornecedores e seus terceiros aplicáveis (clientes, fornecedores etc.), levando em conta o tipo de DP tratado.

Convém que os acordos entre a organização e seus fornecedores forneçam um mecanismo para assegurar que a organização apoie e gerencie o *compliance* com todas as legislações e/ou regulamentações aplicáveis. Convém que os acordos busquem uma auditoria de *compliance* independente, que seja aceita pelo cliente.

NOTA Para tais propósitos de auditoria, o *compliance* com normas de privacidade e segurança, aplicáveis e pertinentes, a exemplo da ABNT NBR ISO/IEC 27001 ou este documento, pode ser considerado.

Diretrizes de implementação de operadores de DP

Convém que a organização especifique nos contratos com quaisquer fornecedores que o DP é apenas tratado com base nas suas instruções.

6.12.1.3 Cadeia de suprimento na tecnologia da informação e comunicação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 15.1.3, se aplicam.

6.12.2 Gerenciamento da entrega do serviço do fornecedor

6.12.2.1 Monitoramento e análise crítica de serviços com fornecedores

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 15.2.1, se aplicam.

6.12.2.2 Gerenciamento de mudanças para serviços com fornecedores

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 15.2.2, se aplicam.

6.13 Gestão de incidentes de segurança da informação

6.13.1 Gestão de incidentes de segurança da informação e melhorias

6.13.1.1 Responsabilidades e procedimentos

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 16.1.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 16.1.1, Responsabilidades e procedimentos, da ABNT NBR ISO/IEC 27002:2013, são:

Como parte do processo de gestão de incidentes de segurança da informação global, convém que a organização estabeleça responsabilidades e procedimentos para a identificação e registro de violações de DP. Adicionalmente, convém que a organização estabeleça responsabilidades e procedimentos relativos à notificação para as partes envolvidas nas violações de DP (incluindo o tempo de tais notificações) e à divulgação para as autoridades, levando em conta a regulamentação e/ou legislação aplicadas.

Algumas jurisdições impõem regulamentações específicas quanto às respostas a uma violação, incluindo a notificação. Convém que as organizações que operem nestas jurisdições assegurem que elas podem demonstrar *compliance* com estas regulamentações.

6.13.1.2 Notificação de eventos de segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 16.1.2, se aplicam.

6.13.1.3 Notificando fragilidades de segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 16.1.3, se aplicam.

6.13.1.4 Avaliação e decisão dos eventos de segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 16.1.4, se aplicam.

6.13.1.5 Resposta aos incidentes de segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 16.1.5, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 16.1.5, Resposta aos incidentes de segurança da informação, da ABNT NBR ISO/IEC 27002:2013, são:

Diretrizes para implementação para os controladores de DP

Um incidente que envolva DP pode desencadear uma análise crítica pela organização, como parte do seu processo de gestão de incidentes de segurança da informação, para determinar se uma violação envolvendo DP que requeira uma resposta foi tomada.

Um evento não necessariamente desencadeia tal análise crítica.

NOTA 1 Um evento de segurança da informação não necessariamente resulta de uma probabilidade significante real de acesso não autorizado ao DP ou a qualquer equipamento ou instalações da organização que armazenem DP. Isto pode incluir, mas não está limitado a, *pings* e outros ataques de *broadcast* a *firewalls* ou servidores de borda, varredura de portas e tentativas de acessos malsucedidas, ataque de *denial of service* e inspeção de pacotes (*sniffing* de pacotes).

Quando ocorrer uma violação de DP, convém que procedimentos com respostas incluam notificações relevantes de registros.

Algumas jurisdições estabelecem casos quando convém que a violação seja notificada à autoridade de supervisão e quando convém que ela seja notificada aos titulares de DP.

Convém que notificações sejam claras e que possam ser exigidas.

NOTA 2 Notificação pode conter detalhes como:

— um ponto de contato onde mais informações podem ser obtidas;

— uma descrição da violação e a probabilidade das consequências;

— uma descrição da violação, incluindo o número de indivíduos envolvidos, bem como o número de registros relacionados;

— medidas tomadas ou planejadas para serem tomadas.

NOTA 3 Informação sobre gestão de incidentes de segurança pode ser encontrada na série ISO/IEC 27035.

Onde uma violação envolvendo DP tenha ocorrido, convém que um registro seja mantido com informação suficiente para fornecer um relatório para propósitos forenses e/ou regulatórios, como:

— uma descrição do incidente;

— período de tempo;

— consequências do incidente;

— nome do relator;

— para quem o incidente foi reportado;

— passos tomados para resolver incidentes (incluindo a pessoa em questão e os dados recuperados);

— o fato de que um incidente resultou em indisponibilidade, perda, divulgação ou alteração de DP.

No caso em que uma violação envolvendo DP tenha ocorrido, convém que o registro também inclua uma descrição do DP comprometido, se for conhecido; e se as notificações forem realizadas, os espaços tomados para notificar aos titulares de DP, agências regulatórias ou clientes.

Diretrizes implementação para operadores de DP

Convém que cláusulas que cobrem a notificação de uma violação envolvendo DP formem parte de um contrato entre a organização e um cliente. Convém que o contrato especifique como a organização irá fornecer as informações necessárias para o cliente cumprir com as suas obrigações para notificar as autoridades pertinentes. Esta notificação obrigatória não se estende a uma violação causada pelo cliente ou titular do DP ou dentro de um sistema de componentes para os quais eles são responsáveis. Convém que o contrato também determine limites obrigatórios esperados que são mandatórios para os times de resposta à notificação.

Em algumas jurisdições, convém que o operador de DP notifique ao controlador de DP a existência de uma violação sem o devido atraso (tão logo quanto possível), preferencialmente tão logo ele seja descoberto, de modo que o controlador de DP possa tomar as ações apropriadas.

Quando uma violação envolvendo DP tiver ocorrido, convém que um registro seja mantido com informação suficiente para fornecer um relatório para propósitos forenses e/ou regulatórios, como:

— uma descrição do incidente;

— período de tempo;

— consequências do incidente;

— nome do relator;

— para quem o incidente foi reportado;

— passos tomados para resolver os incidentes (incluindo a pessoa em questão e os dados recuperados);

— o fato de que o incidente resultou em indisponibilidade, perda, divulgação ou alteração de DP.

No evento em que uma violação envolvendo DP tiver ocorrido, convém que o registro também inclua uma descrição do DP comprometido, se for conhecido; e se as notificações forem realizadas, os passos tomados para notificar ao cliente e/ou agências regulatórias.

Em algumas jurisdições, a legislação e/ou a regulamentação aplicáveis podem requerer que a organização notifique diretamente às autoridades regulamentares apropriadas (por exemplo, uma autoridade de proteção de DP) sobre a violação envolvendo o DP.

6.13.1.6 Aprendendo com os incidentes de segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 16.1.6, se aplicam.

6.13.1.7 Coleta de evidências

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 16.1.7, se aplicam.

6.14 Aspectos da segurança da informação na gestão da continuidade do negócio

6.14.1 Continuidade da segurança da informação

6.14.1.1 Planejando a continuidade da segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 17.1.1, se aplicam.

6.14.1.2 Implementando a continuidade da segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 17.1.2, se aplicam.

6.14.1.3 Verificação, análise crítica e avaliação da continuidade da segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 17.1.3, se aplicam.

6.14.2 Redundâncias

6.14.2.1 Disponibilidade dos recursos de processamento da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 17.2.1, se aplicam.

6.15 *Compliance*

6.15.1 *Compliance* com requisitos legais e contratuais

6.15.1.1 Identificação da legislação aplicável e de requisitos contratuais

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 18.1.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 18.1.1, Identificação da legislação aplicável e de requisitos contratuais, da ABNT NBR ISO/IEC 27002:2013, são:

Convém que a organização identifique quaisquer sanções legais potenciais (que podem resultar de algumas obrigações que têm sido omitidas) relativas ao tratamento de DP, incluindo multas substanciais oriundas diretamente da autoridade de supervisão local. Em algumas jurisdições, Normas, como este documento, podem ser usadas para formar a base para um contrato entre a organização e o cliente, estabelecendo as suas respectivas responsabilidades de proteção, segurança e privacidade do DP. Os termos do contrato podem fornecer uma base para sanções contratuais, no caso de uma violação daquelas responsabilidades.

6.15.1.2 Direitos de propriedade intelectual

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 18.1.2, se aplicam.

6.15.1.3 Proteção de registros

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 18.1.3, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 18.1.3, Proteção de registros, da ABNT NBR ISO/IEC 27002:2013, são:

Pode ser requerida a análise crítica de políticas e de procedimentos atuais e históricos (por exemplo, nos casos em que o cliente entre em litígio e em uma investigação por uma autoridade de supervisão).

Convém que a organização retenha cópias de seus procedimentos e políticas de privacidade associados, por um período conforme especificado na sua programação de retenção (ver 7.4.7). Isto inclui a retenção de versões anteriores destes documentos, quando eles são atualizados.

6.15.1.4 Proteção e privacidade de DP

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 18.1.4, se aplicam.

6.15.1.5 Regulamentação de controles de criptografia

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 18.1.5, se aplicam.

6.15.2 Análise crítica da segurança da informação

6.15.2.1 Análise crítica independente da segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 18.2.1, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 18.2.1, Análise crítica independente da segurança da informação, da ABNT NBR ISO/IEC 27002:2013, são:

Quando uma organização estiver atuando como um operador de DP, e onde auditorias individuais de clientes forem impraticáveis ou puderem aumentar os riscos a segurança, convém que a organização disponibilize aos clientes, antes de celebrar e durante a duração de um contrato, evidências independentes de que a segurança de informação está implementada e é operada de acordo com os procedimentos e as políticas da organização. Convém que uma auditoria independente pertinente, como selecionado pela organização, seja normalmente um método aceitável para atendimento aos interesses de um cliente na análise crítica das operações de tratamento da organização, caso isto cubra antecipadamente as necessidades de usuários e se os resultados forem fornecidos de uma maneira suficientemente transparente.

6.15.2.2 *Compliance* com as políticas e normas de segurança da informação

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 18.2.2, se aplicam.

6.15.2.3 Análise crítica técnica do *compliance*

O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 18.2.3, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 18.2.3, Análise crítica da conformidade técnica, da ABNT NBR ISO/IEC 27002:2013, são:

Como parte das análises críticas técnicas do *compliance* com as normas e políticas de segurança, convém que a organização inclua métodos de análise crítica destas ferramentas e componentes relacionados ao tratamento de DP. Isto pode incluir:

— monitoramento contínuo para verificar que somente o tratamento permitido está sendo executado; e/ou

— testes específicos de vulnerabilidade ou invasão (por exemplo conjunto de dados anonimizados pode estar sujeito a um teste de inclusão motivado para validar que os métodos de anonimização estão em conformidade com os requisitos da organização).

7 Diretrizes adicionais da ABNT NBR ISO/IEC 27002 para controladores de DP

7.1 Geral

A diretriz na Seção 6 e os acréscimos nesta Seção criam diretrizes específicas para o SGPI para controladores de DP. As diretrizes de implementação documentadas nesta Seção se relacionam aos controles listados no Anexo A.

7.2 Condições para coleta e tratamento

Objetivo: Determinar e documentar que o tratamento é lícito, com bases legais, conforme as jurisdições aplicáveis, e com propósitos legítimos e claramente estabelecidos.

7.2.1 Identificação e documentação do propósito

Controle

Convém que a organização identifique e documente os propósitos específicos pelos quais os DP serão tratados.

Diretrizes para implementação

Convém que a organização assegure que os titulares de DP entendam o propósito para os quais os seus DP serão tratados. É responsabilidade da organização comunicar isto e documentar claramente para os titulares de DP. Sem uma clara declaração do propósito para tratamento, não é possível que o consentimento e as escolhas sejam dados adequadamente.

Convém que a documentação do propósito do tratamento do DP seja suficientemente clara e detalhada para poder ser utilizada na informação requerida a ser fornecida aos titulares de DP (ver 7.3.2). Isto inclui as informações necessárias para obter o consentimento (ver 7.2.3), bem como os registros das políticas e procedimentos (ver 7.2.8).

Outras informações

No desdobramento dos serviços de computação em nuvem, a taxonomia e as definições da ISO/IEC 19944 podem ser úteis no fornecimento de termos para descrever o propósito do tratamento de DP.

7.2.2 Identificação de bases legais

Controle

Convém que a organização determine, documente e esteja em *compliance* com a base legal pertinente para o tratamento de DP, para os propósitos identificados.

Diretrizes para implementação

Algumas jurisdições requerem que a organização seja capaz de demonstrar que a legalidade do tratamento foi devidamente estabelecida antes do tratamento.

As bases legais para o tratamento de DP podem incluir:

— consentimento dos titulares de DP;

— cumprimento de um contrato;

— *compliance* com obrigações legais;

— proteção dos interesses vitais dos titulares de DP;

— desempenho de uma tarefa realizada de interesse público;

— interesses legítimos do controlador de DP.

Convém que a organização documente esta base para cada atividade de tratamento de DP (ver 7.2.8).

Os interesses legítimos da organização podem incluir, por exemplo, objetivos de segurança da informação, que convém que sejam balanceados com as obrigações com os titulares de DP relacionados à proteção da privacidade.

Independentemente das categorias especiais de DP que são especificadas, sejam pela natureza do DP (por exemplo, informação sobre saúde) ou pelos titulares de DP (por exemplo, DP relativo a crianças), convém que a organização inclua aquelas categorias de DP nos seus esquemas de classificação.

A classificação de DP que se enquadra dentro destas categorias pode variar de uma jurisdição para outra e pode variar entre diferentes regimes regulatórios que se aplicam a diferentes tipos de negócios; assim a organização necessita estar consciente das classificações que se aplicam ao tratamento de DP que está sendo realizado.

O uso de categorias especiais de DP também pode estar sujeito a controles mais restritos.

Mudar ou ampliar os propósitos para o tratamento de DP pode requerer atualização e/ou revisão das bases legais. Isto pode também requerer consentimento adicional a ser obtido do titular de DP.

NOTA BRASILEIRA A LGPD apresenta 10 hipóteses para o uso de dados pessoais, além da prerrogativa para proteção a fraudes e segurança do titular de DP.

7.2.3 Determinando quando e como o consentimento deve ser obtido

Controle

Convém que a organização determine e documente um processo pelo qual possa demonstrar se, quando e como o consentimento para o tratamento de DP foi obtido dos titulares de DP.

Diretrizes para implementação

Pode ser necessário o consentimento para o tratamento de DP, a menos que outros motivos legais se apliquem. Convém que a organização documente claramente a necessidade de obtenção de consentimento e os requisitos para obter o consentimento. Pode ser útil correlacionar os propósitos para tratamento com as informações sobre se e como o consentimento é obtido.

Algumas jurisdições têm requisitos específicos sobre como o consentimento é coletado e registrado (por exemplo, não estar vinculado com outros acordos). Além disso, certos tipos de coleta de dados (para pesquisa científica, por exemplo) e certos tipos de titulares de DP, como crianças, podem estar sujeitos a requisitos adicionais. Convém que a organização leve em consideração estes requisitos e documente como os mecanismos de consentimento atendem a estes requisitos.

7.2.4 Obtendo e registrando o consentimento

Controle

Convém que a organização obtenha e registre o consentimento dos titulares de DP de acordo com os processos documentados.

Diretrizes para implementação

Convém que a organização obtenha e registre os consentimentos dos titulares de DP de forma que ela possa fornecer, sob solicitação, detalhes do consentimento fornecido (por exemplo, o tempo em que o consentimento foi fornecido, a identificação do titular de DP e a declaração de consentimento).

Convém que as informações fornecidas ao titular de DP, antes do processo de consentimento, sigam a diretriz apresentada em 7.3.3.

Convém que o consentimento seja:

— dado livremente;

— específico quanto ao propósito para tratamento; e

— sem ambiguidade e explícito.

7.2.5 Avaliação de impacto de privacidade

Controle

Convém que a organização avalie a necessidade para, e implemente onde apropriado, uma avaliação de impacto de privacidade, quando novos tratamentos de DP ou mudanças ao tratamento existente de DP forem planejados.

Diretrizes para implementação

O tratamento de DP gera riscos para os titulares de DP. Convém que estes riscos sejam avaliados por meio de uma avaliação de impacto de privacidade. Algumas jurisdições estabelecem casos para os quais a avaliação de impacto de privacidade é mandatória. Os critérios podem incluir tomada de decisão automatizada, que produz efeitos legais nos titulares de DP, tratamento em larga escala de categorias especiais de DP (por exemplo, informação relativa à saúde, origem étnica ou racial, opiniões políticas, crenças religiosas ou filosóficas, membros de sindicatos, dados de biometria ou dados de genética) ou monitoramento sistemático de uma área publicamente acessível em larga escala.

Convém que a organização determine os elementos que são necessários para uma avaliação de impacto de privacidade completa. Isto pode incluir uma lista dos tipos de DP tratados, onde o DP é armazenado e onde ele pode ser transferido. Diagramas de fluxos de dados e mapas de dados podem também ser úteis neste contexto (ver 7.2.8 para detalhes de registros de tratamento de DP que possam informar um impacto da privacidade ou uma outra avaliação de risco).

Outras informações

Diretrizes sobre avaliações de impacto da privacidade relativas ao tratamento de DP podem ser encontradas na ISO/IEC 29134.

7.2.6 Contratos com operadores de DP

Controle

Convém que a organização tenha um contrato por escrito com qualquer operador de DP que ela utilize, e convém assegurar que os seus contratos com os operadores de DP contemplem a implementação de controles apropriados, conforme descrito no Anexo B.

Diretrizes para implementação

Convém que o contrato entre a organização e qualquer operador de DP tratando DP em seu nome requeira que o operador de DP implemente os controles apropriados especificados no Anexo B, levando em conta o processo de avalição de riscos de segurança da informação (ver 5.4.1.2) e o escopo do tratamento de DP realizado pelo operador de DP (ver 6.12). Por padrão, convém que todos os controles especificados no Anexo B sejam assumidos como pertinentes. Se a organização decidir não exigir que o operador de DP implemente os controles do Anexo B, convém que ela justifique a sua exclusão (ver 5.4.1.3).

Um contrato pode estabelecer as responsabilidades de cada parte diferentemente, porém, para ser consistente com este documento, convém que todos os controles sejam considerados e incluídos na informação documentada.

7.2.7 Controlador conjunto de DP

Controle

Convém que a organização determine as responsabilidades e respectivos papéis para o tratamento de DP (incluindo a proteção do DP e os requisitos de segurança) com qualquer controlador conjunto de DP.

Diretrizes para implementação

Convém que os papéis e responsabilidades para o tratamento de DP sejam determinados de forma transparente.

Convém que estas responsabilidades e papéis sejam documentados em um contrato ou em qualquer documento de concorrência similar que contenha os termos e condições para o tratamento combinado de DP. Em algumas jurisdições, tal acordo é chamado de acordo de compartilhamento de dados.

Um acordo com um controlador conjunto de DP pode incluir (esta lista não é definitiva nem exaustiva):

— propósito do compartilhamento de DP/relacionamento do controlador conjunto de DP;

— identidade das organizações (controladores de DP) que são parte do relacionamento do controlador conjunto de DP;

— categorias de DP a serem compartilhadas e/ou transferidas e tratadas com base no acordo;

— visão global das operações de tratamento (por exemplo, transferência, uso);

— descrição dos respectivos papéis e responsabilidades;

— responsabilidade pela implementação técnica e organizacional das medidas de segurança para proteção de DP;

— definição de responsabilidade no caso de uma violação de DP (por exemplo, quem irá notificar, quando e informações mútuas);

— termos de retenção e/ou descarte de DP;

— responsabilidades cíveis por falha na conformidade com acordo;

— como as obrigações dos titulares de DP são atendidas;

— como fornecer aos titulares de DP informações que cubram a essência dos acordos entre os controladores conjuntos de DP;

— como os titulares de DP podem obter outras informações que eles têm direito a receber;

— um ponto de contato para os titulares de DP.

7.2.8 Registros relativos ao tratamento de DP

Controle

Convém que a organização determine e mantenha de maneira segura os registros necessários ao suporte às suas obrigações para o tratamento de DP.

Diretrizes para implementação

Uma maneira de manter os registros de tratamento do DP é ter um inventário ou uma lista das atividades de tratamento do DP que a organização realiza. Esta lista de inventário pode incluir:

— tipo de tratamento;

— propósitos para o tratamento;

— uma descrição das categorias de DP e dos titulares de DP (por exemplo, crianças);

— as categorias de destinatário para quem o DP tem sido ou será divulgado, incluindo os destinatários em outros países ou organizações internacionais;

— uma descrição geral das medidas de segurança técnica e organizacional; e

— um relatório de Avaliação de Impacto de Privacidade.

Convém que este inventário tenha um proprietário que seja responsável por sua completeza e precisão.

7.3 Obrigações dos titulares de DP

Objetivo: Para assegurar que os titulares de DP sejam providos com informações apropriadas sobre o tratamento de seus DP e para atender quaisquer outras obrigações aplicáveis aos titulares de DP, relativas aos tratamentos de seus DP.

7.3.1 Determinando e cumprindo as obrigações para os titulares de DP

Controle

Convém que a organização determine e documente suas obrigações regulatórias, legais e de negócios para os titulares de DP, relativas ao tratamento de seus DP, e forneça os meios para atender a estas obrigações.

Diretrizes para implementação

As obrigações para os titulares de DP e os meios de apoiá-los varia de uma jurisdição para outra.

Convém que a organização assegure que eles forneçam os meios apropriados para atender às obrigações para os titulares de DP de uma forma acessível e em tempo hábil. Convém que uma documentação clara seja fornecida ao titular de DP, descrevendo a abrangência na qual as obrigações para eles são atendidas e como, por meio de um ponto de contato atualizado, eles podem contemplar as suas solicitações.

Convém que o ponto de contato seja fornecido de uma forma similar àquela usada para coletar o DP e obter o consentimento (por exemplo, se os DP são coletados por *e-mail* ou por um *website*, convém que o ponto de contato seja por *e-masil* ou por *website*, e não uma alternativa a exemplo do telefone ou do *fax*).

7.3.2 Determinando as informações para os titulares de DP

Controle

Convém que a organização determine e documente a informação a ser fornecida aos titulares de DP, relativa ao tratamento de seus DP, e o tempo de tal disponibilização.

Diretrizes para implementação

Convém que a organização determine os requisitos legais, regulamentares e/ou de negócio para quando a informação for fornecida para o titular de DP (por exemplo, antes do tratamento, dentro de um certo tempo, a partir da solicitação) e para o tipo de informação a ser fornecida.

Dependendo dos requisitos, a informação pode tomar o formato de uma notícia. Exemplos de tipos de informação que podem ser fornecidas aos titulares de DP são:

— informação sobre o propósito do tratamento;

— detalhes do contato para o controlador de DP ou seu representante;

— informação sobre as bases legais do tratamento;

— informação sobre onde o DP foi obtido, caso não seja obtido diretamente do titular de DP;

— informação sobre se o fornecimento de DP é um requisito contratual ou estatutário, e onde apropriado, as possíveis consequências de falha para fornecer o DP;

— informações sobre obrigações para os titulares de DP, como definido em 7.3.1, e como os titulares de DP podem se beneficiar deles, especialmente em relação ao acesso, acréscimo, correção, solicitação para apagar, recebimento de uma cópia dos seus DP e a desaprovaçãopara o tratamento;

— informação sobre como o titular de DP pode cancelar um consentimento;

— informação sobre transferência de DP;

— informação sobre destinatário e categoria de destinatário de DP;

— informação sobre o período para o qual o DP será retido;

— informação sobre o uso de tomada de decisão automatizada, com base no tratamento automatizado de DP;

— informação sobre o direito de apresentar uma reclamação e como apresentá-la;

— informação relativa à frequência na qual uma informação é fornecida (por exemplo, notificação "*just in time*", frequência definida pela organização etc.).

Convém que a organização forneça informações atualizadas quando os propósitos para o tratamento de DP forem mudados ou estendidos.

7.3.3 Fornecendo informações aos titulares de DP

Controle

Convém que a organização forneça aos titulares de DP, de forma clara e facilmente acessível, informações que identifiquem o controlador de DP e descrevam o tratamento de seus DP.

Diretrizes para implementação

Convém que a organização forneça as informações detalhadas em 7.3.2 para os titulares de DP em tempo hábil e de forma concisa, completa, transparente, inteligível e facilmente acessível, usando uma linguagem curta e clara, como apropriado ao público-alvo.

Onde apropriado, convém que a informação seja dada no momento da coleta do DP, e convém que ela seja também acessível permanentemente.

NOTA Ícones e imagens podem ser úteis ao titular de DP, porque fornece uma condição visual do tratamento pretendido.

7.3.4 Fornecendo mecanismos para modificar ou cancelar o consentimento

Controle

Convém que a organização forneça mecanismos para os titulares de DP para modificar ou cancelar os seus consentimentos.

Diretrizes para implementação

Convém que a organização informe aos titulares de DP sobre os seus direitos relativos ao cancelamento do consentimento (que podem variar por jurisdição) a qualquer tempo, e forneça o mecanismo para fazer isto. O mecanismo usado para cancelamento depende do sistema; convém que ele seja consistente com os mecanismos usados para a obtenção do consentimento, quando possível. Por exemplo, se o consentimento é coletado por *e-mail* ou por *website*, convém que o mecanismo para cancelamento seja o mesmo, e não uma solução alternativa, como telefone ou *fax*.

Modificar o consentimento pode incluir a colocação de restrições sobre o tratamento de DP, o que pode incluir restrição ao controlador de DP para excluir o DP em alguns casos.

Algumas jurisdições impõem restrições sobre quando e como um titular de DP pode modificar ou cancelar o seu consentimento.

Convém que a organização registre qualquer solicitação para cancelar ou mudar o consentimento de uma forma similar ao registro do consentimento propriamente dito.

Convém que qualquer mudança do consentimento seja disseminada por meio de sistemas apropriados, para os usuários autorizados e também para terceiros relevantes.

Convém que a organização defina um tempo de resposta e convém que a solicitação seja tratada de acordo com isto.

Informação adicional

Quando um consentimento para tratamento particular de DP é cancelado, convém que todos os tratamentos de DP realizados antes do cancelamento sejam considerados normalmente, como apropriado, porém convém que os resultados destes tratamentos não sejam usados para novos tratamentos. Por exemplo, se um titular de DP retirar seu consentimento para a criação do perfil, convém que seu perfil não seja usado ou consultado no futuro.

7.3.5 Fornecendo mecanismos para negar o consentimento ao tratamento de DP

Controle

Convém que a organização forneça mecanismos para os titulares de DP para negar o consentimento ao tratamento do seu DP.

Diretrizes para implementação

Algumas jurisdições concedem aos titulares de DP o direito de negar o consentimento ao tratamento de seus DP. Convém que as organizações sujeitas a uma regulamentação e/ou legislação destas jurisdições assegurem que elas implementem medidas apropriadas para permitir que os titulares de DP exercitem este direito.

Convém que a organização documente os requisitos legais e regulamentares relativos às objeções feitas pelos titulares de DP para o tratamento (por exemplo, objeção relativa ao tratamento de DP para propósitos de *marketing* direto). Convém que a organização forneça informações aos titulares quanto à capacidade de negar o consentimento nestas situações. Mecanismos para desaprovação podem variar, porém convém que sejam consistentes com o tipo de serviço fornecido (por exemplo, convém que os serviços *on-line* forneçam esta condição *on-line*).

7.3.6 Acesso, correção e/ou exclusão

Controle

Convém que a organização implemente políticas, procedimentos e/ou mecanismos para atender às suas obrigações para os titulares de DP acessarem, corrigirem e/ou excluirem os seus DP.

Diretrizes para implementação

Convém que a organização implemente políticas, procedimentos e/ou mecanismos para permitir aos titulares de DP obter acesso para corrigir e excluir os seus DP, quando solicitado e sem atraso indevido.

Convém que a organização defina um tempo de resposta e convém que a solicitação seja tratada de acordo com isto.

Convém que quaisquer correções ou exclusões sejam disseminadas por todo o sistema e/ou para os usuários autorizados, e convém que sejam passadas para terceiros (ver 7.3.7), para os quais o DP foi transferido.

NOTA Registros gerados pelo controle especificado em 7.5.3 podem ajudar nesta questão.

Convém que a organização implemente políticas, procedimentos e/ou mecanismos para uso quando puder existir uma disputa sobre a precisão ou correção do dado pelo titular de DP. Convém que estas políticas, procedimentos e/ou mecanismos incluam informação do titular de DP sobre quais mudanças foram feitas, e as razões por que as correções não foram realizadas (quando este for o caso).

Algumas jurisdições impõem restrições sobre quando e como um titular de DP pode requerer uma correção ou exclusão do seu DP. Convém que a organização determine estas restrições, conforme aplicável, e mantenha-se atualizada sobre eles.

7.3.7 Obrigações dos controladores de DP para informar aos terceiros

Controle

Convém que a organização informe aos terceiros com quem o DP foi compartilhado sobre qualquer modificação, cancelamento ou desaprovação pertinente ao DP compartilhado, e implemente políticas e procedimentos apropriados e/ou mecanismos para fazê-lo.

Diretrizes para implementação

Convém que a organização tome passos apropriados, tendo em mente a tecnologia disponível, para informar aos terceiros sobre qualquer modificação ou cancelamento do consentimento, ou objeções pertinentes ao compartilhamento de DP. Algumas jurisdições impõem requisitos por força de lei para informar a estes terceiros sobre estas ações.

Convém que a organização determine e mantenha um canal de comunicação ativo com os terceiros. Responsabilidades relacionadas podem ser atribuídas aos indivíduos encarregados das suas operações e manutenção. Ao informar terceiros, convém que a organização monitore o seu conhecimento de recebimento da informação.

NOTA Mudanças resultantes de obrigações para os titulares de DP podem incluir modificação ou cancelamento do consentimento, solicitações para correção, exclusão, ou restrições sobre o tratamento, ou ainda objeções para o tratamento de DP como solicitado pelo titular de DP.

7.3.8 Fornecendo cópia do DP tratado

Controle

Convém que a organização seja capaz de fornecer uma cópia do DP que é tratado, quando requerido pelo titular de DP.

Diretrizes para implementação

Convém que a organização forneça uma cópia do DP que é tratado em um formato estruturado e usado normalmente, acessível pelo titular de DP.

Algumas jurisdições definem casos onde convém que a organização forneça uma cópia do DP tratado em um formato que permita a portabilidade para os titulares de DP ou para o destinatário dos controladores de DP (estruturado tipicamente, usado normalmente e que seja lido em uma máquina).

Convém que a organização assegure que quaisquer cópias de DP fornecidas para um titular de DP estejam especificamente relacionadas com aquele titular de DP.

Onde o DP solicitado já tiver sido excluído, sujeito à política de retenção e descarte (como descrito em 7.4.7), convém que o controlador de DP informe ao titular de DP que o DP requerido foi excluído.

Nos casos onde a organização não é mais capaz de identificar o titular de DP (por exemplo, como o resultado do processo de anonimização), convém que a organização não procure reidentificar os titulares de DP pela simples razão da implementação deste controle. Entretanto, em algumas jurisdições, solicitações legítimas podem requerer que informações adicionais sejam solicitadas do titular de DP para permitir a reidentificação e consequente divulgação.

Quando for tecnicamente viável, convém que seja possível transferir uma cópia do DP de uma organização diretamente para outra organização, por solicitação do titular de DP.

7.3.9 Tratamento de solicitações

Controle

Convém que a organização defina e documente políticas e procedimentos para tratamento e respostas a solicitações legítimas dos titulares de DP.

Diretrizes para implementação

Solicitações legítimas podem incluir pedidos para uma cópia do DP tratado, ou solicitação para apresentar uma queixa.

Algumas jurisdições permitem que a organização cobre uma taxa em certos casos (por exemplo, solicitações excessivas ou repetitivas).

Convém que as solicitações sejam tratadas dentro dos tempos de respostas apropriados, que estão definidos.

Algumas jurisdições definem os tempos de respostas de acordo com a complexidade e o número de solicitações, como também dos requisitos para informar aos titulares de DP sobre qualquer atraso. Convém que os tempos de respostas apropriados estejam definidos na política de privacidade.

7.3.10 Tomada de decisão automatizada

Controle

Convém que a organização identifique e considere as obrigações, incluindo obrigações legais, para os titulares de DP, como resultado das decisões tomadas pela organização, que estejam relacionadas com o titular de DP, baseadas unicamente no tratamento automatizado de DP.

Diretrizes para implementação

Algumas jurisdições definem obrigações especificas para os titulares de DP, quando uma decisão com base unicamente no tratamento automatizado de DP os afeta significativamente, como a notificação da existência da tomada de decisão automatizada, permitindo aos titulares de DP desaprovar estas decisões tomadas, e/ou solicitar a intervenção humana.

NOTA Em algumas jurisdições, alguns tratamentos de DP podem não ser completamente automatizados.

Convém que as organizações que operam nestas jurisdições considerem o *compliance* com estas obrigações.

7.4 *Privacy by Design* e *Privacy by Default*

Objetivo: Assegurar que os processos e sistemas sejam projetados de tal forma que a coleta e o tratamento (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado.

7.4.1 Limite de coleta

Controle

Convém que a organização limite a coleta de DP a um mínimo que seja relevante, proporcional e necessário para os propósitos identificados.

Diretrizes para implementação

Convém que a organização limite a coleta de DP para o que é adequado, relevante e necessário em na relação para os propósitos identificados. Isto inclui limitar a quantidade de DP que a organização coleta indiretamente (por exemplo, por meio de *logs* da *web*, *logs* de sistemas etc.).

Convém que, ao utilizar o princípio de *Privacy by Default*, onde existir qualquer opção na coleta e tratamento de DP, cada opção seja desabilitada por padrão e somente habilitada por uma escolha explicita do titular de DP.

7.4.2 Limite de tratamento

Controle

Convém que a organização limite o tratamento de DP de tal forma que seja adequado, relevante e necessário para os propósitos identificados.

Diretrizes para implementação

Convém que o limite para o tratamento de DP seja gerenciado por meio de políticas de privacidade de segurança da informação (ver 6.2), juntamente com procedimentos documentados para as suas adoções e *compliance*.

O tratamento de DP inclui:

— a divulgação;

— o período de armazenagem do DP; e

— quem é capaz de acessar seus DP.

E convém que seja limitado por padrão no mínimo necessário para os propósitos identificados.

7.4.3 Precisão e qualidade

Controle

Convém que a organização assegure e documente que o DP é preciso, completo e atualizado, como é necessário para os propósitos aos quais ele é tratado, por meio do ciclo de vida do DP.

Diretrizes para implementação

Convém que a organização implemente políticas, procedimentos e/ou mecanismos para minimizar a imprecisão dos DP que ela trata.

Convém que existam também políticas, procedimentos e/ou mecanismos para responder às questões de imprecisão do DP. Convém que estas políticas, procedimentos e/ou mecanismos sejam incluídos na informação documentada (por exemplo, por meio de configurações de sistemas técnicos etc.) e sejam aplicados ao longo do ciclo de vida do DP.

Informação adicional

Para informações adicionais sobre o tratamento do ciclo de vida do DP, ver ISO/IEC 29101:2018, 6.2.

7.4.4 Objetivos de minimização de DP

Controle

Convém que a organização defina e documente os objetivos da minimização dos dados e quais mecanismos (como a anonimização) são usados para atender àqueles objetivos.

Diretrizes para implementação

Convém que as organizações identifiquem como os DP especificos e a quantidade de DP coletados e tratados estão limitados aos propósitos identificados. Isto pode incluir o uso de anonimização ou outras técnicas de minimização de dados.

O propósito identificado (ver 7.2.1) pode requerer o tratamento do DP que não foi anonimizado, e nestes casos convém que a organização seja capaz de descrever estes tratamentos.

Em outros casos, o propósito identificado não requer o tratamento do DP original, e o tratamento de DP que foi anonimizado pode ser suficiente para alcançar o propósito identificado. Nestes casos, convém que a organização defina e documente a abrangência na qual o DP precisa estar associado com o titular de DP, bem como os mecanismos e técnicas concebidas para tratar o DP, de modo que a anonimização e/ou os objetivos de minimização do DP sejam alcançados.

Mecanismos usados para minimizar o DP variam de acordo com o tipo de tratamento e dos sistemas usados para o tratamento. Convém que a organização documente quaisquer mecanismos (configuração de sistemas técnicos etc.) usados para implementar a minimização dos dados.

Nos casos em que o tratamento de dados anonimizados for suficiente para os propósitos, convém que a organização documente quaisquer mecanismos (configurações de sistema técnico) projetados para implementar os objetivos da anonimização definidos pela organização em um tempo hábil. Por exemplo, a remoção de atributos associados com os titulares de DP pode ser suficiente para permitir que a organização alcance os seus propósitos identificados. Em outros casos, outras técnicas de anomização, como generalização ou técnicas de randomização (por exemplo, adição sonora), podem ser usadas para alcançar um nível adequado de anonimização.

NOTA 1 Para informações adicionais sobre técnicas de anonimização, ver ISO/IEC 20889.

NOTA 2 Para computação em nuvem, a ISO/IEC 19944 fornece uma definição de qualificadores de identificação de dados que pode ser usada para classificar o grau no qual o dado pode identificar um titular de DP ou associado a um titular de DP, com um conjunto de características do DP.

7.4.5 Anonimização e exclusão de DP ao final do tratamento

Controle

Convém que a organização ou exclua o DP ou entregue-o na forma que não permita a identificação ou reidentificação dos titulares de DP, uma vez que o DP original não é mais necessário para os propósitos identificados.

Diretrizes para implementação

Convém que a organização tenha mecanismos para excluir o DP quando nenhum tratamento adicional for antecipado. Alternativamente, algumas técnicas de anonimização podem ser usadas uma vez que os resultados dos dados anonimizados não podem permitir, de forma razoável, a reidentificação dos titulares de DP.

7.4.6 Arquivos temporários

Controle

Convém que a organização assegure que os arquivos temporários criados como um resultado de tratamento de DP sejam descartados (por exemplo, apagado ou destruído) seguindo procedimentos documentados dentro de um período documentado, especificado.

Diretrizes para implementação

Convém que a organização realize verificações periódicas de modo que arquivos temporários não usados sejam excluídos dentro de um período de tempo identificado.

Outras informações

Sistemas de informação podem criar arquivos temporários no curso normal de suas operações. Estes arquivos são específicos para um sistema ou para aplicação, porém podem incluir sistemas de arquivos de reversão (*rollback journals*) e arquivos temporários associados à atualização das bases de dados e à operação de outras aplicações de *software*. Arquivos temporários não são necessários após a tarefa de tratamento da informação relacionada ter sido completada, porém existem circunstâncias nas quais não é possível que eles sejam excluídos. A extensão do tempo para o qual estes arquivos permanecem em uso não é sempre determinada, porém convém que um procedimento

de liberação de espaço ocioso (*garbage collection*) identifique os arquivos relevantes e determine por quanto tempo ele existe desde a última vez que foi usado.

7.4.7 Retenção

Controle

Convém que a organização não retenha DP por um tempo maior do que é necessário para os propósitos para os quais o DP é tratado.

Diretrizes para implementação

Convém que a organização desenvolva e mantenha esquemas de retenção para as informações que ela guarda, considerando o requisito para retenção do DP por um tempo não maior do que é necessário. Convém que estes esquemas considerem requisitos legais, regulamentares e de negócio. Onde ocorrem conflitos com estes requisitos, uma decisão de negócio precisa ser tomada (com base em uma avaliação de riscos) e documentada no esquema apropriado.

7.4.8 Descarte

Controle

Convém que a organização tenha políticas, procedimentos e/ou mecanismos documentados para o descarte de DP.

Diretrizes para implementação

A escolha das técnicas de descarte do DP depende de um número de fatores, uma vez que uma técnica de descarte difere nas suas propriedades e resultado (por exemplo, na granularidade da mídia física resultante, ou a capacidade para recuperar uma informação excluída de uma mídia eletrônica). Fatores a considerar ao escolher uma técnica de descarte apropriada incluem, porém não estão limitados a, a natureza e a abrangência do DP a ser descartado, se existe ou não um metadado associado ao DP, e as caracteristícas físicas da mídia na qual o DP é armazenado.

7.4.9 Controle de transmissão de DP

Controle

Convém que a organização trate o DP transmitido (por exemplo, enviado para outra organização), que trafegue por uma rede de transmissão de dados, com controles apropriados concebidos para assegurar que os dados alcancem seus destinos pretendidos.

Diretrizes para implementação

A transmissão de dados necessita ser controlada, basicamente para assegurar que somente pessoas autorizadas tenham acesso aos sistemas de transmissão, seguindo os processos apropriados (incluindo a retenção de *logs* de auditoria), para assegurar que o DP seja transmitido sem comprometimento para os destinatários corretos.

7.5 Compartilhamento, transferência e divulgação de DP

Objetivo: Determinar se e documentar quando o DP é compartilhado, transferido para outras jurisdições ou terceiros e/ou divulgado de acordo com as obrigações aplicáveis.

7.5.1 Identificando as bases para a transferência de DP entre jurisdições

Controle

Convém que a organização identifique e documente as bases relevantes para a transferência de DP entre jurisdições.

Diretrizes para implementação

Uma transferência de DP pode estar sujeita a uma legislação e/ou regulamentação dependendo da jurisdição ou da organização internacional para a qual os dados estão para serem transferidos (e de onde eles se originam). Convém que a organização documente o *compliance* com estes requisitos como a base para a transferência.

Algumas jurisdições podem requerer que acordos de transferência da informação sejam analisados criticamente por uma autoridade de supervisão designada. Convém que, as organizações que operam nestas jurisdições estejam cientes destes requisitos.

NOTA Onde a transferência ocorrer dentro de uma jurisdição especifica, a regulamentação e/ou legislação aplicadas são as mesmas para o remetente e para o destinatário.

7.5.2 Países e organizações internacionais para os quais os DP podem ser transferidos

Controle

Convém que a organização especifique e documente os países e as organizações internacionais para os quais os DP possam possivelmente ser transferidos.

Diretrizes para implementação

Convém que as identidades dos países e das organizações internacionais, para os quais os DP possam possivelmente ser transferidos em uma operação normal, estejam disponíveis para os clientes. Convém que as identidades dos países que surjam do uso de subcontratados do tratamento de DP sejam incluídas. Convém que os países incluídos sejam considerados na relação conforme 7.5.1.

Fora das operações normais, podem ocorrer casos de transferência feita por solicitação de uma autoridade por força de lei, em que a identidade dos países pode não ser especificada antecipadamente, ou que se for proibido pela jurisdição aplicável para preservar a confidencialidade de uma investigação por força de lei (ver 7.5.1, 8.5.4 e 8.5.5).

7.5.3 Registros de transferência de DP

Controle

Convém que a organização registre a transferência de DP para ou de terceiros e assegure a cooperação com estas partes para apoiar futuras solicitações relativas às obrigações para os titulares de DP.

Diretrizes para implementação

Registros podem incluir transferências de terceiros de DP que tenham sido modificados como um resultado das suas obrigações no gerenciamento dos controladores, ou na transferência para terceiros para implementar solicitações legítimas dos titulares de DP, incluindo solicitações para exclusão do DP (por exemplo, após o consentimento do cancelamento).

Convém que a organização tenha uma política definindo o período de retenção destes registros.

Convém que a organização aplique o princípio de minimização dos dados para os registros de transferência, retendo apenas as informações estritamente necessárias.

7.5.4 Registro de divulgação de DP para terceiros

Controle

Convém que a organização registre a divulgação de DP para terceiros, incluindo qual DP foi divulgado, para quem e quando.

Diretrizes para implementação

O DP pode ser divulgado durante o curso das operações normais. Convém que estas divulgações sejam registradas. Convém que quaisquer divulgações adicionais para terceiros, como aquelas que surgem de investigações legais ou de auditorias externas, sejam registradas. Convém que os registros incluam as fontes da divulgação e a fonte da autoridade que fez a divulgação.

8 Diretrizes adicionais da ABNT NBR ISO/IEC 27002 para os operadores de DP

8.1 Geral

As diretrizes na Seção 6 e os acréscimos desta Seção criam diretrizes específicas do SGPI para os operadores de DP. As diretrizes de implementação documentadas nesta Seção estão relacionadas aos controles listados no Anexo B.

8.2 Condições para coleta e tratamento

Objetivo: Documentar e determinar que o tratamento é lícito, com base legal, conforme as jurisdições aplicáveis e com propósitos legítimos e claramente definidos.

8.2.1 Acordos com o cliente

Controle

Convém que a organização assegure, onde pertinente que o contrato para tratar o DP considera os papéis da organização em fornecer assistência com as obrigações do cliente (considerando a natureza do tratamento e a informação disponível para a organização).

Diretrizes para implementação

Convém que o contrato entre a organização e o cliente inclua os seguintes itens, onde pertinente, e dependendo do papel do cliente (controlador de DP ou operador de DP) (esta lista não é definitiva nem exaustiva):

— *privacy by design* e *privacy by default* (ver 7.4, 8.4);

— obtenção da segurança do tratamento;

— notificação de violações envolvendo DP para uma autoridade de supervisão;

— notificação de violações envolvendo DP para os clientes e titulares de DP;

— realização de avaliações de impacto da privacidade (AIP);

— garantia de assistência pelo operador de DP no caso em que consultas prévias com autoridades de proteção de DP relevantes sejam necessárias.

Algumas jurisdições requerem que o contrato inclua o assunto e a duração do tratamento, a natureza e o propósito do tratamento, o tipo de DP e as categorias de titulares de DP.

8.2.2 Propósitos da organização

Controle

Convém que a organização assegure que os DP tratados em nome do cliente sejam apenas tratados para o propósito expresso nas instruções documentadas do cliente.

Diretrizes para implementação

Convém que o contrato entre a organização e o cliente inclua, mas não esteja limitado a, o objetivo e o tempo de duração do serviço.

Para alcançar o propósito do cliente, podem existir razões técnicas pelas quais seja apropriado para a organização determinar o método para tratamento do DP, consistente com as instruções gerais do cliente, porém, sem as instruções expressas do cliente. Por exemplo, para utilizar efetivamente a capacidade de rede ou de tratamento, pode ser necessário alocar recursos de tratamento específicos, a depender de certas características do titular de DP.

Convém que a organização permita ao cliente verificar o *compliance* com o propósito dos princípios da limitação e especificação. Isto também assegura que nenhum DP é tratado pela organização ou por qualquer um de seus subcontratados, para outros propósitos que não sejam aqueles expressos nas instruções documentadas do cliente.

8.2.3 Uso de *marketing* e propaganda

Controle

Convém que a organização não utilize os DP tratados sob um contrato para o propósito de *marketing* e propaganda, sem o estabelecimento de que um consentimento antecipado foi obtido do titular de DP apropriado. Convém que a organização não forneça este consentimento como uma condição para o recebimento do serviço.

Diretrizes para implementação

Convém que o *compliance* dos operadores de DP com os requisitos contratuais do cliente, sejam documentados, especialmente onde a atividade de *marketing* e/ou propaganda esteja planejada.

Convém que as organizações não insistam na inclusão do uso de *marketing* e/ou da propaganda onde o consentimento expresso não tenha sido obtido com a certeza do titular de DP.

NOTA Este controle é complementar a um controle mais genérico descrito em 8.2.2 e não substitui nem se sobrepõe a ele.

8.2.4 Violando instruções

Controle

Convém que a organização informe ao cliente se, na sua opinião, uma instrução de tratamento viola uma regulamentação e/ou legislação aplicável.

Diretrizes para implementação

A capacidade da organização para verificar se uma instrução viola a legislação e/ou regulamentação depende do contexto tecnológico, da instrução em si, e do contrato entre a organização e o cliente.

8.2.5 Obrigações do cliente

Controle

Convém que a organização forneça ao cliente informações apropriadas de tal modo que o cliente possa demonstrar *compliance* com suas obrigações.

Diretrizes para implementação

As informações necessárias ao cliente podem incluir se a organização permite e contribui para a realização de auditorias por parte do cliente ou outro auditor obrigatório, ou de outra maneira acordada pelo cliente.

8.2.6 Registros relativos ao tratamento de DP

Controle

Convém que a organização determine e mantenha os registros necessários para apoiar a demonstração do *compliance* com suas obrigações (como especificado no contrato aplicável) para tratamento de DP realizado em nome do cliente.

Diretrizes para implementação

Algumas jurisdições podem requerer que a organização registre informações como:

— categorias de tratamento realizadas em nome de cada cliente;

— transferências para outros países ou organizações internacionais; e

— uma descrição geral das medidas de segurança técnicas e organizacionais.

8.3 Obrigações para os titulares de DP

Objetivo: Assegurar que os titulares de DP sejam providos com informações apropriadas sobre o tratamento de seus DP, e que estejam de acordo com quaisquer outras obrigações aplicáveis para os titulares de DP relativas ao tratamento de seus DP.

8.3.1 Obrigações para os titulares de DP

Controle

Convém que a organização forneça ao cliente meios para estar em *compliance* com suas obrigações relativas aos titulares de DP.

Diretrizes para implementação

As obrigações do controlador de DP podem ser definidas pela legislação, pela regulamentação e/ou pelo contrato. Estas obrigações podem incluir assuntos onde o cliente utiliza os serviços da organiza-

ção para a implementação destas obrigações. Por exemplo, isto pode incluir a correção ou exclusão dos DP em um tempo hábil.

Onde um cliente depende da organização para medidas técnicas ou informações de modo a facilitar o atendimento com as obrigações dos titulares de DP, convém que as medidas técnicas ou informações relevantes sejam especificadas em um contrato.

8.4 *Privacy by design* e *privacy by default*

Objetivo: Assegurar que processos e sistemas sejam projetados de forma que a coleta e o tratamento de DP (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado.

8.4.1 Arquivos temporários

Controle

Convém que a organização assegure que os arquivos temporários criados como um resultado do tratamento de DP sejam descartados (por exemplo, apagados ou destruídos) seguindo os procedimentos documentados, dentro de um período especificado e documentado.

Diretrizes para implementação

Convém que a organização conduza verificações periódicas, de modo que arquivos temporários não usados sejam removidos dentro do período de tempo identificado.

Outras informações

Sistemas de informação podem criar arquivos temporários durante o curso normal de suas operações. Estes arquivos são específicos para o sistema ou para a aplicação, mas podem incluir arquivos de sistemas de arquivos de reversão (*roll-back journals)* e arquivos temporários associados à atualização das bases de dados e à operação de outros *softwares* de aplicação. Arquivos temporários não são necessários depois que a tarefa de tratamento da informação relacionada tenha sido completada, porém, existem circunstâncias nas quais eles não podem ser removidos. A extensão do tempo pelo qual estes arquivos permanecem em uso nem sempre é determinístico, porém, convém que um procedimento de reciclagem (*garbage collection)* identifique os arquivos relevantes e determine quanto tempo passou desde a última vez que foi usado.

8.4.2 Retorno, transferência ou descarte de DP

Controle

Convém que a organização forneça a capacidade de retornar, transferir e/ou descartar DP de uma maneira segura. Convém também que sua política esteja disponível para o cliente.

Diretrizes para implementação

Em algum momento, DP podem precisar ser descartados de alguma maneira. Isto pode envolver o retorno dos DP para o cliente, a transferência deles para outra organização ou para um controlador de DP (por exemplo, como um resultado de uma fusão), exclusão ou outra forma de destruição deles, desanonimização ou o seu arquivamento. Convém que a capacidade para o retorno, transferência e/ou descarte dos DP sejam gerenciados de forma segura.

Convém que a organização forneça a garantia necessária para permitir ao cliente assegurar que DP tratados sob um contrato sejam apagados (pela organização e quaisquer de seus subcontratados) do ponto onde eles estão armazenados, incluindo para os propósitos de cópias de segurança e continuidade dos negócios, tão logo eles não sejam mais necessários, para os propósitos identificados do cliente.

Convém que a organização desenvolva e implemente uma política quanto ao descarte de DP e convém tornar esta política disponível para o cliente quando solicitado.

Convém que a política cubra o período de retenção para DP antes do seu descarte, e depois do encerramento de um contrato, para proteger um cliente da perda de DP por meio de um lapso acidental de um contrato.

NOTA Este controle e diretriz é também relevante sob o princípio de retenção (ver 7.4.7).

8.4.3 Controles de transmissão de DP

Controle

Convém que a organização sujeite DP transmitidos sobre uma rede de transmissão de dados a controles apropriados projetados para assegurar que os dados alcancem seus destinos pretendidos.

Diretrizes para implementação

A transmissão de DP precisa ser controlada, tipicamente para assegurar que somente pessoas autorizadas tenham acesso a sistemas de transmissão e sigam os processos apropriados (incluindo a retenção de dados de auditoria) para assegurar que DP sejam transmitidos sem comprometimento para os destinatários corretos. Requisitos para controles de transmissão podem ser incluídos no operador de DP – contrato com o cliente.

Onde não existem implementados requisitos contratuais relativos à transmissão, pode ser apropriado obter aconselhamento do cliente, antes da transmissão.

8.5 Compartilhamento, transferência e divulgação de DP

Objetivo: Determinar se e documentar quando DP são compartilhados, transferidos para outras jurisdições ou terceiros e/ou divulgados, de acordo com as obrigações aplicáveis.

8.5.1 Bases para a transferência de DP entre jurisdições

Controle

Convém que a organização informe ao cliente em um tempo hábil sobre as bases para a transferência de DP entre jurisdições e de qualquer mudança pretendida nesta questão, de modo que o cliente tenha a capacidade de contestar estas mudanças ou rescindir o contrato.

Diretrizes para implementação

A transferência de DP entre jurisdições pode estar sujeita à legislação e/ou regulamentação, a depender da jurisdição ou organização para a qual DP serão transferidos (e de onde se originam). Convém que a organização documente o *compliance* com estes requisitos como a base para transferência.

Convém que a organização informe ao cliente sobre qualquer transferência de DP incluindo transferências para:

— fornecedores;

— outras partes;

— outros países ou organizações internacionais.

Em casos de mudanças, convém que a organização informe ao cliente de forma antecipada, de acordo com um prazo acordado, de tal modo que o cliente tenha a capacidade de contestar estas mudanças ou rescindir o contrato.

O acordo entre a organização e o cliente pode ter cláusulas onde a organização possa implementar mudanças sem informar ao cliente. Nestes casos, convém que os limites desta tolerância sejam estabelecidos (por exemplo, a organização pode mudar de fornecedores sem comunicar o cliente, porém, não é possível transferir o DP para outros países).

No caso de transferência internacional de DP, acordos como Cláusulas Contratuais Modelo, Regras Corporativas de Concorrência ou Regras de Privacidade Transfronteiriça, convém que os países envolvidos e as circunstâncias nas quais estes acordos se aplicam, sejam identificados.

8.5.2 Países e organizações internacionais para os quais DP podem ser transferidos

Controle

Convém que a organização especifique e documente os países e as organizações internacionais para os quais DP possam, possivelmente, ser transferidos.

Diretrizes para implementação

Convém que a identificação dos países e organizações internacionais para os quais DP possam possivelmente ser transferidos em operações normais seja tornada disponível para os clientes. Convém que as identidades dos clientes que surgem a partir do uso de subcontratados que tratam DP sejam incluídas. Convém que os países incluídos sejam considerados quanto a 8.5.1.

Fora de operações normais, podem ocorrer casos de transferência feita por requisição de uma autoridade de aplicação da lei, para a qual não é possível identificar a identidade dos países previamente, ou que é proibida pela jurisdição aplicável para preservar a confidencialidade da investigação de aplicação da lei (ver 7.5.1, 8.5.4 e 8.5.5).

8.5.3 Registros de DP divulgados para terceiros

Controle

Convém que a organização registre a divulgação de DP para terceiros, incluindo quais DP foram divulgados, para quem e quando.

Diretrizes para implementação

DP podem ser divulgados durante o curso normal das operações. Convém que estas divulgações sejam registradas. Convém que quaisquer divulgações adicionais para terceiros, como aquelas que surgem de investigações legais ou por auditorias externas sejam registradas. Convém que os registros incluam a fonte da divulgação e a fonte da autoridade que fez a divulgação.

8.5.4 Notificação de solicitações de divulgação de DP

Controle

Convém que a organização notifique o cliente sobre quaisquer solicitações legalmente obrigatórias para a divulgação de DP.

Diretrizes para implementação

A organização pode receber solicitações legalmente obrigatórias para divulgação de DP (por exemplo, por autoridades de aplicação da lei). Nestes casos, convém que a organização notifique ao cliente sobre quaisquer solicitações dentro de um prazo acordado e de acordo com um procedimento acordado (que pode ser incluído no contrato do cliente).

Em alguns casos, solicitações legalmente obrigatórias incluem uma solicitação para a organização não notificar a ninguém sobre o evento (um exemplo de uma possível proibição sobre divulgação seria uma proibição sob uma lei criminal para preservar a confidencialidade da investigação de aplicação da lei).

8.5.5 Divulgações legalmente obrigatórias de DP

Controle

Convém que a organização rejeite quaisquer solicitações para a divulgação de DP que não sejam legalmente obrigatórias, consulte o cliente em questão antes de realizar quaisquer divulgações de DP e aceite quaisquer solicitações contratualmente acordadas para a divulgação de DP, que sejam autorizadas pelo respectivo cliente.

Diretrizes para implementação

Detalhes relevantes para a implementação do controle podem ser incluídos no contrato do cliente.

Estas solicitações podem ser originadas de várias fontes, incluindo cortes, tribunais e autoridades administrativas. Elas podem surgir de qualquer jurisdição.

8.5.6 Divulgação de subcontratados usados para tratar DP

Controle

Convém que a organização divulgue para o cliente qualquer uso de subcontratados para tratar DP, antes do uso.

Diretrizes para implementação

Convém que o fornecimento para o uso de subcontratados para tratar o DP seja incluído no contrato do cliente. Convém que informações divulgadas incluam o fato de que a subcontratação é usada e os nomes de subcontratados são pertinentes. Convém que a informação divulgada também inclua os países e as organizações internacionais para as quais os subcontratados podem transferir os dados (ver 8.5.2) e os meios pelos quais os subcontratados são obrigados a cumprir ou exceder as obrigações da organização (ver 8.5.7).

Onde divulgação pública da informação de um subcontratado for avaliada como aumento dos riscos de segurança além dos limites aceitáveis, convém que a divulgação seja feita sob um acordo de não

divulgação e/ou por uma solicitação do cliente. Convém que o cliente esteja ciente de que a informação está disponível.

Isto não está relacionado à lista de países para onde DP podem ser transferidos. Convém que esta lista seja divulgada para o cliente em todos os casos, de modo a permitir-lhes informar de maneira apropriada aos titulares de DP.

8.5.7 Contratação de um subcontratado para tratar DP

Controle

Convém que a organização somente contrate um subcontratado para tratar DP com base no contrato do cliente.

Diretrizes para implementação

Onde a organização subcontrata parte ou todo o tratamento daqueles DP para outra organização, uma autorização escrita do cliente é requerida, antes de os DP serem tratados pelo subcontratado. Isto pode ser feito na forma de cláusulas apropriadas no contrato do cliente, ou pode ser um acordo "pontual" específico.

Convém que a organização tenha um contrato por escrito com quaisquer subcontratados que ela utilize para o tratamento de DP, atuando em seu nome, e convém assegurar que seus contratos com subcontratados contemplem a implementação de controles apropriados conforme descrito no Anexo B.

Convém que o contrato entre a organização e qualquer subcontratado que esteja tratando DP em seu nome, requeira que o subcontratado implemente controles apropriados como especificado no Anexo B, considerando o processo de avaliação de riscos de segurança da informação (ver 5.4.1.2) e o escopo do tratamento de DP desempenhado pelo operador de DP (ver 6.12). Por padrão, convém que todos os controles especificados no Anexo B, sejam assumidos como pertinentes. Caso a organização decida não requerer ao subcontratado implementar os controles do Anexo B, convém justificar esta exclusão.

Um contrato pode definir as responsabilidades de cada parte diferentemente, porém, para ser consistente com este documento, convém que todos os controles sejam considerados e incluídos na informação documentada.

8.5.8 Mudança de subcontratado para tratar DP

Controle

Convém que a organização, no caso de ter uma autorização geral por escrito, informe o cliente sobre quaisquer alterações pretendidas relativas à adição ou substituição de subcontratados para tratar DP, dando assim ao cliente a oportunidade de se opor a essas alterações.

Diretrizes para implementação

Quando a organização altera a organização com a qual subcontrata parte ou todo o processamento desses DP, é necessária uma autorização por escrito do cliente para a alteração, antes de os DP serem tratados pelo novo subcontratado. Isto pode ser na forma de cláusulas apropriadas no contrato do cliente ou pode ser um contrato "pontual" específico.

Anexo A
(normativo)

SGPI – Referências específicas de controles e objetivos de controle (Controladores de DP)

Este Anexo deve ser usado pelas organizações que atuam como controladores de DP, com ou sem o uso de operadores de DP. Ele é uma extensão da ABNT NBR ISO/IEC 27001:2013, Anexo A.

Os controles e objetivos de controles acrescentados ou modificados listados na Tabela A.1 são diretamente derivados e estão alinhados com aqueles definidos neste documento e são para serem usados no contexto da ABNT NBR ISO/IEC 27001:2013, 6.1.3, como detalhado por 5.4.1.3.

Nem todos os controles e objetivos de controles listados neste Anexo precisam ser incluídos na implementação de um SGPI. Uma justificativa para exclusão de quaisquer objetivos de controle deve ser incluída na Declaração de Aplicabilidade (ver 5.4.1.3). A justificativa para exclusão pode incluir situações onde os controles não são considerados necessários pela avaliação de riscos, e onde eles não sejam requeridos pela (ou estão sujeitos a exceções sob) regulamentação e/ou legislação aplicável.

NOTA Os números das Seções neste Anexo estão relacionados com os números das subseções contidas na Seção 7.

Tabela A.1 – Controles e objetivos de controle (continua)

A.7.2 Condições para coleta e tratamento Objetivo: Determinar e documentar que o tratamento é lícito, com bases legais conforme as jurisdições aplicáveis, e com propósitos legítimos e claramente estabelecidos.		
A.7.2.1	Identificação e documentação do propósito	*Controle* A organização deve identificar e documentar os propósitos específicos pelos quais os DP serão tratados.
A.7.2.2	Identificação de bases legais	*Controle* A organização deve determinar, documentar e estar em *compliance* com a base legal pertinente para o tratamento de DP para os propósitos identificados.
A.7.2.3	Determinando quando e como o consentimento deve ser obtido	*Controle* A organização deve determinar e documentar um processo pelo qual ela possa demonstrar se, quando e como o consentimento para o tratamento de DP foi obtido dos titulares de DP.
A.7.2.4	Obtendo e registrando o consentimento	*Controle* A organização deve obter e registrar o consentimento dos titulares de DP de acordo com os processos documentados.

Tabela A.1 (continuação)

A.7.2.5	Avaliação de impacto de privacidade	*Controle* A organização deve avaliar a necessidade para, e implementar onde apropriado, uma avaliação de impacto de privacidade quando novos tratamentos de DP ou mudanças ao tratamento existente de DP forem planejados.
A.7.2.6	Contratos com operadores de DP	*Controle* A organização deve ter um contrato por escrito com qualquer operador de DP que ela utilize, e deve assegurar que os seus contratos com os operadores de DP contemplem a implementação de controles apropriados, conforme descrito no Anexo B.
A.7.2.7	Controlador conjunto de DP	*Controle* A organização deve determinar as responsabilidades e respectivos papéis para o tratamento de DP (incluindo a proteção de DP e os requisitos de segurança) com qualquer controlador conjunto de DP.
A.7.2.8	Registros relativos ao tratamento de DP	*Controle* A organização deve determinar e manter de forma segura os registros necessários ao suporte às suas obrigações para o tratamento do DP.
A.7.3 Obrigações para os titulares de DP Objetivo: Para assegurar que os titulares de DP sejam providos com informações apropriadas sobre o tratamento de seus DP e para atender quaisquer outras obrigações aplicáveis aos titulares de DP, relativas ao tratamento dos seus DP.		
A.7.3.1	Determinando e cumprindo as obrigações para os titulares de DP	*Controle* A organização deve determinar e documentar suas obrigações regulatórias, legais e de negócios para os titulares de DP, relativas ao tratamento de seus DP e fornecer meios para atender a estas obrigações.
A.7.3.2	Determinando as informações para os titulares de DP	*Controle* A organização deve determinar e documentar a informação a ser fornecida aos titulares de DP, relativa ao tratamento de seus DP, e o tempo de tal disponibilização.
A.7.3.3	Fornecendo informações aos titulares de DP	*Controle* A organização deve fornecer aos titulares de DP, de forma clara e facilmente acessível, informações que identifiquem o controlador de DP e descrevam o tratamento de seus DP.
A.7.3.4	Fornecendo mecanismos para modificar ou cancelaro consentimento	*Controle* A organização deve fornecer mecanismos para os titulares de DP para modificar ou cancelar os seus consentimentos.

Tabela A.1 (continuação)

A.7.3.5	Fornecendo mecanismos para negar o consentimento ao tratamento de DP	*Controle* A organização deve fornecer mecanismos para os titulares de DP para negar o consentimento ao tratamento do seu DP.
A.7.3.6	Acesso, correção e/ou exclusão	*Controle* A organização deve implementar políticas, procedimentos e/ou mecanismos para atender às suas obrigações para os titulares de DP acessarem, corrigirem e/ou excluírem os seus DP.
A.7.3.7	Obrigações dos controladores de DP para informar aos terceiros	*Controle* A organização deve informar aos terceiros com quem o DP foi compartilhado sobre qualquer modificação, cancelamento ou desaprovação pertinente ao DP compartilhado, e implementar políticas e procedimentos apropriados e/ou mecanismos para fazê-lo.
A.7.3.8	Fornecendo cópia do DP tratado	*Controle* A organização deve ser capaz de fornecer uma cópia do DP que é tratado, quando requerido pelo titular de DP.
A.7.3.9	Tratamento de solicitações	*Controle* A organização deve definir e documentar políticas e procedimentos para tratamento e respostas, a solicitações legítimas dos titulares de DP.
A.7.3.10	Tomada de decisão automatizada	*Controle* A organização deve identificar e considerar as obrigações, incluindo obrigações legais, para os titulares de DP, como resultado das decisões feitas pela organização que estejam relacionadas ao titular de DP, baseadas unicamente no tratamento automatizado de DP.
A.7.4 *Privacy by design* e *Privacy by Default* Objetivo: Assegurar que processos e sistemas sejam projetados de tal forma que a coleta e o tratamento (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado.		
A.7.4.1	Limite de coleta	*Controle* A organização deve limitar a coleta de DP a um mínimo que seja relevante, proporcional e necessário para os propósitos identificados.
A.7.4.2	Limite de tratamento	*Controle* A organização deve limitar o tratamento de DP de tal forma que seja adequado, relevante e necessário para os propósitos identificados.

Tabela A.1 (continuação)

A.7.4.3	Precisão e qualidade	*Controle* A organização deve assegurar e documentar que o DP é preciso, completo e atualizado, como é necessário para os propósitos aos quais ele é tratado, por meio do ciclo de vida do DP.
A.7.4.4	Objetivos de minimização de DP	*Controle* A organização deve definir e documentar os objetivos da minimização dos dados e quais mecanismos (como a anonimização) são usados para atender àqueles objetivos.
A.7.4.5	Anonimização e exclusão de DP ao final do tratamento	*Controle* A organização deve excluir DP ou entregá-lo na forma que não permita a identificação ou reidentificação dos titulares de DP, uma vez que o DP original não é mais necessário para os propósitos identificados.
A.7.4.6	Arquivos temporários	*Controle* A organização deve assegurar que os arquivos temporários criados como um resultado de tratamento de DP sejam descartados (por exemplo, apagados ou destruídos) seguindo procedimentos documentados dentro de um período documentado, especificado.
A.7.4.7	Retenção	*Controle* A organização não pode reter o DP por um tempo maior do que é necessário para os propósitos para os quais o DP é tratado.
A.7.4.8	Descarte	*Controle* A organização deve ter políticas, procedimentos e/ou mecanismos documentados para o descarte de DP.
A.7.4.9	Controles de transmissão de DP	*Controle* A organização deve tratar DP transmitido (por exemplo, enviado para outra organização) que trafegue por uma rede de transmissão de dados, com controles apropriados concebidos para assegurar que os dados alcancem seus destinos pretendidos.
A.7.5 Compartilhamento, transferência e divulgação de DP Objetivo: Determinar se e documentar quando o DP é compartilhado, transferido para outras jurisdições ou terceiros e/ou divulgado de acordo com as obrigações aplicáveis.		
A.7.5.1	Identificando as bases para a transferência de DP entre jurisdições	*Controle* A organização deve identificar e documentar as bases relevantes para a transferência de DP entre jurisdições

Tabela A.1 (conclusão)

A.7.5.2	Países e organizações internacionais para os quais DP podem ser transferidos	*Controle* A organização deve especificar e documentar os países e as organizações internacionais para os quais o DP possam possivelmente ser transferidos.
A.7.5.3	Registros de transferência de DP	*Controle* A organização deve registrar a transferência de DP para ou de terceiros e assegurar a cooperação com essas partes para apoiar futuras solicitações relativas às obrigações para os titulares de DP.
A.7.5.4	Registro de divulgação de DP para terceiros	*Controle* A organização deve registrar a divulgação de DP para terceiros, incluindo qual DP foi divulgado, para quem e quando.

Anexo B
(normativo)

SGPI – Referências específicas de controles e objetivos de controle (Operadores de DP)

Este Anexo deve ser usado pelas organizações que atuam como operadores de DP, com ou sem o uso de subcontratados de DP. Ele é uma extensão da ABNT NBR ISO/IEC 27001:2013, Anexo A.

Os controles e objetivos de controles modificados ou acrescentados listados na Tabela B.1 são diretamente derivados e estão alinhados com aqueles definidos neste documento e são para serem usados no contexto da ABNT NBR ISO/IEC 27001:2013, 6.1.3, como detalhado por 5.4.1.3.

Nem todos os controles e objetivos de controles listados neste Anexo precisam ser incluídos na implementação de um SGPI. Uma justificativa para exclusão de quaisquer objetivos de controle deve ser incluída na Declaração de Aplicabilidade (ver 5.4.1.3). A justificativa para exclusão pode incluir situações onde os controles não sejam considerados necessários pela avaliação de riscos, e onde eles não sejam requeridos pela (ou estejam sujeitos a exceções sob) regulamentação e/ou legislação aplicável.

NOTA Os números das seções neste Anexo estão relacionados com os números das subseções contidas na Seção 8.

Tabela B.1 – Controles e objetivos de controle (continua)

B.8.2 Condições para coleta e tratamento Objetivo: Documentar e determinar que o tratamento é lícito, com base legal, conforme as jurisdições aplicáveis e com propósitos legítimos e claramente definidos.		
B.8.2.1	Acordos com o cliente	*Controle* A organização deve assegurar, onde pertinente, que o contrato para tratar DP considera os papéis da organização em fornecer assistência com as obrigações do cliente (considerando a natureza do tratamento e a informação disponível para a organização).
B.8.2.2	Propósitos da organização	*Controle* A organização deve assegurar que os DP tratados em nome do cliente sejam apenas tratados para o propósito expresso nas instruções documentadas do cliente.
B.8.2.3	Uso de *marketing* e propaganda	*Controle* A organização não pode utilizar os DP tratados sob um contrato para o propósito de *marketing* e propaganda, sem o estabelecimento de que um consentimento antecipado foi obtido do titular de DP apropriado. A organização não pode fornecer este consentimento como uma condição para o recebimento do serviço.

Tabela B.1 (continuação)

B.8.2.4	Violando instruções	*Controle* A organização deve informar ao cliente se, na sua opinião, uma instrução de tratamento viola uma regulamentação e/ou legislação aplicável.
B.8.2.5	Obrigações do cliente	*Controle* A organização deve fornecer ao cliente informações apropriadas de tal modo que o cliente possa demonstrar *compliance* com suas obrigações.
B.8.2.6	Registros relativos ao tratamento de DP	*Controle* A organização deve determinar e manter os registros necessários para apoiar a demonstração do *compliance* com suas obrigações (como especificado no contrato aplicável) para tratamento de DP realizado em nome do cliente.
B.8.3 Obrigações para os titulares de DP Objetivo: Assegurar que os titulares de DP sejam providos com informações apropriadas sobre o tratamento de seus DP, e que estejam de acordo com quaisquer outras obrigações aplicáveis para os titulares de DP relativas ao tratamento de seus DP.		
B.8.3.1	Obrigações para os titulares de DP	*Controle* A organização deve fornecer ao cliente meios para estar em *compliance* com suas obrigações relativas aos titulares de DP.
B.8.4 *Privacy by design* e *Privacy by Default* Objetivo: Assegurar que processos e sistemas sejam projetados de forma que a coleta e o tratamento de DP (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado.		
B.8.4.1	Arquivos temporários	*Controle* A organização deve assegurar que os arquivos temporários criados como um resultado do tratamento de DP sejam descartados (por exemplo, apagados ou destruídos) seguindo os procedimentos documentados, dentro de um período especificado e documentado.
B.8.4.2	Retorno, transferência ou descarte de DP	*Controle* A organização deve fornecer a capacidade de retornar, transferir e/ou descartar DP de uma maneira segura. Deve também tornar sua política disponível para o cliente.
B.8.4.3	Controles de transmissão de DP	*Controle* A organização deve sujeitar DP transmitidos sobre uma rede de transmissão de dados a controles apropriados projetados, para assegurar que os dados alcancem seus destinos pretendidos.

Tabela B.1 (conclusão)

B.8.5 Compartilhamento, transferência e descarte de DP Objetivo: Determinar se e documentar quando DP são compartilhados, transferidos para outras jurisdições ou terceiros e/ou divulgados, de acordo com as obrigações aplicáveis.		
B.8.5.1	Bases para a transferência de DP entre jurisdições	*Controle* A organização deve informar ao cliente em um tempo hábil sobre as bases para a transferência de DP entre jurisdições e de qualquer mudança pretendida nesta questão, de modo que o cliente tenha a capacidade de contestar estas mudanças ou rescindir o contrato.
B.8.5.2	Países e organizações internacionais para os quais o DP podem ser transferidos	*Controle* A organização deve especificar e documentar os países e as organizações internacionais para os quais DP possam, possivelmente, ser transferidos.
B.8.5.3	Registros de DP divulgados para terceiros	*Controle* A organização deve registrar a divulgação de DP para terceiros, incluindo quais DP foram divulgados, para quem e quando.
B.8.5.4	Notificação de solicitações de divulgação de DP	*Controle* A organização deve notificar ao cliente sobre quaisquer solicitações legalmente obrigatórias para a divulgação de DP.
B.8.5.5	Divulgações legalmente obrigatórias de DP	*Controle* A organização deve rejeitar quaisquer solicitações para a divulgação de DP que não sejam legalmente obrigatórias, consultar o cliente em questão antes de realizar quaisquer divulgações do DP e aceitar quaisquer solicitações contratualmente acordadas para a divulgação de DP, que sejam autorizadas pelo respectivo cliente.
B.8.5.6	Divulgação de subcontratados usados para tratar DP	*Controle* A organização deve divulgar para o cliente qualquer uso de subcontratados para tratar DP, antes do uso.
B.8.5.7	Contratação de um subcontratado para tratar DP	*Controle* A organização deve somente contratar um subcontratado para tratar DP com base no contrato do cliente.
B.8.5.8	Mudança de subcontratado para tratar DP	*Controle* A organização deve, no caso de ter uma autorização geral por escrito, informar o cliente de quaisquer alterações pretendidas relativas à adição ou substituição de subcontratados no tratamento de DP, dando assim ao cliente a oportunidade de se opor a essas alterações.

Anexo C
(informativo)

Mapeamento com a ISO/IEC 29100

As Tabelas C.1 e C.2 fornecem um indicativo de mapeamento entre as provisões deste documento com os princípios de privacidade contidos na ISO/IEC 29100. Ele mostra simplesmente como um indicativo como o *compliance* com os requisitos e controles deste documento se relacionam com os princípios de privacidade gerais especificados na ISO/IEC 29100.

Tabela C.1 – Mapeamento dos controles para os controladores de DP e a ISO/IEC 29100 (continua)

Princípios de privacidade da ISO/IEC 29100	Controles relacionados para os Controladores de DP
1. Consentimento e escolha	A.7.2.1 Identificação e documentação do propósito A.7.2.2 Identificação de bases legais A.7.2.3 Determinando quando e como o consentimento deve ser obtido A.7.2.4 Obtendo e registrando o consentimento A.7.2.5 Avaliação de impacto de privacidade A.7.3.4 Fornecendo mecanismos para modificar ou cancelar o consentimento A.7.3.5 Fornecendo mecanismos para negar o consentimento ao tratamento de DP A.7.3.7 Obrigações dos controlares de DP para informar aos terceiros
2. Legitimidade e especificação de propósito	A.7.2.1 Identificação e documentação do propósito A.7.2.2 Identificação de bases legais A.7.2.5 Avaliação de impacto de privacidade A.7.3.2 Determinando as informações para os titulares de DP A.7.3.3 Fornecendo informações aos titulares de DP A.7.3.10 Tomada de decisão automatizada
3. Limitação de coleta	A.7.2.5 Avaliação de impacto de privacidade A.7.4.1 Limite de coleta
4. Minimização de dados	A.7.4.2 Limite de tratamento A.7.4.4 Objetivos de minimização de DP A.7.4.5 Anonimização e exclusão de DP ao final do tratamento

Tabela C.1 (conclusão)

Princípios de privacidade da ISO/IEC 29100	Controles relacionados para os Controladores de DP
5. Uso, retenção e limitação de divulgação	A.7.4.4 Objetivos de minimização de DP A.7.4.5 Anonimização e exclusão de DP ao final do tratamento A.7.4.6 Arquivos temporários A.7.4.7 Retenção A.7.4.8 Descarte A.7.5.1 Identificando as bases para a transferência de DP entre jurisdições A.7.5.4 Registro de divulgação de DP para terceiros
6. Precisão e qualidade	A.7.4.3 Precisão e qualidade
7. Abertura, transparência e notificação	A.7.3.2 Determinando as informações para os titulares de DP A.7.3.3 Fornecendo informações aos titulares de DP
8. Participação individual e acesso	A.7.3.1 Determinando e cumprindo as obrigações para os titulares de DP A.7.3.3 Fornecendo informações aos titulares de DP A.7.3.6 Acesso, correção e/ou exclusão A.7.3.8 Fornecendo cópia de DP tratado A.7.3.9 Tratamento de solicitações
9. Responsabilização	A.7.2.6 Contratos com operadores de DP A.7.2.7 Controlador conjunto de DP A.7.2.8 Registros relativos ao tratamento de DP A.7.3.9 Tratamento de solicitações A.7.5.1 Identificando as bases para a transferência de DP entre jurisdições A.7.5.2 Países e organizações internacionais para os quais o DP pode ser transferido A.7.5.3 Registros de transferência de DP
10. Segurança da informação	A.7.2.6 Contratos com operadores de DP A.7.4.9 Controle de transmissão de DP
11. *Compliance* com a privacidade	A.7.2.5 Avaliação de impacto de privacidade

Tabela C.2 – Mapeamento dos controles para os operadores de DP e a ISO/IEC 29100

Princípios de privacidade da ISO/IEC 29100	Controles relacionados dos operadores de DP
1. Consentimento e escolha	B.8.2.5 Obrigações do cliente
2. Legitimidade e especificação de objetivo	B.8.2.2 Propósitos da organização B.8.2.3 Uso de *marketing* e propaganda B.8.2.4 Violando instruções B.8.3.1 Obrigações para os titulares de DP
3. Limitação de coleta	N/A
4. Minimização de dados	B.8.4.1 Arquivos temporários
5. Uso, retenção e limitação de divulgação	B.8.5.3 Registros de DP divulgados para terceiros B.8.5.4 Notificação de solicitações de divulgação de DP B.8.5.5 Divulgações legalmente obrigatórias de DP
6. Precisão e qualidade	N/A
7. Abertura, transparência e notificação	B.8.5.6 Divulgação de subcontratados usados para tratar DP B.8.5.7 Contratação de um subcontratado para tratar DP B.8.5.8 Mudança de subcontratado para tratar DP
8. Participação individual e acesso	B.8.3.1 Obrigações para os titulares de DP
9. Responsabilização	B.8.4.2 Retorno, transferência ou descarte de DP B.8.5.1 Bases para a transferência de DP entre jurisdições B.8.5.2 Países e organizações internacionais para os quais o DP pode ser transferido
10. Segurança da informação	B.8.4.3 Controles de transmissão de DP
11. *Compliance* com a privacidade	B.8.2.5 Obrigações do cliente

Anexo D
(informativo)

Mapeamento com o *General Data Protection Regulation*

Este Anexo fornece um indicativo do mapeamento entre as provisões deste documento e os Artigos 5 a 49, exceto o 43, do *General Data Protection Regulation* (Regulamento Geral de Proteção de Dados da União Europeia). Ele mostra como o *compliance* com os requisitos e controles deste documento podem ser relevantes para cumprir as obrigações do GDPR.

Entretanto, isto é puramente indicativo e, como descrito neste documento, é responsabilidade das organizações avaliarem suas obrigações legais e decidirem como devem estar em *compliance* com elas.

Tabela D.1 – Mapeamento da estrutura da ABNT NBR ISO/IEC 27701 com os artigos do GDPR (continua)

Subseção deste documento	Artigos do GDPR
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7),(42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f), (32)(2)
6.5.2.2	(5)(1)(f)
6.5.3.1	(5)(1)(f), (32)(1)(a)
6.5.3.2	(5)(1)(f)

Tabela D.1 (continuação)

Subseção deste documento	Artigos do GDPR
6.5.3.3	(5)(1)(f), (32)(1)(a)
6.6.2.1	(5)(1)(f)
6.6.2.2	(5)(1)(f)
6.6.4.2	(5)(1)(f)
6.7.1.1	(32)(1)(a)
6.8.2.7	(5)(1)(f)
6.8.2.9	(5)(1)(f)
6.9.3.1	(5)(1)(f), (32)(1)(c)
6.9.4.1	(5)(1)(f)
6.9.4.2	(5)(1)(f)
6.10.2.1	(5)(1)(f)
6.10.2.4	(5)(1)(f), (28)(3)(b), (38)(5)
6.11.1.2	(5)(1)(f), (32)(1)(a)
6.11.2.1	(25)(1)
6.11.2.5	(25)(1)
6.11.3.1	(5)(1)(f)
6.12.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.13.1.1	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
6.13.1.5	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
6.15.1.1	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.15.1.3	(5)(2), (24)(2)
6.15.2.1	(32)(1)(d), (32)(2)
6.15.2.3	(32)(1)(d), (32)(2)
7.2.1	(5)(1)(b), (32)(4)
7.2.2	(10), (5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)

Tabela D.1 (continuação)

Subseção deste documento	Artigos do GDPR
7.2.3	(8)(1), (8)(2)
7.2.4	(7)(1), (7)(2), (9)(2)(a)
7.2.5	(35)(1), (35)(2), (35)(3)(a), (35)(3)(b), (35)(3)(c), (35)(4), (35)(5), (35)(7)(a), (35)(7)(b), (35)(7)(c), (35)(7)(d), (35)(8), (35)(9), (35)(10), (35)(11), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
7.2.6	(5)(2), (28)(3)(e), (28)(9)
7.2.7	(26)(1), (26)(2), (26)(3)
7.2.8	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(f), (30)(1)(g), (30)(3), (30)(4), (30)(5)
7.3.1	(12)(2)
7.3.2	(11)(2), (13)(3), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)
7.3.3	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
7.3.4	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
7.3.5	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
7.3.6	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
7.3.7	(19)
7.3.8	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
7.3.9	(15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (12)(3), (12)(4), (12)(5), (12)(6)
7.3.10	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)
7.4.1	(5)(1)(b), (5)(1)(c)
7.4.2	(25)(2)
7.4.3	(5)(1)(d)
7.4.4	(5)(1)(c), (5)(1)(e)
7.4.5	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)
7.4.6	(5)(1)(c)
7.4.7	(13)(2)(a), (14)(2)(a)

Tabela D.1 (conclusão)

Subseção deste documento	Artigos do GDPR
7.4.8	(5)(1)(f)
7.4.9	(5)(1)(f)
7.5.1	(15)(2), (44), (45)(1), (45)(2)(a), (45)(2)(b), (45)(2)(c), (45)(3), (45)(4), (45)(5), (45)(6), (45)(7), (45)(8), (45)(9), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (46)(4), (46)(5), (47)(1)(a), (47)(1)(b), (47)(1)(c), (47)(2)(a), (47)(2)(b), (47)(2)(c), (47)(2)(d), (47)(2)(e), (47)(2)(f), (47)(2)(g), (47)(2)(h), (47)(2)(i), (47)(2)(j), (47)(2)(k), (47)(2)(l), (47)(2)(m), (47)(2)(n), (47)(3), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6), (30)(1)(e), (48)
7.5.2	(15)(2), (30)(1)(e)
7.5.3	(30)(1)(e)
7.5.4	(30)(1)(d)
8.2.1	(28)(3)(f), (28)(3)(e), (28)(9), (35)(1)
8.2.2	(5)(1)(a), (5)(1)(b), (28)(3)(a), (29), (32)(4)
8.2.3	(7)(4)
8.2.4	(28)(3)(h)
8.2.5	(28)(3)(h)
8.2.6	(30)(3), (30)(4), (30)(5), (30)(2)(a), (30)(2)(b)
8.3.1	(15)(3), (17)(2), (28)(3)(e)
8.4.1	(5)(1)(c)
8.4.2	(28)(3)(g), (30)(1)(f)
8.4.3	(5)(1)(f)
8.5.1	(44), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)
8.5.2	(30)(2)(c)
8.5.3	(30)(1)(d)
8.5.4	(28)(3)(a)
8.5.5	(48)
8.5.6	(28)(2), (28)(4)
8.5.7	(28)(2), (28)(3)(d)
8.5.8	(28)(2)

Anexo E
(informativo)

Mapeamento das ABNT NBR ISO/IEC 27018 e ISO/IEC 29151

A ABNT NBR ISO/IEC 27018 fornece informações adicionais para as organizações que atuam como operadoras de DP e fornecem serviços públicos de computação em nuvem. A ISO/IEC 29151 fornece controles adicionais e diretrizes para o tratamento de DP pelos controladores de DP.

A Tabela E.1 fornece um indicativo de mapeamento entre as provisões deste documento e as provisões oriundas das ABNT NBR ISO/IEC 27018 e ISO/IEC 29151. Ela mostra como os requisitos e controles deste documento tem alguma correspondência com as provisões da ABNT NBR ISO/IEC 27018 e/ou ISO/IEC 29151.

Isto é puramente indicativo e convém que não seja assumido que uma relação entre essas provisões significam uma equivalência.

Tabela E.1 – Mapeamento da ABNT NBR ISO/IEC 27701 com as ABNT NBR ISO/IEC 27018 e ISO/IEC 29151 (continua)

Subseção deste documento	Subseção da ABNT NBR ISO/IEC 27018	Subseção da ISO/IEC 29151
5.2	N/A	N/A
5.3	N/A	N/A
5.4	N/A	4.2
5.5	N/A	7.2.3
5.6	N/A	N/A
5.7	N/A	N/A
5.8	N/A	N/A
6.1	N/A	N/A
6.2	5.1.1	5
6.3	6.1.1	N/A
6.4	7.2.2	N/A
6.5.1	N/A	8.1
6.5.2	N/A	8.2
6.5.3	A.11.4, A.11.5	8.3
6.6.1	N/A	N/A
6.6.2	9.2.1, A.11.8, A,11,9, A.11.10	9.2
6.6.3	N/A	9.3

Tabela E.1 (continuação)

Subseção deste documento	Subseção da ABNT NBR ISO/IEC 27018	Subseção da ISO/IEC 29151
6.6.4	7.2.2, 9.4.2	9.4
6.7	10.1.1	N/A
6.8.1	N/A	11.1
6.8.2	11.2.7, A.11.2, A.11.13	N/A
6.9.1	N/A	12.1
6.9.2	N/A	12.2
6.9.3	N/A	12.3
6.9.4	12.4.1, 12.4.2	12.4
6.9.5	N/A	N/A
6.9.6	N/A	N/A
6.9.7	N/A	N/A
6.10.1	N/A	13.1
6.10.2	13.2.1, A.11.1	13.2
6.11.1	A.11.6	N/A
6.11.2	N/A	N/A
6.11.3	12.1.4	N/A
6.12.1	A.11.11	N/A
6.12.2	N/A	N/A
6.13	16.1.1, A.10.1	N/A
6.14	N/A	N/A
6.15.1	A.10.2	N/A
6.15.2	18.2.1	18.2
7.2.1	N/A	A.4
7.2.2	N/A	A.4.1
7.2.3	N/A	N/A
7.2.4	N/A	A.3.1
7.2.5	N/A	A.11.2
7.2.6	N/A	A.11.3
7.2.7	N/A	N/A
7.2.8	N/A	N/A

Tabela E.1 (continuação)

Subseção deste documento	Subseção da ABNT NBR ISO/IEC 27018	Subseção da ISO/IEC 29151
7.3.1	N/A	A.10
7.3.2	N/A	N/A
7.3.3	N/A	A.9
7.3.4	N/A	N/A
7.3.5	N/A	N/A
7.3.6	N/A	A.10.1
7.3.7	N/A	N/A
7.3.8	N/A	N/A
7.3.9	N/A	N/A
7.3.10	N/A	N/A
7.4.1	N/A	A.5
7.4.2	N/A	N/A
7.4.3	N/A	A.8
7.4.4	N/A	N/A
7.4.5	N/A	A.7.1
7.4.6	N/A	A.7.2
7.4.7	N/A	A.7.1
7.4.8	N/A	N/A
7.4.9	N/A	N/A
7.5.1	N/A	A.13.2
7.5.2	N/A	A.13.2
7.5.3	N/A	A.13.2
7.5.4	N/A	A.7.4
8.2.1	N/A	N/A
8.2.2	A.3.1	N/A
8.2.3	A.3.2	N/A
8.2.4	N/A	N/A
8.2.5	N/A	N/A
8.2.6	N/A	N/A
8.3.1	A.2.1	N/A

Tabela E.1 (conclusão)

Subseção deste documento	Subseção da ABNT NBR ISO/IEC 27018	Subseção da ISO/IEC 29151
8.4.1	A.5.1	N/A
8.4.2	A.10.3	N/A
8.4.3	A.12.2	N/A
8.5.1	N/A	N/A
8.5.2	A.12.1	N/A
8.5.3	A.6.2	N/A
8.5.4	A.6.1	N/A
8.5.5	A.6.1	N/A
8.5.6	A.8.1	A.7.5
8.5.7	A.8.1	N/A
8.5.8	A.8.1	N/A

Anexo F
(informativo)

Como aplicar a ABNT NBR ISO/IEC 27701 com as ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002

F.1 Como usar este documento

Este documento está baseado na ABNT NBR ISO/IEC 27001:2013 e na ABNT NBR ISO/IEC 27002:2013, e estende os seus requisitos e diretrizes para considerar, em complementação à segurança da informação, a proteção da privacidade dos titulares de DP, que podem ser potencialmente afetados pelo tratamento de DP. Isto significa que, onde o termo “segurança da informação” for usado na ABNT NBR ISO/IEC 27001 ou na ABNT NBR ISO/IEC 27002, o termo “segurança da informação e privacidade” se aplica.

A Tabela F.1 apresenta o mapeamento da extensão do termo segurança da informação para fins de aplicação e uso deste documento.

Tabela F.1 – Mapeamento da extensão do termo segurança da informação por privacidade

ABNT NBR ISO/IEC 27001	Este documento (extensão)
Segurança da informação	Segurança da informação e privacidade
Política de segurança da informação	Política de segurança da informação e privacidade
Gestão da segurança da informação	Gestão da segurança da informação e privacidade da informação
Sistema de Gestão da Segurança da Informação (SGSI)	Sistema de gestão da privacidade da informação (SGPI)
Objetivos de segurança da informação	Objetivos da segurança da informação e privacidade
Desempenho da segurança da informação	Desempenho da segurança da informação e privacidade
Requisitos da segurança da informação	Requisitos da segurança da informação e privacidade
Riscos de segurança da informação	Riscos da segurança da informação e privacidade
Avaliação de riscos de segurança da informação	Avaliação de riscos de segurança da informação e privacidade
Tratamento dos riscos de segurança da informação	Tratamento dos riscos de segurança da informação e privacidade

Basicamente existem três casos para a aplicação deste documento, visando à proteção da privacidade dos titulares de DP, quando do tratamento de DP:

1) Aplicação das normas de segurança como são: As normas em referência se aplicam como elas são, com as extensões dos termos listados acima. Entretanto, as normas em referência não são repetitivas, mas apenas referenciadas para cada Seção respectiva.

2) Acréscimos de normas de segurança: As normas em referência se aplicam com os requisitos ou diretrizes adicionais específicos para privacidade;

3) Extensão de normas de segurança: As normas em referência são estendidas por requisitos ou diretrizes para implementação, específicos para privacidade.

F.2 Exemplo de extensão de normas de segurança

Esta Seção descreve como a 5.4.1.2 se aplica à ABNT NBR ISO/IEC 27001:2013, 6.1.2.

Considerando a proteção da privacidade dos titulares de DP, quando do tratamento de DP, ABNT NBR ISO/IEC 27001:2013, 6.1.2, convém que seja alterada com a seguinte descrição de texto:

6.1.2 Avaliação de riscos de segurança da informação

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

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

   1) critérios de aceitação de riscos; e

   2) critérios para o desempenho das avaliações de riscos de segurança da informação e privacidade;

b) assegure que avaliações de riscos de segurança da informação e privacidade repetidas, são consistentes, válidas e com resultados comparáveis;

c) identifique os riscos de segurança da informação e privacidade:

   1) aplique o processo de avaliação de riscos de segurança da informação e privacidade, para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade da informação dentro do escopo do sistema de gestão da segurança da informação e privacidade da informação; e

   2) identifique os proprietários dos riscos;

d) analise os riscos de segurança da informação e privacidade:

   1) avalie as consequências potenciais que podem resultar caso o risco identificado em 6.1.2-c) se materialize;

   2) avalie a probabilidade real da ocorrência dos riscos identificados em 6.1.2-c)-1); e

   3) determine os níveis de riscos;

e) avalie os riscos de segurança da informação e privacidade:

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

   2) priorize os riscos analisados para o tratamento dos riscos.

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

Anexo N/A
(informativo)

Mapeamento da ABNT NBR ISO/IEC 27701 com a LGPD

Este anexo fornece um indicativo do mapeamento entre as provisões deste documento e a LGPD-Lei Geral de Proteção de Dados Pessoais.

Ele mostra como a aplicação dos requisitos, diretrizes e controles deste documento podem ser relevantes para atender as obrigações da LGPD.

Entretanto, isto é puramente indicativo e como descrito neste documento, é responsabilidade das organizações avaliarem suas obrigações legais e decidirem como devem estar em compliance com elas.

Tabela N/A.1 – Mapeamento da estrutura da ABNT NBR ISO/IEC 27701 com os artigos da LGPD (continua)

Subseções deste documento	Artigos da LGPD
5.2.1	Artigo 50º, §1º , Artigo 5 VI, VII e IX
5.2.2	Artigo 50º
5.2.3	Artigo 50º §1º
5.2.4	Artigo 50º §2º I
5.4.1.2	Artigo 38º, Artigo 50º §1º
5.4.1.3	Artigo 38º, Artigo 50º §1º
6.2.1.1	Artigo 38º
6.3.1.1	Artigo 41º
6.3.2.1	Art. 6o., VII, Art. 46., Art. 47., Art. 49
6.4.2.2	Artigo 50º Caput
6.5.2.1	Art. 5 X, Art. 6o., VII, Art. 46., Art. 47., Art. 49
6.5.2.2	Art. 5 X, Art. 6o., VII, Art. 46., Art. 47., Art. 49
6.5.3.1	Art. 5 I, Art. 6o., VII, Art. 46., Art. 47., Art. 49.
6.5.3.2	Art. 5 X, Art. 6o., VII, Art. 46., Art. 47., Art. 49
6.5.3.3	Art. 5 X, Art. 6o., VII, Art. 46., Art. 47., Art. 49
6.6.2.1	Artigo 46
6.6.2.2	Artigos 46 e 49
6.6.4.2	Artigos 46 e 49

Tabela N/A.1 (continuação)

Subseções deste documento	Artigos da LGPD
6.7.1.1	Artigo 46
6.8.2.7	Artigo 46
6.8.2.9	Artigo 46
6.9.3.1	Artigo 46
6.9.4.1	Artigo 46
6.9.4.2	Artigo 46
6.10.2.1	Artigo 46
6.10.2.4	Artigo 46 e 47
6.11.1.2	Artigo 46
6.11.2.1	Artigo 49
6.11.2.5	Artigo 49
6.11.3.1	Artigo 46
6.12.1.2	Artigo 46
6.13.1.1	Artigo 46
6.13.1.5	Artigo 48 e 50(g)
6.15.1.1	Artigo 12 § 3º, 32, 46 § 1º, 49, 50 e 51
6.15.1.3	Artigo 6 § 1º
6.15.2.1	Artigo 50
6.15.2.3	Artigo 50
7.2.1	Art. 9º - I, Art. 14º § 6º
7.2.2	Art. 7º - II, Art. 8º § 4º, Art. 11º - IIa, Art.23º, Art. 26º - IV , Art. 34º - I
7.2.3	Art. 5º XII, Art. 7º, Art. 8º, Art. 11º, Art. 14.
7.2.4	Art. 5º XII, Art. 7º, Art. 8º, Art. 11º, Art. 14.
7.2.5	Art. 4º - § 3º, Art. 5º XVII, Art. 10º III, Art. 32º, Art. 38º
7.2.6	Art. 7º, Art. 39º
7.2.7	Art. 7º - § 5º
7.2.8	Art. 37º
7.3.1	Art. 9º
7.3.2	Art. 9º
7.3.3	Art. 9º

Tabela N/A.1 (continuação)

Subseções deste documento	Artigos da LGPD
7.3.4	Art. 8º § 5º, Art. 9º § 2º
7.3.5	Art. 8º § 5º, Art. 9º § 2º
7.3.6	Art. 9º
7.3.7	Art. 18º § 6º
7.3.8	Art. 18º II
7.3.9	Art. 18º
7.3.10	Art. 18º
7.4.1	Art. 6º - III
7.4.2	Art. 16
7.4.3	Art. 6º - V
7.4.4	Art. 6º - III
7.4.5	Art. 16º
7.4.6	CAPÍTULO VII
7.4.7	Art. 16º
7.4.8	CAPÍTULO VII
7.4.9	CAPÍTULO VII
7.5.1	Art. 7º
7.5.2	CAPÍTULO V
7.5.3	CAPÍTULO V
7.5.4	Art. 37º
8.2.1	Artigo 10o, I, II Artigo 18º.
8.2.2	Artigo 9o, I, II, III, IV, V, VI, VII Artigo 23º.
8.2.3	Artigo 6º. Artigo 9o, I, II, III, IV, V, VI, VII Artigo 10º., I
8.2.4	Artigo 44º. Artigo 45º.
8.2.5	Artigo 44º.
8.2.6	Artigo 37º.

Tabela N/A.1 (conclusão)

Subseções deste documento	Artigos da LGPD
8.3.1	Artigo 6º., I, II, III, IV, V, VI, VII, VIII, IX, X Artigo 7º., I, II, III, IV, V, VI, VII, VIII, IX, X Artigo 42º.
8.4.1	Artigo 46º. Artigo 49º.
8.4.2	Artigo 15º., I, II, III, IV Artigo 16º., I, II, III, IV Artigo 46º.
8.4.3	Artigo 6º., VII, VIII Artigo 37º. Artigo 46º.
8.5.1	Artigo 33º., I, II, III, IV, V, VI, VII, VIII, IX Artigo 34º., I, II, III, IV, V, VI
8.5.2	Artigo 33º., I, II, III, IV, V, VI, VII, VIII, IX Artigo 34º., I, II, III, IV, V, VI
8.5.3	Artigo 16º. Artigo 37º.
8.5.4	Artigo 6º., I, VI Artigo 41º.
8.5.5	Artigo 4º., III, IV Artigo 41º.
8.5.6	Artigo 41º.
8.5.7	Artigo 39º. Artigo 41º.
8.5.8	Artigo 39º. Artigo 41º.

Bibliografia

[1] ISO/IEC 19944, *Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use*

[2] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*

[3] ABNT NBR ISO/IEC 27005, *Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação*

[4] ABNTNBR ISO/IEC 27018, *Tecnologia da informação – Técnicas de segurança – Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII*

[5] ISO/IEC 27035-1, *Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management*

[6] ISO/IEC 29101, *Information technology – Security techniques – Privacy architecture framework*

[7] ISO/IEC 29134, *Information technology – Security techniques – Guidelines for privacy impact assessment*

[8] ISO/IEC 29151, *Information technology – Security techniques – Code of practice for personally identifiable information protection*

[9] ISO/IEC/DIS 29184, *Information technology – Security techniques – Guidelines for online privacy notices and consent*