NORMA
BRASILEIRA

ABNT NBR ISO/IEC 27001

Primeira edição
31.03.2006

Válida a partir de
30.04.2006

Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos

Information technology — Security techniques — Information security management systems — Requirements

Palavras-chave: Tecnologia da informação. Segurança.
Descriptors: Information technology. Security.

ICS 35.040

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO/IEC 27001:2006
34 páginas

Sede da ABNT
Av.Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 2220-1762
abnt@abnt.org.br
www.abnt.org.br

Impresso no Brasil

Sumário

Página

Prefácio Nacional iv

0 Introdução v
0.1 Geral v
0.2 Abordagem de processo v
0.3 Compatibilidade com outros sistemas de gestão vi

1 Objetivo 1
1.1 Geral 1
1.2 Aplicação 1

2 Referência normativa 2

3 Termos e definições 2

4 Sistema de gestão de segurança da informação 4
4.1 Requisitos gerais 4
4.2 Estabelecendo e gerenciando o SGSI 4
4.2.1 Estabelecer o SGSI 4
4.2.2 Implementar e operar o SGSI 6
4.2.3 Monitorar e analisar criticamente o SGSI 7
4.2.4 Manter e melhorar o SGSI 8
4.3 Requisitos de documentação 8
4.3.1 Geral 8
4.3.2 Controle de documentos 9
4.3.3 Controle de registros 9

5 Responsabilidades da direção 9
5.1 Comprometimento da direção 9
5.2 Gestão de recursos 10
5.2.1 Provisão de recursos 10
5.2.2 Treinamento, conscientização e competência 10

6 Auditorias internas do SGSI 11

7 Análise crítica do SGSI pela direção 11
7.1 Geral 11
7.2 Entradas para a análise crítica 11
7.3 Saídas da análise crítica 12

8 Melhoria do SGSI 12
8.1 Melhoria contínua 12
8.2 Ação corretiva 12
8.3 Ação preventiva 13

Anexo A (normativo) **Objetivos de controle e controles** 14

Anexo B (informativo) **Princípios da OECD e desta Norma** 31

Anexo C (informativo) **Correspondência entre a ABNT NBR ISO 9001:2000, a ABNT NBR ISO 14001:2004 e esta Norma** 32

Bibliografia 34

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Fórum 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 Temporárias (ABNT/CEET), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

A ABNT NBR ISO/IEC 27001 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:204.01). O Projeto circulou em Consulta Nacional conforme Edital nº 12, de 31.12.2005, com o número de Projeto 21:204.01-012.

Esta Norma é uma tradução idêntica da ISO/IEC 27001:2005, que foi elaborada pelo *Join Technical Committee Information Technology* (ISO/IEC/JTC 1), *subcommittee IT Security Tecchniques* (SC 27).

Esta Norma contém o anexo A, de caráter normativo, e os anexos B e C, de caráter informativo.

0 Introdução

0.1 Geral

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

Esta Norma pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas.

0.2 Abordagem de processo

Esta Norma promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI de uma organização.

Uma organização precisa identificar e gerenciar muitas atividades para funcionar efetivamente. Qualquer atividade que faz uso de recursos e os gerencia para habilitar a transformação de entradas em saídas pode ser considerada um processo. Freqüentemente a saída de um processo forma diretamente a entrada do processo seguinte.

A aplicação de um sistema de processos dentro de uma organização, junto com a identificação e interações destes processos, e a sua gestão podem ser consideradas como "abordagem de processo".

A abordagem de processo para a gestão da segurança da informação apresentada nesta Norma encoraja que seus usuários enfatizem a importância de:

a) entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;

b) implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;

c) monitoração e análise crítica do desempenho e eficácia do SGSI; e

d) melhoria contínua baseada em medições objetivas.

Esta Norma adota o modelo conhecido como "*Plan-Do-Check-Act*" (PDCA), que é aplicado para estruturar todos os processos do SGSI. A figura 1 ilustra como um SGSI considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e expectativas. A figura 1 também ilustra os vínculos nos processos apresentados nas seções 4, 5, 6, 7 e 8.

A adoção do modelo PDCA também refletirá os princípios como definidos nas Diretrizes da OECD[1)] (2002) para governar a segurança de sistemas de informação e redes. Esta Norma provê um modelo robusto para

[1)] Diretrizes da OECD para a Segurança de Sistemas de Informação e Redes - Para uma Cultura de Segurança. Paris: OECD, 2002 de julho. http://www.oecd.org.

implementar os princípios nessas diretrizes para direcionar a análise/avaliação de riscos, especificação e implementação de segurança, gerenciamento de segurança e reavaliação.

EXEMPLO 1

Um requisito pode significar que violações de segurança da informação não causem sérios danos financeiros e/ou constrangimentos à organização.

EXEMPLO 2

Uma expectativa pode significar que se um incidente grave ocorrer – por exemplo, a invasão da página Internet de comércio eletrônico de uma organização – deveria haver pessoas com treinamento suficiente nos procedimentos apropriados para minimizar o impacto.

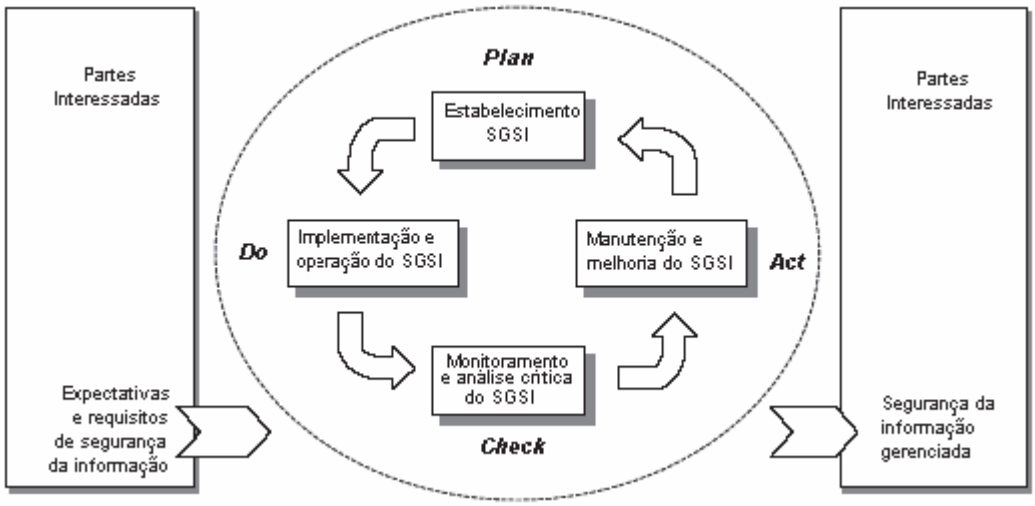

Figura 1 — Modelo PDCA aplicado aos processos do SGSI

***Plan* (planejar) (estabelecer o SGSI)**	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
***Do* (fazer) (implementar e operar o SGSI)**	Implementar e operar a política, controles, processos e procedimentos do SGSI.
***Check* (checar) (monitorar e analisar criticamente o SGSI)**	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
***Act* (agir) (manter e melhorar o SGSI)**	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

0.3 Compatibilidade com outros sistemas de gestão

Esta Norma está alinhada às ABNT NBR ISO 9001:2000 e ABNT NBR ISO 14001:2004 para apoiar a implementação e a operação de forma consistente e integrada com normas de gestão relacionadas. Um sistema

de gestão adequadamente projetado pode, assim, satisfazer os requisitos de todas estas normas. A tabela C.1 ilustra a relação entre as seções desta Norma, da ABNT NBR ISO 9001:2000 e da ABNT NBR ISO 14001:2004.

Esta Norma é projetada para permitir a uma organização alinhar ou integrar seu SGSI com requisitos de sistemas de gestão relacionados.

Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos

IMPORTANTE – Esta publicação não tem o propósito de incluir todas as cláusulas necessárias a um contrato. Os usuários são responsáveis pela sua correta aplicação. Conformidade com esta Norma por si só não confere imunidade em relação às obrigações legais.

1 Objetivo

1.1 Geral

Esta Norma cobre todos os tipos de organizações (por exemplo, empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos). Esta Norma especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes.

O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas.

NOTA 1 Convém que referências a “negócio” nesta Norma sejam interpretadas, de modo geral, tendo em vista as atividades que são essenciais aos objetivos de existência da organização.

NOTA 2 A ABNT NBR ISO/IEC 17799:2005 provê orientação para implementação que pode ser usada quando da especificação de controles.

1.2 Aplicação

Os requisitos definidos nesta Norma são genéricos e é pretendido que sejam aplicáveis a todas as organizações, independentemente de tipo, tamanho e natureza. A exclusão de quaisquer dos requisitos especificados nas seções 4, 5, 6, 7, e 8 não é aceitável quando uma organização reivindica conformidade com esta Norma.

Qualquer exclusão de controles considerados necessários para satisfazer aos critérios de aceitação de riscos precisa ser justificada e as evidências de que os riscos associados foram aceitos pelas pessoas responsáveis precisam ser fornecidas. Onde quaisquer controles sejam excluídos, reivindicações de conformidade a esta Norma não são aceitáveis, a menos que tais exclusões não afetem a capacidade da organização, e/ou responsabilidade de prover segurança da informação que atenda os requisitos de segurança determinados pela análise/avaliação de riscos e por requisitos legais e regulamentares aplicáveis.

NOTA Se uma organização já tiver um sistema de gestão de processo de negócio em operação (por exemplo, em relação com a ABNT NBR ISO 9001 ou ABNT NBR ISO 14001), é preferível na maioria dos casos satisfazer os requisitos desta Norma dentro deste sistema de gestão existente.

2 Referência normativa

O documento a seguir referenciado é indispensável para a aplicação desta Norma. Para referência datada, aplica-se apenas a edição citada. Para referência não datada, aplica-se a última edição do documento referenciado (incluindo as emendas).

ABNT NBR ISO/IEC 17799:2005, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.

3 Termos e definições

Para os efeitos desta Norma, aplicam-se os seguintes termos e definições.

3.1
ativo
qualquer coisa que tenha valor para a organização

[ISO/IEC 13335-1:2004]

3.2
disponibilidade
propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada

[ISO/IEC 13335-1:2004]

3.3
confidencialidade
propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados

[ISO/IEC 13335-1:2004]

3.4
segurança da informação
preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas

[ABNT NBR ISO/IEC 17799:2005]

3.5
evento de segurança da informação
uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação

[ISO/IEC TR 18044:2004]

3.6
incidente de segurança da informação
um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação

[ISO/IEC TR 18044:2004]

3.7
sistema de gestão da segurança da informação
SGSI
a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação

NOTA O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.

3.8
integridade
propriedade de salvaguarda da exatidão e completeza de ativos

[ISO/IEC 13335-1:2004]

3.9
risco residual
risco remanescente após o tratamento de riscos

[ABNT ISO/IEC Guia 73:2005]

3.10
aceitação do risco
decisão de aceitar um risco

[ABNT ISO/IEC Guia 73:2005]

3.11
análise de riscos
uso sistemático de informações para identificar fontes e estimar o risco

[ABNT ISO/IEC Guia 73:2005]

3.12
análise/avaliação de riscos
processo completo de análise e avaliação de riscos

[ABNT ISO/IEC Guia 73:2005]

3.13
avaliação de riscos
processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco

[ABNT ISO/IEC Guia 73:2005]

3.14
gestão de riscos
atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos

NOTA A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.

[ABNT ISO/IEC Guia 73:2005]

3.15
tratamento do risco
processo de seleção e implementação de medidas para modificar um risco

[ABNT ISO/IEC Guia 73:2005]

NOTA Nesta Norma o termo “controle” é usado como um sinônimo para “medida”.

3.16
declaração de aplicabilidade
declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI da organização

NOTA Os objetivos de controle e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.

4 Sistema de gestão de segurança da informação

4.1 Requisitos gerais

A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta. Para os efeitos desta Norma, o processo usado está baseado no modelo de PDCA mostrado na figura 1.

4.2 Estabelecendo e gerenciando o SGSI

4.2.1 Estabelecer o SGSI

A organização deve:

a) Definir o escopo e os limites do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo (ver 1.2);

b) Definir uma política do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia que:

   1) inclua uma estrutura para definir objetivos e estabeleça um direcionamento global e princípios para ações relacionadas com a segurança da informação;

   2) considere requisitos de negócio, legais e/ou regulamentares, e obrigações de segurança contratuais;

   3) esteja alinhada com o contexto estratégico de gestão de riscos da organização no qual o estabelecimento e manutenção do SGSI irão ocorrer ;

   4) estabeleça critérios em relação aos quais os riscos serão avaliados (ver 4.2.1c)); e

   5) tenha sido aprovada pela direção.

NOTA Para os efeitos desta Norma, a política do SGSI é considerada um documento maior da política de segurança da informação. Estas políticas podem estar descritas em um documento.

c) Definir a abordagem de análise/avaliação de riscos da organização.

1) Identificar uma metodologia de análise/avaliação de riscos que seja adequada ao SGSI e aos requisitos legais, regulamentares e de segurança da informação, identificados para o negócio.

2) Desenvolver critérios para a aceitação de riscos e identificar os níveis aceitáveis de risco (ver 5.1f)).

A metodologia de análise/avaliação de riscos selecionada deve assegurar que as análises/avaliações de riscos produzam resultados comparáveis e reproduzíveis.

NOTA Existem diferentes metodologias para análise/avaliação de riscos. São discutidos exemplos de metodologias de análise/avaliação de riscos na ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security*.

d) Identificar os riscos.

1) Identificar os ativos dentro do escopo do SGSI e os proprietários[2)] destes ativos.

2) Identificar as ameaças a esses ativos.

3) Identificar as vulnerabilidades que podem ser exploradas pelas ameaças.

4) Identificar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.

e) Analisar e avaliar os riscos.

1) Avaliar os impactos para o negócio da organização que podem resultar de falhas de segurança, levando em consideração as conseqüências de uma perda de confidencialidade, integridade ou disponibilidade dos ativos.

2) Avaliar a probabilidade real da ocorrência de falhas de segurança à luz de ameaças e vulnerabilidades prevalecentes, e impactos associados a estes ativos e os controles atualmente implementados.

3) Estimar os níveis de riscos.

4) Determinar se os riscos são aceitáveis ou se requerem tratamento utilizando os critérios para aceitação de riscos estabelecidos em 4.2.1c)2).

f) Identificar e avaliar as opções para o tratamento de riscos.

Possíveis ações incluem:

1) aplicar os controles apropriados;

2) aceitar os riscos consciente e objetivamente, desde que satisfaçam claramente às políticas da organização e aos critérios de aceitação de riscos (ver 4.2.1c)2));

3) evitar riscos; e

4) transferir os riscos associados ao negócio a outras partes, por exemplo, seguradoras e fornecedores.

---

2) O termo 'proprietário' identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo 'proprietário' não significa que a pessoa realmente tenha qualquer direito de propriedade ao ativo.

g) Selecionar objetivos de controle e controles para o tratamento de riscos.

Objetivos de controle e controles devem ser selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos e pelo processo de tratamento de riscos. Esta seleção deve considerar os critérios para aceitação de riscos (ver 4.2.1c)2)) como também os requisitos legais, regulamentares e contratuais.

Os objetivos de controle e controles do anexo A devem ser selecionados como parte deste processo, como adequados para cobrir os requisitos identificados.

Os objetivos de controle e controles listados no anexo A não são exaustivos, e objetivos de controles e controles adicionais podem também ser selecionados.

NOTA O anexo A contém uma lista detalhada de objetivos de controle e controles que foram comumente considerados relevantes nas organizações. Os usuários desta Norma são direcionados para o anexo A como um ponto de partida para a seleção de controles, para assegurar que nenhuma opção de controle importante seja negligenciada.

h) Obter aprovação da direção dos riscos residuais propostos.

i) Obter autorização da direção para implementar e operar o SGSI.

j) Preparar uma Declaração de Aplicabilidade.

Uma Declaração de Aplicabilidade deve ser preparada, incluindo o seguinte:

1) Os objetivos de controle e os controles selecionados em 4.2.1g) e as razões para sua seleção;

2) Os objetivos de controle e os controles atualmente implementados (ver 4.2.1e)2)); e

3) A exclusão de quaisquer objetivos de controle e controles do anexo A e a justificativa para sua exclusão.

NOTA A Declaração de Aplicabilidade provê um resumo das decisões relativas ao tratamento de riscos. A justificativa das exclusões provê uma checagem cruzada de que nenhum controle foi omitido inadvertidamente.

4.2.2 Implementar e operar o SGSI

A organização deve:

a) Formular um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para a gestão dos riscos de segurança (ver seção 5).

b) Implementar o plano de tratamento de riscos para alcançar os objetivos de controle identificados, que inclua considerações de financiamentos e atribuição de papéis e responsabilidades.

c) Implementar os controles selecionados em 4.2.1g) para atender aos objetivos de controle.

d) Definir como medir a eficácia dos controles ou grupos de controles selecionados, e especificar como estas medidas devem ser usadas para avaliar a eficácia dos controles de modo a produzir resultados comparáveis e reproduzíveis (ver 4.2.3c)).

NOTA A medição da eficácia dos controles permite aos gestores e à equipe determinar o quanto os controles alcançam de forma satisfatória os objetivos de controle planejados.

e) Implementar programas de conscientização e treinamento (ver 5.2.2).

f) Gerenciar as operações do SGSI.

g) Gerenciar os recursos para o SGSI (ver 5.2).

h) Implementar procedimentos e outros controles capazes de permitir a pronta detecção de eventos de segurança da informação e resposta a incidentes de segurança da informação (ver 4.2.3 a)).

4.2.3 Monitorar e analisar criticamente o SGSI

A organização deve:

a) Executar procedimentos de monitoração e análise crítica e outros controles para:

   1) prontamente detectar erros nos resultados de processamento;

   2) prontamente identificar tentativas e violações de segurança bem-sucedidas, e incidentes de segurança da informação;

   3) permitir à direção determinar se as atividades de segurança da informação delegadas a pessoas ou implementadas por meio de tecnologias de informação são executadas conforme esperado;

   4) ajudar a detectar eventos de segurança da informação e assim prevenir incidentes de segurança da informação pelo uso de indicadores; e

   5) determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes.

b) Realizar análises críticas regulares da eficácia do SGSI (incluindo o atendimento da política e dos objetivos do SGSI, e a análise crítica de controles de segurança), levando em consideração os resultados de auditorias de segurança da informação, incidentes de segurança da informação, resultados da eficácia das medições, sugestões e realimentação de todas as partes interessadas.

c) Medir a eficácia dos controles para verificar que os requisitos de segurança da informação foram atendidos.

d) Analisar criticamente as análises/avaliações de riscos a intervalos planejados e analisar criticamente os riscos residuais e os níveis de riscos aceitáveis identificados, levando em consideração mudanças relativas a:

   1) organização;

   2) tecnologias;

   3) objetivos e processos de negócio;

   4) ameaças identificadas;

   5) eficácia dos controles implementados;

   6) eventos externos, tais como mudanças nos ambientes legais ou regulamentares, alterações das obrigações contratuais e mudanças na conjuntura social.

e) Conduzir auditorias internas do SGSI a intervalos planejados (ver seção 6).

   NOTA Auditorias internas, às vezes chamadas de auditorias de primeira parte, são conduzidas por ou em nome da própria organização para propósitos internos.

f) Realizar uma análise crítica do SGSI pela direção em bases regulares para assegurar que o escopo permanece adequado e que são identificadas melhorias nos processos do SGSI (ver 7.1).

g) Atualizar os planos de segurança da informação para levar em consideração os resultados das atividades de monitoramento e análise crítica.

h) Registrar ações e eventos que possam ter um impacto na eficácia ou no desempenho do SGSI (ver 4.3.3).

4.2.4 Manter e melhorar o SGSI

A organização deve regularmente :

a) Implementar as melhorias identificadas no SGSI.

b) Executar as ações preventivas e corretivas apropriadas de acordo com 8.2 e 8.3. Aplicar as lições aprendidas de experiências de segurança da informação de outras organizações e aquelas da própria organização.

c) Comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhe apropriado às circunstâncias e, se relevante, obter a concordância sobre como proceder.

d) Assegurar-se de que as melhorias atinjam os objetivos pretendidos.

4.3 Requisitos de documentação

4.3.1 Geral

A documentação deve incluir registros de decisões da direção, assegurar que as ações sejam rastreáveis às políticas e decisões da direção, e assegurar que os resultados registrados sejam reproduzíveis.

É importante que se possa demonstrar a relação dos controles selecionados com os resultados da análise/avaliação de riscos e do processo de tratamento de riscos, e conseqüentemente com a política e objetivos do SGSI.

A documentação do SGSI deve incluir:

a) declarações documentadas da política (ver 4.2.1b)) e objetivos do SGSI;

b) o escopo do SGSI (ver 4.2.1a));

c) procedimentos e controles que apoiam o SGSI;

d) uma descrição da metodologia de análise/avaliação de riscos (ver 4.2.1c));

e) o relatório de análise/avaliação de riscos (ver 4.2.1c) a 4.2.1g));

f) o plano de tratamento de riscos (ver 4.2.2b));

g) procedimentos documentados requeridos pela organização para assegurar o planejamento efetivo, a operação e o controle de seus processos de segurança de informação e para descrever como medir a eficácia dos controles (ver 4.2.3c));

h) registros requeridos por esta Norma (ver 4.3.3); e

i) a Declaração de Aplicabilidade.

NOTA 1 Onde o termo "procedimento documentado" aparecer nesta Norma, significa que o procedimento é estabelecido, documentado, implementado e mantido.

NOTA 2 A abrangência da documentação do SGSI pode variar de uma organização para outra devido ao:

— tamanho da organização e o tipo de suas atividades; e

— escopo e complexidade dos requisitos de segurança e o do sistema gerenciado.

NOTA 3 Documentos e registros podem estar em qualquer forma ou tipo de mídia.

4.3.2 Controle de documentos

Os documentos requeridos pelo SGSI devem ser protegidos e controlados. Um procedimento documentado deve ser estabelecido para definir as ações de gestão necessárias para:

a) aprovar documentos para adequação antes de sua emissão;

b) analisar criticamente e atualizar, quando necessário, e reaprovar documentos;

c) assegurar que as alterações e a situação da revisão atual dos documentos sejam identificadas;

d) assegurar que as versões pertinentes de documentos aplicáveis estejam disponíveis nos locais de uso;

e) assegurar que os documentos permaneçam legíveis e prontamente identificáveis;

f) assegurar que os documentos estejam disponíveis àqueles que deles precisam e sejam transferidos, armazenados e finalmente descartados conforme os procedimentos aplicáveis à sua classificação;

g) assegurar que documentos de origem externa sejam identificados;

h) assegurar que a distribuição de documentos seja controlada;

i) prevenir o uso não intencional de documentos obsoletos; e

j) aplicar identificação adequada nos casos em que sejam retidos para qualquer propósito.

4.3.3 Controle de registros

Registros devem ser estabelecidos e mantidos para fornecer evidências de conformidade aos requisitos e da operação eficaz do SGSI. Eles devem ser protegidos e controlados. O SGSI deve levar em consideração quaisquer requisitos legais ou regulamentares pertinentes e obrigações contratuais. Os registros devem permanecer legíveis, prontamente identificáveis e recuperáveis. Os controles necessários para a identificação, armazenamento, proteção, recuperação, tempo de retenção e disposição de registros devem ser documentados e implementados.

Devem ser mantidos registros do desempenho do processo como definido em 4.2 e de todas as ocorrências de incidentes de segurança da informação significativos relacionados ao SGSI.

EXEMPLO

Exemplos de registros são: livros de visitantes, relatórios de auditoria e formulários de autorização de acesso preenchidos.

5 Responsabilidades da direção

5.1 Comprometimento da direção

A Direção deve fornecer evidência do seu comprometimento com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria do SGSI mediante:

a) o estabelecimento da política do SGSI;

b) a garantia de que são estabelecidos os planos e objetivos do SGSI;

c) o estabelecimento de papéis e responsabilidades pela segurança de informação;

d) a comunicação à organização da importância em atender aos objetivos de segurança da informação e a conformidade com a política de segurança de informação, suas responsabilidades perante a lei e a necessidade para melhoria contínua;

e) a provisão de recursos suficientes para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI (ver 5.2.1);

f) a definição de critérios para aceitação de riscos e dos níveis de riscos aceitáveis;

g) a garantia de que as auditorias internas do SGSI sejam realizadas (ver seção 6); e

h) a condução de análises críticas do SGSI pela direção (ver seção 7).

5.2 Gestão de recursos

5.2.1 Provisão de recursos

A organização deve determinar e prover os recursos necessários para:

a) estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI;

b) assegurar que os procedimentos de segurança da informação apoiam os requisitos de negócio;

c) identificar e tratar os requisitos legais e regulamentares e obrigações contratuais de segurança da informação;

d) manter a segurança da informação adequada pela aplicação correta de todos os controles implementados;

e) realizar análises críticas, quando necessário, e reagir adequadamente aos resultados destas análises críticas; e

f) onde requerido, melhorar a eficácia do SGSI.

5.2.2 Treinamento, conscientização e competência

A organização deve assegurar que todo o pessoal que tem responsabilidades atribuídas definidas no SGSI seja competente para desempenhar as tarefas requeridas:

a) determinando as competências necessárias para o pessoal que executa trabalhos que afetam o SGSI;

b) fornecendo treinamento ou executando outras ações (por exemplo, contratar pessoal competente) para satisfazer essas necessidades;

c) avaliando a eficácia das ações executadas; e

d) mantendo registros de educação, treinamento, habilidades, experiências e qualificações (ver 4.3.3).

A organização deve também assegurar que todo o pessoal pertinente esteja consciente da relevância e importância das suas atividades de segurança da informação e como eles contribuem para o alcance dos objetivos do SGSI.

6 Auditorias internas do SGSI

A organização deve conduzir auditorias internas do SGSI a intervalos planejados para determinar se os objetivos de controle, controles, processos e procedimentos do seu SGSI:

a) atendem aos requisitos desta Norma e à legislação ou regulamentações pertinentes;

b) atendem aos requisitos de segurança da informação identificados;

c) estão mantidos e implementados eficazmente; e

d) são executados conforme esperado.

Um programa de auditoria deve ser planejado levando em consideração a situação e a importância dos processos e áreas a serem auditadas, bem como os resultados de auditorias anteriores. Os critérios da auditoria, escopo, freqüência e métodos devem ser definidos. A seleção dos auditores e a execução das auditorias devem assegurar objetividade e imparcialidade do processo de auditoria. Os auditores não devem auditar seu próprio trabalho.

As responsabilidades e os requisitos para planejamento e para execução de auditorias e para relatar os resultados e a manutenção dos registros (ver 4.3.3) devem ser definidos em um procedimento documentado.

O responsável pela área a ser auditada deve assegurar que as ações sejam executadas, sem demora indevida, para eliminar as não-conformidades detectadas e suas causas. As atividades de acompanhamento devem incluir a verificação das ações executadas e o relato dos resultados de verificação (ver seção 8).

NOTA A ABNT NBR ISO 19011:2002 – *Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental* – pode prover uma orientação útil para realizar auditorias internas do SGSI.

7 Análise crítica do SGSI pela direção

7.1 Geral

A direção deve analisar criticamente o SGSI da organização a intervalos planejados (pelo menos uma vez por ano) para assegurar a sua contínua pertinência, adequação e eficácia. Esta análise crítica deve incluir a avaliação de oportunidades para melhoria e a necessidade de mudanças do SGSI, incluindo a política de segurança da informação e objetivos de segurança da informação. Os resultados dessas análises críticas devem ser claramente documentados e os registros devem ser mantidos (ver 4.3.3).

7.2 Entradas para a análise crítica

As entradas para a análise crítica pela direção devem incluir:

a) resultados de auditorias do SGSI e análises críticas;

b) realimentação das partes interessadas;

c) técnicas, produtos ou procedimentos que podem ser usados na organização para melhorar o desempenho e a eficácia do SGSI ;

d) situação das ações preventivas e corretivas;

e) vulnerabilidades ou ameaças não contempladas adequadamente nas análises/avaliações de risco anteriores;

f) resultados da eficácia das medições ;

g) acompanhamento das ações oriundas de análises críticas anteriores pela direção;

h) quaisquer mudanças que possam afetar o SGSI; e

i) recomendações para melhoria.

7.3 Saídas da análise crítica

As saídas da análise crítica pela direção devem incluir quaisquer decisões e ações relacionadas a:

a) Melhoria da eficácia do SGSI.

b) Atualização da análise/avaliação de riscos e do plano de tratamento de riscos.

c) Modificação de procedimentos e controles que afetem a segurança da informação, quando necessário, para responder a eventos internos ou externos que possam impactar no SGSI, incluindo mudanças de:

   1) requisitos de negócio;

   2) requisitos de segurança da informação;

   3) processos de negócio que afetem os requisitos de negócio existentes;

   4) requisitos legais ou regulamentares;

   5) obrigações contratuais; e

   6) níveis de riscos e/ou critérios de aceitação de riscos.

d) Necessidade de recursos.

e) Melhoria de como a eficácia dos controles está sendo medida.

8 Melhoria do SGSI

8.1 Melhoria contínua

A organização deve continuamente melhorar a eficácia do SGSI por meio do uso da política de segurança da informação, objetivos de segurança da informação, resultados de auditorias, análises de eventos monitorados, ações corretivas e preventivas e análise crítica pela direção (ver seção 7).

8.2 Ação corretiva

A organização deve executar ações para eliminar as causas de não-conformidades com os requisitos do SGSI, de forma a evitar a sua repetição. O procedimento documentado para ação corretiva deve definir requisitos para:

a) identificar não-conformidades;

b) determinar as causas de não-conformidades;

c) avaliar a necessidade de ações para assegurar que aquelas não-conformidades não ocorram novamente;

d) determinar e implementar as ações corretivas necessárias;

e) registrar os resultados das ações executadas (ver 4.3.3); e

f) analisar criticamente as ações corretivas executadas.

8.3 Ação preventiva

A organização deve determinar ações para eliminar as causas de não-conformidades potenciais com os requisitos do SGSI, de forma a evitar a sua ocorrência. As ações preventivas tomadas devem ser apropriadas aos impactos dos potenciais problemas. O procedimento documentado para ação preventiva deve definir requisitos para:

a) identificar não-conformidades potenciais e suas causas;

b) avaliar a necessidade de ações para evitar a ocorrência de não-conformidades;

c) determinar e implementar as ações preventivas necessárias;

d) registrar os resultados de ações executadas (ver 4.3.3); e

e) analisar criticamente as ações preventivas executadas.

A organização deve identificar mudanças nos riscos e identificar requisitos de ações preventivas focando a atenção nos riscos significativamente alterados.

A prioridade de ações preventivas deve ser determinada com base nos resultados da análise/avaliação de riscos.

NOTA Ações para prevenir não-conformidades freqüentemente têm melhor custo-benefício que as ações corretivas.

Anexo A
(normativo)

Objetivos de controle e controles

Os objetivos de controle e controles listados na tabela A.1 são derivados diretamente e estão alinhados com aqueles listados na ABNT NBR ISO/IEC 17799:2005 – seções 5 a 15. As listas na tabela A.1 não são exaustivas e uma organização pode considerar que objetivos de controle e controles adicionais são necessários. Os objetivos de controle e controles desta tabela devem ser selecionados como parte do processo de SGSI especificado em 4.2.1.

A ABNT NBR ISO/IEC 17799:2005 - seções 5 a 15 fornece recomendações e um guia de implementação das melhores práticas para apoiar os controles especificados em A.5 a A.15.

Tabela A.1 — Objetivos de controle e controles

A.5 Política de segurança		
A.5.1 Política de segurança da informação *Objetivo:* Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.		
A.5.1.1	Documento da política de segurança da informação	*Controle* Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica da política de segurança da informação	*Controle* A política de segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.
A.6 Organizando a segurança da informação		
A.6.1 Infra-estrutura da segurança da informação *Objetivo:* Gerenciar a segurança da informação dentro da organização.		
A.6.1.1	Comprometimento da direção com a segurança da informação	*Controle* A Direção deve apoiar ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação.
A.6.1.2	Coordenação da segurança da informação	*Controle* As atividades de segurança da informação devem ser coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.

A.6.1.3	Atribuição de responsabilidades para a segurança da informação	*Controle* Todas as responsabilidades pela segurança da informação devem estar claramente definidas.
A.6.1.4	Processo de autorização para os recursos de processamento da informação	*Controle* Deve ser definido e implementado um processo de gestão de autorização para novos recursos de processamento da informação.
A.6.1.5	Acordos de confidencialidade	*Controle* Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados e analisados criticamente, de forma regular.
A.6.1.6	Contato com autoridades	*Controle* Contatos apropriados com autoridades relevantes devem ser mantidos.
A.6.1.7	Contato com grupos especiais	*Controle* Contatos apropriados com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais devem ser mantidos.
A.6.1.8	Análise crítica independente de segurança da informação	*Controle* O enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação) deve ser analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.
A.6.2 Partes externas *Objetivo:* Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.		
A.6.2.1	Identificação dos riscos relacionados com partes externas	*Controle* Os riscos para os recursos de processamento da informação e para a informação da organização oriundos de processos do negócio que envolvam as partes externas devem ser identificados e controles apropriados devem ser implementados antes de se conceder o acesso.
A.6.2.2	Identificando a segurança da informação quando tratando com os clientes.	*Controle* Todos os requisitos de segurança da informação identificados devem ser considerados antes de conceder aos clientes o acesso aos ativos ou às informações da organização.
A.6.2.3	Identificando segurança da informação nos acordos com terceiros	*Controle* Os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos de processamento da informação ou da informação da organização, ou o acréscimo de produtos ou serviços aos recursos de processamento da informação devem cobrir todos os requisitos de segurança da informação relevantes.

A.7 Gestão de ativos		
A.7.1 Responsabilidade pelos ativos		
Objetivo: Alcançar e manter a proteção adequada dos ativos da organização.		
A.7.1.1	Inventário dos ativos	*Controle* Todos os ativos devem ser claramente identificados e um inventário de todos os ativos importantes deve ser estruturado e mantido.
A.7.1.2	Proprietário dos ativos	*Controle* Todas as informações e ativos associados com os recursos de processamento da informação devem ter um "proprietário"[3)] designado por uma parte definida da organização.
A.7.1.3	Uso aceitável dos ativos	*Controle* Devem ser identificadas, documentadas e implementadas regras para que seja permitido o uso de informações e de ativos associados aos recursos de processamento da informação.
A.7.2 Classificação da informação		
Objetivo: Assegurar que a informação receba um nível adequado de proteção.		
A.7.2.1	Recomendações para classificação	*Controle* A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.
A.7.2.2	Rótulos e tratamento da informação	*Controle* Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser definido e implementado de acordo com o esquema de classificação adotado pela organização.
A.8 Segurança em recursos humanos		
A.8.1 Antes da contratação[4)]		
Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades, e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos.		
A.8.1.1	Papéis e responsabilidades	*Controle* Os papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros devem ser definidos e documentados de acordo com a política de segurança da informação da organização.

[3)] Explicação: O termo “proprietário” identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo “proprietário” não significa que a pessoa realmente tenha qualquer direito de propriedade pelo ativo

[4)] Explicação: A palavra “contratação”, neste contexto, visa cobrir todas as seguintes diferentes situações: contratação de pessoas (temporárias ou por longa duração), nomeação de funções, mudança de funções, atribuições de contratos e encerramento de quaisquer destas situações.

A.8.1.2	Seleção	*Controle* Verificações de controle de todos os candidatos a emprego, fornecedores e terceiros devem ser realizadas de acordo com as leis relevantes, regulamentações e éticas, e proporcionalmente aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.
A.8.1.3	Termos e condições de contratação	*Controle* Como parte das suas obrigações contratuais, os funcionários, fornecedores e terceiros devem concordar e assinar os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidade e da organização para a segurança da informação.
A.8.2 Durante a contratação		
Objetivo: Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.		
A.8.2.1	Responsabilidades da direção	*Controle* A direção deve solicitar aos funcionários, fornecedores e terceiros que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.
A.8.2.2	Conscientização, educação e treinamento em segurança da informação	*Controle* Todos os funcionários da organização e, onde pertinente, fornecedores e terceiros devem receber treinamento apropriado em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais relevantes para as suas funções.
A.8.2.3	Processo disciplinar	*Controle* Deve existir um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação.
A.8.3 Encerramento ou mudança da contratação		
Objetivo: Assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.		
A.8.3.1	Encerramento de atividades	*Controle* As responsabilidades para realizar o encerramento ou a mudança de um trabalho devem ser claramente definidas e atribuídas.
A.8.3.2	Devolução de ativos	*Controle* Todos os funcionários, fornecedores e terceiros devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.

A.8.3.3	Retirada de direitos de acesso	*Controle* Os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou devem ser ajustados após a mudança destas atividades.
A.9 Segurança física e do ambiente		
A.9.1 Áreas seguras *Objetivo:* Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.		
A.9.1.1	Perímetro de segurança física	*Controle* Devem ser utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e recursos de processamento da informação.
A.9.1.2	Controles de entrada física	*Controle* As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.
A.9.1.3	Segurança em escritórios salas e instalações	*Controle* Deve ser projetada e aplicada segurança física para escritórios, salas e instalações.
A.9.1.4	Proteção contra ameaças externas e do meio ambiente	*Controle* Deve ser projetada e aplicada proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.
A.9.1.5	Trabalhando em áreas seguras	*Controle* Deve ser projetada e aplicada proteção física, bem como diretrizes para o trabalho em áreas seguras.
A.9.1.6	Acesso do público, áreas de entrega e de carregamento	*Controle* Pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados dos recursos de processamento da informação, para evitar o acesso não autorizado.
A.9.2 Segurança de equipamentos *Objetivo:* Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.		
A.9.2.1	Instalação e proteção do equipamento	*Controle* Os equipamentos devem ser colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

A.9.2.2	Utilidades	*Controle* Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.
A.9.2.3	Segurança do cabeamento	*Controle* O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação ou danos.
A.9.2.4	Manutenção dos equipamentos	*Controle* Os equipamentos devem ter manutenção correta, para assegurar sua disponibilidade e integridade permanente.
A.9.2.5	Segurança de equipamentos fora das dependências da organização	*Controle* Devem ser tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.
A.9.2.6	Reutilização e alienação segura de equipamentos	*Controle* Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobregravados com segurança.
A.9.2.7	Remoção de propriedade	*Controle* Equipamentos, informações ou *software* não devem ser retirados do local sem autorização prévia.
A.10 Gerenciamento das operações e comunicações		
A.10.1 Procedimentos e responsabilidades operacionais *Objetivo:* Garantir a operação segura e correta dos recursos de processamento da informação.		
A.10.1.1	Documentação dos procedimentos de operação	*Controle* Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.
A.10.1.2	Gestão de mudanças	*Controle* Modificações nos recursos de processamento da informação e sistemas devem ser controladas.
A.10.1.3	Segregação de funções	*Controle* Funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.
A.10.1.4	Separação dos recursos de desenvolvimento, teste e de produção	*Controle* Recursos de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

A.10.2 Gerenciamento de serviços terceirizados		
Objetivo: Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.		
A.10.2.1	Entrega de serviços	*Controle* Deve ser garantido que os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro.
A.10.2.2	Monitoramento e análise crítica de serviços terceirizados	*Controle* Os serviços, relatórios e registros fornecidos por terceiro devem ser regularmente monitorados e analisados criticamente, e auditorias devem ser executadas regularmente.
A.10.2.3	Gerenciamento de mudanças para serviços terceirizados	*Controle* Mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, dos procedimentos e controles existentes, devem ser gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócio envolvidos e a reanálise/reavaliação de riscos.
A.10.3 Planejamento e aceitação dos sistemas		
Objetivo: Minimizar o risco de falhas nos sistemas.		
A.10.3.1	Gestão de capacidade	*Controle* A utilização dos recursos deve ser monitorada e sincronizada e as projeções devem ser feitas para necessidades de capacidade futura, para garantir o desempenho requerido do sistema.
A.10.3.2	Aceitação de sistemas	*Controle* Devem ser estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões e que sejam efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação.
A.10.4 Proteção contra códigos maliciosos e códigos móveis		
Objetivo: Proteger a integridade do *software* e da informação.		
A.10.4.1	Controle contra códigos maliciosos	*Controle* Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.
A.10.4.2	Controles contra códigos móveis	*Controle* Onde o uso de códigos móveis é autorizado, a configuração deve garantir que o código móvel autorizado opere de acordo com uma política de segurança da informação claramente definida e que códigos móveis não autorizados tenham sua execução impedida.

A.10.5 Cópias de segurança		
Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.		
A.10.5.1	Cópias de segurança das informações	*Controle* Cópias de segurança das informações e dos *softwares* devem ser efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança definida.
A.10.6 Gerenciamento da segurança em redes		
Objetivo: Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte.		
A.10.6.1	Controles de redes	*Controle* Redes devem ser adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito.
A.10.6.2	Segurança dos serviços de rede	*Controle* Características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.
A.10.7 Manuseio de mídias		
Objetivo: Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos e interrupções das atividades do negócio.		
A.10.7.1	Gerenciamento de mídias removíveis	*Controle* Devem existir procedimentos implementados para o gerenciamento de mídias removíveis.
A.10.7.2	Descarte de mídias	*Controle* As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.
A.10.7.3	Procedimentos para tratamento de informação	*Controle* Devem ser estabelecidos procedimentos para o tratamento e o armazenamento de informações, para proteger tais informações contra a divulgação não autorizada ou uso indevido.
A.10.7.4	Segurança da documentação dos sistemas	*Controle* A documentação dos sistemas deve ser protegida contra acessos não autorizados.
A.10.8 Troca de informações		
Objetivo: Manter a segurança na troca de informações e *softwares* internamente à organização e com quaisquer entidades externas.		
A.10.8.1	Políticas e procedimentos para troca de informações	*Controle* Políticas, procedimentos e controles devem ser estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação.

A.10.8.2	Acordos para a troca de informações	*Controle* Devem ser estabelecidos acordos para a troca de informações e *softwares* entre a organização e entidades externas.
A.10.8.3	Mídias em trânsito	*Controle* Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externo aos limites físicos da organização.
A.10.8.4	Mensagens eletrônicas	*Controle* As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas.
A.10.8.5	Sistemas de informações do negócio	*Controle* Políticas e procedimentos devem ser desenvolvidos e implementados para proteger as informações associadas com a interconexão de sistemas de informações do negócio.
A.10.9 Serviços de comércio eletrônico *Objetivo:* Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.		
A.10.9.1	Comércio eletrônico	*Controle* As informações envolvidas em comércio eletrônico transitando sobre redes públicas devem ser protegidas de atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas.
A.10.9.2	Transações *on-line*	*Controle* Informações envolvidas em transações *on-line* devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.
A.10.9.3	Informações publicamente disponíveis	*Controle* A integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida, para prevenir modificações não autorizadas.
A.10.10 Monitoramento *Objetivo:* Detectar atividades não autorizadas de processamento da informação.		
A.10.10.1	Registros de auditoria	*Controle* Registros (*log*) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.
A.10.10.2	Monitoramento do uso do sistema	*Controle* Devem ser estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento devem ser analisados criticamente, de forma regular.

A.10.10.3	Proteção das informações dos registros (*logs*)	*Controle* Os recursos e informações de registros (*log*) devem ser protegidos contra falsificação e acesso não autorizado.
A.10.10.4	Registros (*log*) de administrador e operador	*Controle* As atividades dos administradores e operadores do sistema devem ser registradas.
A.10.10.5	Registros (*logs*) de falhas	*Controle* As falhas ocorridas devem ser registradas e analisadas, e devem ser adotadas as ações apropriadas.
A.10.10.6	Sincronização dos relógios	*Controle* Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados de acordo com uma hora oficial.
A.11 Controle de acessos		
A.11.1 Requisitos de negócio para controle de acesso *Objetivo:* Controlar o acesso à informação.		
A.11.1.1	Política de controle de acesso	*Controle* A política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e da segurança da informação.
A.11.2 Gerenciamento de acesso do usuário *Objetivo:* Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.		
A.11.2.1	Registro de usuário	*Controle* Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.
A.11.2.2	Gerenciamento de privilégios	*Controle* A concessão e o uso de privilégios devem ser restritos e controlados.
A.11.2.3	Gerenciamento de senha do usuário	*Controle* A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal.
A.11.2.4	Análise crítica dos direitos de acesso de usuário	*Controle* O gestor deve conduzir a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal.

A.11.3 Responsabilidades dos usuários		
Objetivo: Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.		
A.11.3.1	Uso de senhas	*Controle* Os usuários devem ser orientados a seguir boas práticas de segurança da informação na seleção e uso de senhas.
A.11.3.2	Equipamento de usuário sem monitoração	*Controle* Os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada.
A.11.3.3	Política de mesa limpa e tela limpa	*Controle* Deve ser adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.
A.11.4 Controle de acesso à rede		
Objetivo: Prevenir acesso não autorizado aos serviços de rede.		
A.11.4.1	Política de uso dos serviços de rede	*Controle* Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar.
A.11.4.2	Autenticação para conexão externa do usuário	*Controle* Métodos apropriados de autenticação devem ser usados para controlar o acesso de usuários remotos.
A.11.4.3	Identificação de equipamento em redes	*Controle* Devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.
A.11.4.4	Proteção e configuração de portas de diagnóstico remotas	*Controle* Deve ser controlado o acesso físico e lógico para diagnosticar e configurar portas.
A.11.4.5	Segregação de redes	*Controle* Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.
A.11.4.6	Controle de conexão de rede	*Controle* Para redes compartilhadas, especialmente as que se estendem pelos limites da organização, a capacidade de usuários para conectar-se à rede deve ser restrita, de acordo com a política de controle de acesso e os requisitos das aplicações do negócio (ver 11.1).
A.11.4.7	Controle de roteamento de redes	*Controle* Deve ser implementado controle de roteamento na rede para assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negócio.

A.11.5 Controle de acesso ao sistema operacional		
Objetivo: Prevenir acesso não autorizado aos sistemas operacionais.		
A.11.5.1	Procedimentos seguros de entrada no sistema (*log-on*)	*Controle* O acesso aos sistemas operacionais deve ser controlado por um procedimento seguro de entrada no sistema (*log-on*).
A.11.5.2	Identificação e autenticação de usuário	*Controle* Todos os usuários devem ter um identificador único (ID de usuário), para uso pessoal e exclusivo, e uma técnica adequada de autenticação deve ser escolhida para validar a identidade alegada por um usuário.
A.11.5.3	Sistema de gerenciamento de senha	*Controle* Sistemas para gerenciamento de senhas devem ser interativos e assegurar senhas de qualidade.
A.11.5.4	Uso de utilitários de sistema	*Controle* O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.
A.11.5.5	Desconexão de terminal por inatividade	*Controle* Terminais inativos devem ser desconectados após um período definido de inatividade.
A.11.5.6	Limitação de horário de conexão	*Controle* Restrições nos horários de conexão devem ser utilizadas para proporcionar segurança adicional para aplicações de alto risco.
A.11.6 Controle de acesso à aplicação e à informação		
Objetivo: Prevenir acesso não autorizado à informação contida nos sistemas de aplicação.		
A.11.6.1	Restrição de acesso à informação	*Controle* O acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte deve ser restrito de acordo com o definido na política de controle de acesso.
A.11.6.2	Isolamento de sistemas sensíveis	*Controle* Sistemas sensíveis devem ter um ambiente computacional dedicado (isolado).
A.11.7 Computação móvel e trabalho remoto		
Objetivo: Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.		
A.11.7.1	Computação e comunicação móvel	*Controle* Uma política formal deve ser estabelecida e medidas de segurança apropriadas devem ser adotadas para a proteção contra os riscos do uso de recursos de computação e comunicação móveis.
A.11.7.2	Trabalho remoto	*Controle* Uma política, planos operacionais e procedimentos devem ser desenvolvidos e implementados para atividades de trabalho remoto.

A.12 Aquisição, desenvolvimento e manutenção de sistemas de informação		
A.12.1 Requisitos de segurança de sistemas de informação *Objetivo:* Garantir que segurança é parte integrante de sistemas de informação.		
A.12.1.1	Análise e especificação dos requisitos de segurança	*Controle* Devem ser especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes.
A.12.2 Processamento correto de aplicações *Objetivo:* Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.		
A.12.2.1	Validação dos dados de entrada	*Controle* Os dados de entrada de aplicações devem ser validados para garantir que são corretos e apropriados.
A.12.2.2	Controle do processamento interno	*Controle* Devem ser incorporadas, nas aplicações, checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas.
A.12.2.3	Integridade de mensagens	*Controle* Requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações devem ser identificados e os controles apropriados devem ser identificados e implementados.
A.12.2.4	Validação de dados de saída	*Controle* Os dados de saída das aplicações devem ser validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.
A.12.3 Controles criptográficos *Objetivo:* Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.		
A.12.3.1	Política para o uso de controles criptográficos	*Controle* Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.
A.12.3.2	Gerenciamento de chaves	*Controle* Um processo de gerenciamento de chaves deve ser implantado para apoiar o uso de técnicas criptográficas pela organização.
A.12.4 Segurança dos arquivos do sistema *Objetivo:* Garantir a segurança de arquivos de sistema.		
A.12.4.1	Controle de *software* operacional	*Controle* Procedimentos para controlar a instalação de *software* em sistemas operacionais devem ser implementados.
A.12.4.2	Proteção dos dados para teste de sistema	*Controle* Os dados de teste devem ser selecionados com cuidado, protegidos e controlados.

A.12.4.3	Controle de acesso ao código- fonte de programa	*Controle* O acesso ao código-fonte de programa deve ser restrito.
A.12.5 Segurança em processos de desenvolvimento e de suporte *Objetivo:* Manter a segurança de sistemas aplicativos e da informação.		
A.12.5.1	Procedimentos para controle de mudanças	*Controle* A implementação de mudanças deve ser controlada utilizando procedimentos formais de controle de mudanças.
A.12.5.2	Análise crítica técnica das aplicações após mudanças no sistema operacional	*Controle* Aplicações críticas de negócios devem ser analisadas criticamente e testadas quando sistemas operacionais são mudados, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.
A.12.5.3	Restrições sobre mudanças em pacotes de *software*	*Controle* Modificações em pacotes de *software* não devem ser incentivadas e devem estar limitadas às mudanças necessárias, e todas as mudanças devem ser estritamente controladas.
A.12.5.4	Vazamento de informações	*Controle* Oportunidades para vazamento de informações devem ser prevenidas.
A.12.5.5	Desenvolvimento terceirizado de *software*	*Controle* A organização deve supervisionar e monitorar o desenvolvimento terceirizado de *software*.
A.12.6 Gestão de vulnerabilidades técnicas *Objetivo:* Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.		
A.12.6.1	Controle de vulnerabilidades técnicas	*Controle* Deve ser obtida informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a estas vulnerabilidades e tomadas as medidas apropriadas para lidar com os riscos associados.
A.13 Gestão de incidentes de segurança da informação		
A.13.1 Notificação de fragilidades e eventos de segurança da informação *Objetivo:* Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.		
A.13.1.1	Notificação de eventos de segurança da informação	*Controle* Os eventos de segurança da informação devem ser relatados através dos canais apropriados da direção, o mais rapidamente possível.
A.13.1.2	Notificando fragilidades de segurança da informação	*Controle* Os funcionários, fornecedores e terceiros de sistemas e serviços de informação devem ser instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços.

A.13.2 Gestão de incidentes de segurança da informação e melhorias		
Objetivo: Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.		
A.13.2.1	Responsabilidades e procedimentos	*Controle* Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.
A.13.2.2	Aprendendo com os incidentes de segurança da informação	*Controle* Devem ser estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.
A.13.2.3	Coleta de evidências	*Controle* Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), evidências devem ser coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes.
A.14 Gestão da continuidade do negócio		
***A.14.1* Aspectos da gestão da continuidade do negócio, relativos à segurança da informação**		
Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.		
A.14.1.1	Incluindo segurança da informação no processo de gestão da continuidade de negócio	*Controle* Um processo de gestão deve ser desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.
A.14.1.2	Continuidade de negócios e análise/avaliação de risco	*Controle* Devem ser identificados os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as conseqüências para a segurança de informação.
A.14.1.3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	*Controle* Os planos devem ser desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.
A.14.1.4	Estrutura do plano de continuidade do negócio	*Controle* Uma estrutura básica dos planos de continuidade do negócio deve ser mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.

A.14.1.5	Testes, manutenção e reavaliação dos planos de continuidade do negócio	*Controle* Os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.
A.15 Conformidade		
A.15.1 **Conformidade com requisitos legais** *Objetivo:* Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação		
A.15.1.1	Identificação da legislação vigente	*Controle* Todos os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a estes requisitos devem ser explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação da organização.
A.15.1.2	Direitos de propriedade intelectual	*Controle* Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de *software* proprietários.
A.15.1.3	Proteção de registros organizacionais	*Controle* Registros importantes devem ser protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.
A.15.1.4	Proteção de dados e privacidade da informação pessoal	*Controle* A privacidade e a proteção de dados devem ser asseguradas conforme exigido nas legislações relevantes, regulamentações e, se aplicável, nas cláusulas contratuais.
A.15.1.5	Prevenção de mau uso de recursos de processamento da informação	*Controle* Os usuários devem ser dissuadidos de usar os recursos de processamento da informação para propósitos não autorizados.
A.15.1.6	Regulamentação de controles de criptografia	*Controle* Controles de criptografia devem ser usados em conformidade com leis, acordos e regulamentações relevantes.
A.15.2 **Conformidade com normas e políticas de segurança da informação e conformidade técnica** *Objetivo:* Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.		
A.15.2.1	Conformidade com as políticas e normas de segurança da informação	*Controle* Os gestores devem garantir que todos os procedimentos de segurança dentro da sua área de responsabilidade sejam executados corretamente para atender à conformidade com as normas e políticas de segurança da informação.
A.15.2.2	Verificação da conformidade técnica	*Controle* Os sistemas de informação devem ser periodicamente verificados quanto à sua conformidade com as normas de segurança da informação implementadas.

A.15.3 **Considerações quanto à auditoria de sistemas de informação** *Objetivo:* Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.		
A.15.3.1	Controles de auditoria de sistemas de informação	*Controle* Os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos do negócio.
A.15.3.2	Proteção de ferramentas de auditoria de sistemas de informação	*Controle* O acesso às ferramentas de auditoria de sistema de informação deve ser protegido para prevenir qualquer possibilidade de uso impróprio ou comprometimento.

Anexo B
(informativo)

Princípios da OECD e desta Norma

Os princípios definidos pelas Diretrizes de OECD para a Segurança de Sistemas de Informação e Redes aplicam-se para toda a política e níveis operacionais que governam a segurança de sistemas de informação e redes. Esta Norma provê uma estrutura de um sistema de gestão de segurança da informação para implementar alguns dos princípios da OECD que usam o modelo PDCA e os processos descritos nas seções 4, 5, 6 e 8, como indicado na tabela B.1.

Tabela B.1 — Princípios da OECD e o modelo PDCA

Princípios da OECD	Correspondência entre o processo do ISMS e a fase do PDCA
Conscientização Convém que os participantes estejam conscientes da necessidade de segurança de sistemas de informação e redes e do que eles podem fazer para aumentar a segurança.	Esta atividade é parte da fase 'Fazer' (*Do*) (ver 4.2.2 e 5.2.2).
Responsabilidade Todos os participantes são responsáveis pela segurança de sistemas de informação e redes.	Esta atividade é parte da fase 'Fazer' (*Do*) (ver 4.2.2 e 5.1).
Resposta Convém que os participantes ajam de modo oportuno e cooperativo para prevenir, detectar e responder a incidentes de segurança da informação.	Esta é, em parte, uma atividade de monitoração da fase 'Checar' (*Check*) (ver 4.2.3 e 6 a 7.3) e uma atividade de resposta da fase 'Agir' (*Act*) (ver 4.2.4 e 8.1 a 8.3). Isto também pode ser coberto por alguns aspectos das fases 'Planejar' (*Plan*) e 'Checar' (*Check*).
Análise/Avaliação de riscos Convém que os participantes conduzam análises/avaliações de risco.	Esta atividade é parte da fase 'Planejar' (*Plan*) (ver 4.2.1) e a reanálise/reavaliação dos riscos é parte da fase 'Checar' (*Check*) (ver 4.2.3 e 6 até 7.3).
Arquitetura e implementação de segurança Convém que os participantes incorporem a segurança como um elemento essencial de sistemas de informação e redes.	Uma vez finalizada a análise/avaliação de riscos, os controles são selecionados para o tratamento dos riscos como parte da fase 'Planejar' (*Plan*) (ver 4.2.1). A fase 'Fazer' (*Do*) (ver 4.2.2 e 5.2) então cobre a implementação e o uso operacional destes controles.
Gestão de segurança Convém que os participantes adotem uma abordagem detalhada para a gestão da segurança.	A gestão de riscos é um processo que inclui a prevenção, detecção e resposta a incidentes, atuação, manutenção, análise crítica e auditoria. Todos estes aspectos são cercados nas fases 'Planejar' (*Plan*), 'Fazer' (*Do*), 'Checar' (*Check*) e 'Agir' (*Act*).
Reavaliação Convém que os participantes analisem criticamente e reavaliem a segurança dos sistemas de informação e redes, e façam as modificações apropriadas nas políticas de segurança, práticas, medidas e procedimentos.	A reanálise/revaliação de segurança da informação é uma parte da fase 'Checar' (*Check*) (ver 4.2.3 e 6 até 7.3), onde análises críticas regulares devem ser realizadas para verificar a eficácia do sistema de gestão de segurança da informação, e a melhoria da segurança é parte da fase 'Agir' (*Act*) (ver 4.2.4 e 8.1 a 8.3).

Anexo C
(informativo)

Correspondência entre a ABNT NBR ISO 9001:2000, a ABNT NBR ISO 14001:2004 e esta Norma

A tabela C.1 mostra a correspondência entre a ABNT NBR ISO 9001:2000, a ABNT NBR ISO 14001:2004 e esta Norma.

Tabela C.1 — Correspondência entre a ABNT NBR ISO 9001:2000, a ABNT NBR ISO 14001:2004 e esta Norma

Esta Norma	ABNT NBR ISO 9001:2000	ABNT NBR ISO 14001:2004
0 Introdução	**0 Introdução**	**Introdução**
0.1 Geral	0.1 Geral	
0.2 Abordagem de processo	0.2 Estratégia do processo	
	0.3 Relação com ABNT NBR ISO 9004	
0.3 Compatibilidade com outros sistemas de gestão	0.4 Compatibilidade com outros sistemas de gestão	
1 Objetivo	**1 Objetivo**	**2 Objetivo**
1.1 Geral	1.1 Generalidades	
1.2 Aplicação	1.2 Aplicação	
2 Referências normativas	**2 Referência normativa**	**2 Referências normativas**
3 Termos e definições	**3 Termos e definições**	**3 Termos e definições**
4 Sistema de gestão de segurança da informação	**4 Sistema de gestão da qualidade**	**4 Requisitos do SGA**
4.1 Requisitos gerais	4.1 Requisitos gerais	4.1 Requisitos gerais
4.2 Estabelecendo e gerenciando o SGSI		
4.2.1 Estabelecer o SGSI		
4.2.2 Implementar e operar o SGSI		4.4 Implementação e operação
4.2.3 Monitorar e analisar criticamente o SGSI	8.2.3 Medição e monitoramento de processos	4.5.1 Monitoramento e medição
	8.2.4 Medição e monitoramento de produtos	
4.2.4 Manter e melhorar o SGSI		

Esta Norma	ABNT NBR ISO 9001:2000	ABNT NBR ISO 14001:2004
4.3 Requisitos de documentação	4.3 Requisitos de documentação	
4.3.1 Geral	4.3.1 Geral	
	4.3.2 Manual da qualidade	
4.3.2 Controle de documentos	4.3.3 Controle de documentos	4.4.5 Controle de documentos
4.3.3 Controle de registros	4.3.4 Controle de registros	4.5.4 Controle de registros
5 Responsabilidades da direção	**5 Responsabilidades de gestão**	
5.1 Comprometimento da direção	5.1 Comprometimento da direção	
	5.2 Foco no cliente	
	5.3 Política da qualidade	4.2 Política ambiental
	5.4 Planejamento	4.3 Planejamento
	5.5 Responsabilidade, autoridade e comunicação	
5.2 Gestão de recursos	**6 Gestão de recursos**	
5.2.1 Provisão de recursos	6.1 Provisão de recursos	
	6.2 Recursos humanos	
5.2.2 Treinamento, conscientização e competência	6.2.2 Competência, conscientização e treinamento	4.2.2 Competência,treinamento e conscientização
	6.3 Infraestrutura	
	6.4 Ambiente de trabalho	
6 Auditorias internas do SGSI	8.2.2 Auditorias internas	4.5.5 Auditorias internas
7 Análise crítica do SGSI pela direção	**5.6 Análise crítica pela direção**	**4.6 Análise pela administração**
7.1 Geral	5.6.1 Generalidades	
7.2 Entradas para a análise crítica	5.6.2 Entradas para a análise crítica	
7.3 Saídas da análise crítica	5.6.3 Saídas para análise crítica	
8 Melhoria do SGSI	**8.5 Melhorias**	
8.1 Melhoria contínua	8.5.1 Melhoria contínua	
8.2 Ações corretivas	8.5.3 Ações corretivas	4.5.3 Não-conformidades, ação corretiva e ação preventiva
8.3 Ações preventivas	8.5.3 Ações preventivas	
Anexo A - Objetivos de controle e controles		**Anexo A - Guia para o uso desta Norma**
Anexo B - Princípios da OECD e esta Norma		
Anexo C - Correspondência entre a ABNT NBR ISO 9001:2000, a ABNT NBR ISO 14001:2004 e esta Norma	**Anexo A - Correspondência entre a ABNT NBR ISO 9001:2000 e a ABNT NBR ISO 14001:2004**	**Anexo B - Correspondência entre ABNT NBR ISO 14001:2004 e ABNT NBR ISO 9001:2000**

Bibliografia

Normas publicadas

[1] ABNT NBR ISO 9001:2000, Sistemas de gestão da qualidade - Requisitos

[2] ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[3] ISO/IEC TR 13335-3:1998, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security*

[4] ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards

[5] ABNT NBR ISO 14001:2004, Sistemas da gestão ambiental - Requisitos com orientações para uso

[6] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management*

[7] ABNT NBR ISO 19011:2002, Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental

[8] ABNT ISO/IEC Guia 62:1997, Requisitos gerais para organismos que operam avaliação e certificação/registro de sistemas da qualidade

[9] ABNT ISO/IEC Guia 73:2005, Gestão de riscos - Vocabulário - Recomendações para uso em normas

Outras Publicações

[1] OECD, Guidelines for the Security of Information Systems and Networks — Towards a Culture of

Security. Paris: OECD, July 2002. www.oecd.org

[2] NIST SP 800-30, Risk Management Guide for Information Technology Systems

[3] Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986