NORMA
BRASILEIRA

ABNT NBR ISO/IEC 27014

Primeira edição
25.06.2013

Válida a partir de
25.07.2013

Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação

Information technology — Security techniques — Governance of information security

ICS 35.040

ISBN 978-85-07-04333-1

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO/IEC 27014:2013
12 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

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 por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Os Documentos Técnicos ABNT são elaborados conforme as regras da Diretiva ABNT, Parte 2.

A Associação Brasileira de Normas Técnicas (ABNT) chama atenção para a possibilidade de que alguns dos elementos deste documento podem ser objeto de direito de patente. A ABNT não deve ser considerada responsável pela identificação de quaisquer direitos de patentes.

A ABNT NBR ISO/IEC 27014 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança da Informação (CE-21:027.00). O Projeto circulou em Consulta Nacional conforme Edital nº 01, de 08.01.2013 a 13.02.2013, com o número de Projeto 21:027.00-027.

Esta Norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO IEC 27014:2013, que foi elaborada pelo *Joint Technical Committee Information Technology* (ISO/IEC JTC 1), *Subcommittee IT Security techniques* (SC 27) em colaboração com a ITU-T, conforme ISO/IEC Guide 21-1:2005.

O Escopo desta Norma Brasileira em inglês é o seguinte:

Scope

This Recommendation | International Standard provides guidance on concepts and principles for the governance of information security, by which organisations can evaluate, direct, monitor and communicate the information security related activities within the organisation.

This International Standard is applicable to all types and sizes of organisations.

Introdução

Esta Recomendação | Norma fornece orientações sobre a governança de segurança da informação.

A segurança da informação tornou-se uma questão-chave para as organizações. Não somente os requisitos regulamentares estão aumentando, mas também as falhas nas medidas de segurança da informação de uma organização podem ter um impacto direto na reputação da organização.

Portanto é altamente recomendado que o corpo diretivo, como parte de suas responsabilidades de governança, supervisione, cada vez mais, a segurança da informação para garantir que os objetivos da organização sejam alcançados.

Além disso, a governança de segurança da informação provê uma forte ligação entre o corpo diretivo de uma organização, a gerência executiva e os responsáveis pela implementação e operação de um sistema de gestão de segurança da informação.

Ela fornece a ordem essencial para direcionar as iniciativas de segurança da informação por toda a organização.

Ademais, uma governança de segurança da informação eficaz garante que o corpo diretivo receba informação relevante – dentro de um contexto de negócios – sobre as atividades relacionadas com a segurança da informação. Isso permite decisões pertinentes e oportunas sobre as questões de segurança da informação em apoio aos objetivos estratégicos da organização

Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação

1 Escopo

Esta recomendação I Norma fornece orientação sobre conceitos e princípios para a governança de segurança da informação, pela qual as organizações podem avaliar, dirigir, monitorar e comunicar as atividades relacionadas com a segurança da informação dentro da organização.

Esta Norma é aplicável a todos os tipos e tamanhos de organizações

2 Referências normativas

O documento relacionado a seguir é indispensável à aplicação deste 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 27000:2009, *Information Technology – Security Techniques – Information security management systems – Overview and vocabulary*

3 Termos e definições

Para os efeitos deste documento, aplicam-se os termos e definições da ISO/IEC 27000:2009 e os seguintes.

3.1
gerência executiva
pessoa ou grupo de pessoas que possuem responsabilidade delegada pelo corpo diretivo para a implementação de estratégias e políticas para alcançar o propósito da organização

NOTA 1 A gerência executiva faz parte da alta administração: Para maior clareza de papéis, esta Norma distingue dois grupos no âmbito da alta administração: o corpo diretivo e os gerentes executivos.

NOTA 2 A gerência executiva pode incluir Diretores Executivos (CEO), Chefes de Organizações Governamentais, Diretores Financeiros (CFOs), Diretores de Operações (COO), Diretores de Tecnologia da Informação (CIOs), Diretores de Segurança da Informação (CISOs) e funções semelhantes.

3.2
corpo diretivo
pessoa ou grupo de pessoas, que são responsáveis pelo desempenho e conformidade da organização

NOTA O corpo diretivo faz parte da alta administração: Para maior clareza de papéis, esta Norma distingue dois grupos no âmbito da alta administração: o corpo diretivo e a gerência executiva.

3.3
governança de segurança da informação
sistema pelo qual as atividades de segurança da informação de uma organização são dirigidas e controladas

3.4
parte interessada
qualquer pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma atividade da organização.

NOTA Um tomador de decisão pode ser uma parte interessada.

4 Conceitos

4.1 Geral

A governança de segurança da informação necessita alinhar os objetivos e estratégias de segurança da informação com os objetivos e estratégias do negócio e requer a conformidade com leis, regulamentos e contratos. Convém que seja avaliada, analisada e implementada por meio de uma abordagem de gestão de riscos, apoiada por um sistema de controles internos.

O corpo diretivo é o maior responsável pelas decisões de uma organização e pelo seu desempenho. Em relação à segurança da informação, o foco principal do corpo diretivo é garantir que a abordagem da organização para a segurança da informação seja eficiente, eficaz, aceitável e alinhada com os objetivos e estratégias de negócios, dando devida consideração às expectativas das partes interessadas. Diversas partes interessadas podem ter diferentes valores e necessidades.

4.2 Objetivos

Os objetivos da governança da segurança da informação são para:

- alinhar os objetivos e estratégia da segurança da informação com os objetivos e estratégia do negócio (alinhamento estratégico)
- agregar valor para o corpo diretivo e para as partes interessadas (entrega de valor)
- garantir que os riscos da informação estão sendo adequadamente endereçados (responsabilidade)

4.3 Resultados Desejados

Os resultados desejados a partir da implementação eficaz da governança da segurança da informação incluem:

- visibilidade do corpo diretivo sobre a situação da segurança da informação
- uma abordagem ágil para a tomada de decisões sobre os riscos da informação
- investimentos eficientes e eficazes em segurança da informação
- conformidade com requisitos externos (legais, regulamentares ou contratuais)

4.4 Relacionamento

Existem várias outros modelos de áreas de governança em uma organização, como a governança da tecnologia da informação e governança organizacional. Cada modelo de governança é um componente integrante da governança de uma organização, que enfatiza a importância do alinhamento com os objetivos de negócios. Geralmente, é vantajoso para o corpo diretivo desenvolver uma visão holística e integrada de seu modelo de governança, na qual convém que a governança da segurança da informação seja uma parte. Os escopos de modelos de governança às vezes se sobrepõem. Por exemplo, a relação entre governança da segurança da informação e governança de tecnologia da informação está ilustrada na Figura 1.

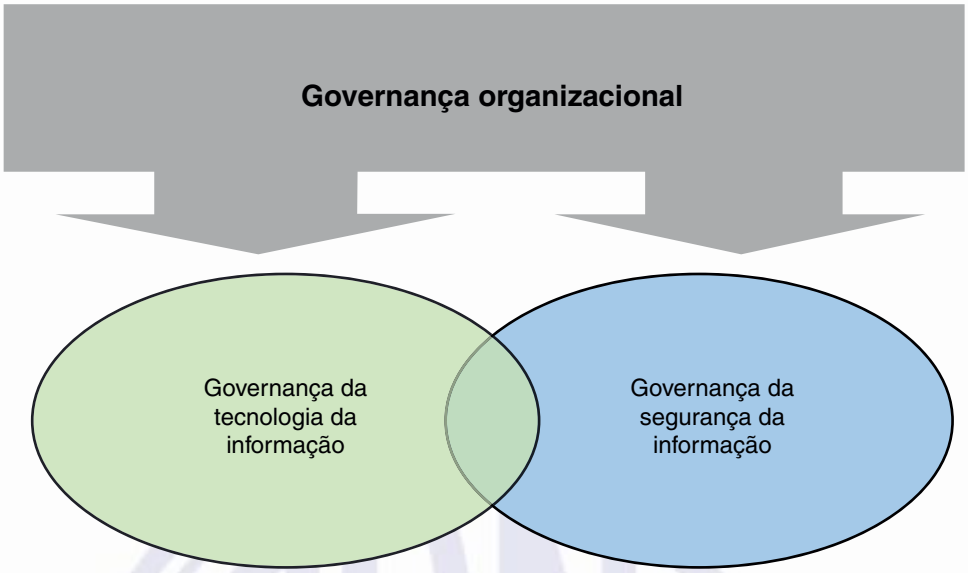

Figura 1 – Relação entre governança de segurança da informação e governança de tecnologia da informação

Enquanto o escopo abrangente da governança de tecnologia da informação visa recursos necessários para adquirir, processar, armazenar e disseminar a informação, o escopo da governança da segurança da informação abrange a confidencialidade, integridade e disponibilidade da informação. Ambos os esquemas de governança precisam ser tratados pelos seguintes processos de governança: ADM (Avaliação, Direção e Monitoração). Entretanto, a governança da segurança da informação requer também o processo interno de “comunicação”.

As tarefas requeridas do corpo diretivo para estabelecer a governança da segurança da informação são descritas na Seção 5. Tarefas de governança também estão relacionadas com os requisitos especificados na ABNT NBR ISO/IEC 27001, bem como com as outras normas da família SGSI, como referenciado na Bibliografia.

5 Princípios e processos

5.1 Visão Geral

Esta seção descreve os princípios e processos que, juntos, formam a governança da segurança da informação. Princípios de governança da segurança da informação são regras aceitas para a ação ou conduta de governança que atuam como um guia para a implementação de governança. Um processo de governança para a segurança da informação descreve uma série de tarefas que viabilizam a governança da segurança da informação e suas interrelações. Também mostra a relação entre governança e gestão da segurança da informação. Estes dois componentes são explicados nas seguintes subseções.

5.2 Princípios

Atender às necessidades das partes interessadas e entregar valor para cada uma é fundamental para o sucesso da segurança da informação em longo prazo. Para alcançar o objetivo da governança em alinhar rigorosamente segurança da informação com os objetivos do negócio e entregar valor às partes interessadas, esta subseção estabelece seis princípios orientados para ação.

Os princípios fornecem uma base sólida para a implementação de processos de governança para a segurança da informação. A declaração de cada princípio faz referência ao que convém que aconteça mas não prescreve como, quando, nem por quem os princípios seriam implementados, porque estes aspectos dependem da natureza da organização que implementará os princípios. Convém ao corpo diretivo exigir que esses princípios sejam aplicados e designar alguém com responsabilidade, responsabilização e autoridade para implementá-las.

Princípio 1: Estabelecer a segurança da informação em toda a organização

Convém a governança da segurança da informação garantir que as atividades de segurança da informação sejam entendidas e integradas. Convém que a segurança da informação seja tratada em um nível organizacional, com a tomada de decisões que leve em consideração o negócio, a segurança da informação e todos os outros aspectos relevantes. Convém que atividades relativas à segurança física e lógica sejam rigorosamente coordenadas.

Para estabelecer a segurança em toda a organização, convém que a responsabilidade e a responsabilização da segurança da informação seja estabelecida em cada porção das atividades de uma organização. Isto normalmente ultrapassa as “fronteiras” geralmente percebidas da organização, por exemplo, com informações que estão sendo armazenadas ou transferidas por terceiros.

Princípio 2: Adotar uma abordagem baseada em riscos

Convém que a governança da segurança da informação seja fundamentada em decisões baseadas nos riscos. Convém que a definição “de quanto” de segurança é aceitável seja baseado no apetite ao risco da organização, incluindo a perda da vantagem competitiva, conformidade e riscos de responsabilidade civil, interrupções operacionais, danos à reputação e perdas financeiras.

Para adotar uma gestão de riscos da informação adequada para a organização, convém que esta esteja consistente e integrada à abordagem global de gestão de riscos da organização. Convém que os níveis aceitáveis de segurança da informação sejam definidos com base no apetite ao risco da organização, incluindo a perda da vantagem competitiva, conformidade e riscos de responsabilidade civil, interrupções operacionais, danos à reputação e perdas financeiras. Convém que os recursos apropriados para a implementação da gestão de riscos da informação sejam alocados pelo corpo diretivo.

Princípio 3: Estabelecer a direção de decisões de investimento

Convém à governança da segurança da informação estabelecer uma estratégia de investimento em segurança da informação com base em resultados de negócios alcançados, resultando na harmonização entre os requisitos de negócio e os da segurança da informação, tanto em curto como em longo prazo, visando atender às necessidades atuais e crescentes das partes interessadas.

Para otimizar os investimentos em segurança da informação no apoio aos objetivos da organização, convém ao corpo diretivo assegurar que a segurança da informação seja integrada com os atuais processos da organização para gastos com capital e operação (investimentos e despesas), conformidade legal e regulatória, para reporte de riscos.

Princípio 4: Assegurar conformidade com os requisitos internos e externos

Convém à governança da segurança da informação garantir que as políticas e práticas de segurança da informação atendam à legislação e regulamentações pertinentes obrigatórias, assim como aos requisitos de negócio ou contratuais e aos outros requisitos externos ou internos.

Para endereçar as questões de conformidade e cumprimento, convém ao corpo diretivo obter a garantia de que as atividades de segurança da informação estejam satisfatoriamente cumprindo os requisitos internos e externos autorizando encomendando/autorizando auditorias de segurança independentes.

Princípio 5: Promover um ambiente positivo de segurança

Convém que a governança da segurança da informação seja construída sobre o comportamento humano, incluindo as crescentes necessidades de todas as partes interessadas, visto que o comportamento humano é um dos elementos fundamentais para manter o nível apropriado de segurança da informação. Caso não estejam adequadamente coordenados, os objetivos, papéis, responsabilidades e recursos podem entrar em conflito uns com os outros, resultando em falhas para o cumprimento dos objetivos de negócio. Por isso, a harmonização e a orientação orquestradas entre as diversas partes interessadas são muito importantes.

Para estabelecer uma cultura positiva de segurança da informação, convém que o corpo diretivo exija, promova e apoie a coordenação das atividades das partes interessadas para alcançar uma direção coerente para a segurança da informação. Isto viabilizará a implantação de programas de educação, treinamento e conscientização em segurança.

Princípio 6: Analisar criticamente o desempenho em relação aos resultados de negócios

Convém que a governança da segurança da informação garanta que a abordagem adotada para proteger a informação esteja adequada à sua finalidade de apoio à organização, proporcionando níveis acordados de segurança da informação. Convém que o desempenho da segurança seja mantido nos níveis necessários para atender aos requisitos de negócio atuais e futuros.

Para analisar criticamente o desempenho de segurança da informação a partir de uma perspectiva da governança, convém que o corpo diretivo avalie o desempenho da segurança da informação em relação ao seu impacto no negócio, e não apenas a eficácia e eficiência dos controles de segurança. Isto pode ser feito realizando-se análises críticas agendadas de um programa de medição de desempenho para monitoramento, auditoria e melhoria, e, assim, associando o desempenho da segurança da informação com o desempenho do negócio.

5.3 Processos

5.3.1 Visão geral

O corpo diretivo executa os processos de “avaliação”, “direção”, “monitoração” e “comunicação” para governar a segurança da informação. Além disso, o processo de “garantia” fornece um parecer independente e objetivo em relação a governança da segurança da informação e do nível atingido. A Figura 2 mostra a relação entre estes processos.

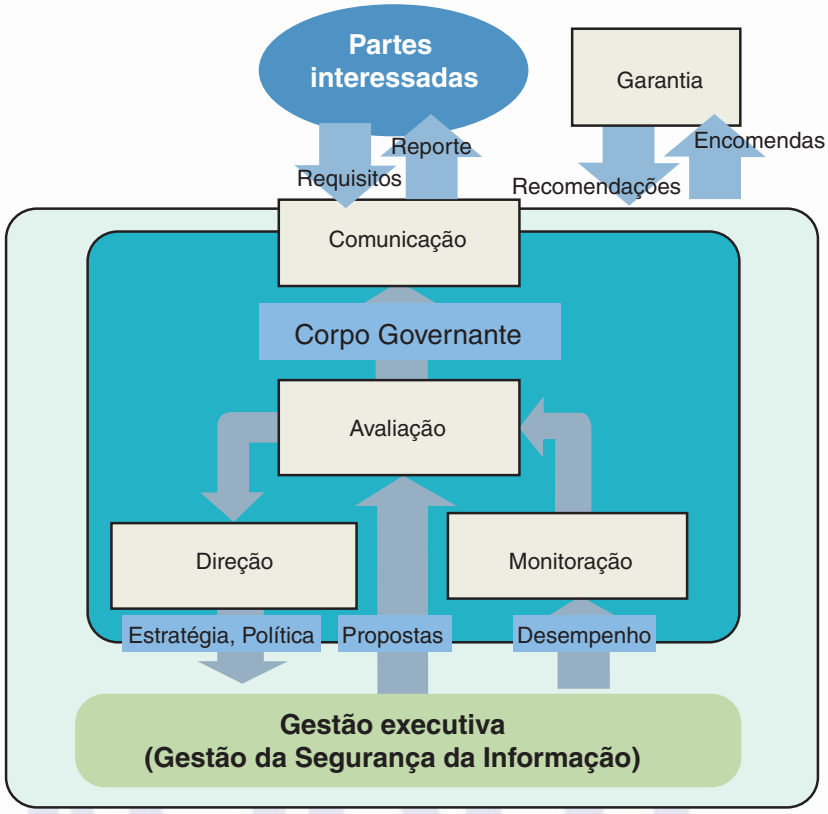

Figura 2 – Implementação do modelo de governança para a segurança da informação

5.3.2 Avaliação

"Avaliação" é o processo de governança que considera o atingimento atual e previsto dos objetivos de segurança com base nos processos atuais e nas mudanças planejadas e determina onde eventuais ajustes são necessários para otimizar o atingimento dos objetivos estratégicos no futuro.

Para realizar o processo de "avaliação", convém ao corpo diretivo:

- assegurar que as iniciativas de negócio levem em consideração questões da segurança da informação,
- responder aos resultados de desempenho da segurança da informação, priorizar e iniciar ações necessárias.

Para viabilizar o processo de "avaliação", convém à gerência executiva:

- garantir que a segurança da informação suporte devidamente e sustente os objetivos de negócios,
- submeter novos projetos de segurança da informação com impacto significativo para o corpo diretivo.

5.3.3 Direção

"Direção" é o processo de governança pelo qual o corpo diretivo fornece o direcionamento sobre os objetivos e estratégia da segurança da informação que precisam ser implementados. Direcionamento pode incluir alterações nos níveis de recursos, alocação de recursos, priorização de atividades e aprovações de políticas, aceitação de riscos materiais e planos de gestão de riscos.

Para realizar o processo de “direção”, convém ao corpo diretivo:

- determinar o apetite ao risco da organização,
- aprovar a estratégia e política de segurança da informação,
- alocar investimentos e recursos adequados.

Para viabilizar o processo de “direção”, convém à gerência executiva:

- desenvolver e implementar a estratégia e política de segurança da informação,
- alinhar os objetivos de segurança da informação com os objetivos de negócio,
- promover uma cultura positiva de segurança da informação.

5.3.4 Monitoração

“Monitoração” é o processo de governança que permite ao corpo diretivo avaliar o atingimento de objetivos estratégicos.

Para realizar o processo de “monitoração”, convém ao corpo diretivo:

- avaliar a eficácia das atividades de gerenciamento de segurança da informação ,
- assegurar a conformidade com os requisitos internos e externos,
- considerar alterações no ambiente de negócio, legal e regulatório, e seu potencial impacto sobre o risco de informação.

Para viabilizar o processo de “monitoração”, convém a gerência executiva:

- selecionar as métricas de desempenho apropriadas a partir de uma perspectiva de negócio,
- fornecer *feedback* sobre os resultados do desempenho da segurança da informação para o corpo diretivo, incluindo o desempenho das ações previamente identificadas pelo corpo diretivo e seus impactos sobre a organização,
- alertar o corpo diretivo sobre novos desenvolvimentos que afetam os riscos de informação e segurança da informação.

5.3.5 Comunicação

“Comunicação” é o processo de governança bidirecional, pelo qual o corpo diretivo e as partes interessadas trocam informações sobre a segurança da informação, adequadas às suas necessidades específicas.

Um dos métodos para “comunicação” é o status da segurança da informação, que explica as atividades da segurança de informação e questões para as partes interessadas, cujos exemplos são mostrados nos anexos A e B.

Para executar o processo de “comunicação”, convém ao corpo diretivo:

- comunicar às partes interessadas externas que a organização pratica um nível de segurança da informação compatível com a natureza do seu negócio,
- notificar à gerência executiva dos resultados de avaliações externas que identificaram questões de segurança da informação e solicitar ações corretivas,

- reconhecer as obrigações regulatórias, as expectativas das partes interessadas e as necessidades de negócio com relação à segurança da informação.

Para viabilizar o processo de “comunicação”, convém à gerência executiva:

- aconselhar o corpo diretivo de quaisquer assuntos que requeiram a sua atenção e, eventualmente, alguma decisão,

- instruir as partes interessadas sobre as ações detalhadas a serem tomadas para apoiar os direcionamentos e decisões do corpo diretivo.

5.3.6 Garantia

“Garantia” é o processo de governança pelo qual o corpo diretivo encomenda/autoriza auditorias, análises críticas ou certificações independentes e objetivas. Estas irão identificar e validar os objetivos e ações relacionadas com a execução de atividades de governança e condução de operações para atingir o nível desejado de segurança da informação.

Para executar o processo de “garantia”, convém ao corpo diretivo:

- encomendar pareceres independentes e objetivos sobre quanto se está cumprindo com a sua responsabilidade para o nível desejado de segurança da informação.

Para viabilizar o processo de “garantia”, convém à gerência executiva:

- apoiar a auditoria, análises críticas ou certificações encomendadas pelo corpo diretivo.

Anexo A
(informativo)

Um exemplo de status de segurança da informação

Uma organização pode elaborar um status de segurança da informação e divulgá-lo para as partes interessadas como uma ferramenta de comunicação em segurança da informação.

Convém que a organização selecione e decida o formato e o conteúdo do status de segurança da informação. O Anexo A é um exemplo que usa um relatório de auditoria de segurança da informação para declaração de satisfação.

Tabela A.1 – Um status de segurança da informação

A Administração está convencida de que para o período compreendido entre **mmm** até **nnn**, os controles e procedimentos de segurança da informação, que estão baseados nos critérios definidos em **xyz** (por exemplo, da série ABNT NBR ISO/IEC 27000, CobiT), relacionados com os procedimentos e sistemas operacionais da organização suplementados por controles de gestão de alto nível estavam operando com eficácia suficiente para fornecer garantia razoável de que foram atendidos os objetivos de controle de segurança da informação definidos para a confidencialidade, integridade e disponibilidade. A Administração forneceu à **ABC**, como auditores externos de segurança da informação, uma carta de representação para este efeito. **ABC** foi nomeada pelo conselho de administração para examinar a declaração da gestão sobre os controles de segurança da informação. Seu exame foi feito de acordo com os padrões estabelecidos e incluiu a avaliação da eficácia do desenho e operação dos controles da segurança de informação e procedimentos através de amostragem. Neste sentido, a **ABC** emitiu um parecer para a gestão que os resultados de seus testes indicam que, com exceções específicas, com base nos critérios de gestão identificados de **xyz** (por exemplo, da série ABNT NBR ISO/IEC 27000, CobiT), os controles apresentaram-se eficazes em seus aspectos relevantes. A Carta de Concordância completa da administração e o relatório de auditoria externa, com as exceções identificadas em relação aos controles de segurança da informação, foram discutidos com o comitê de auditoria e fornecidos a todos os membros do conselho. As cópias estão disponíveis aos acionistas, mediante solicitação.

NOTA “nnn”, “mmm”, “xyz” e “ABC” são espaços reservados. Datas específicas e nomes devem aparecer em declarações reais.

Anexo B
(informativo)

Um exemplo de status de segurança da informação detalhado

O Anexo B é um exemplo de status de segurança da informação divulgando conteúdos detalhados. É particularmente útil para as organizações que esperam melhorar a sua reputação, enfatizando a sua segurança, por exemplo, empresas de TIC (Tecnologia, Informação e Comunicação). A transparência da abordagem da organização para o seu risco de segurança e divulgação adequada também é eficaz para aumentar a confiança. A conscientização comum pode ser compartilhada entre as partes interessadas através dessas atividades.

Tabela B.1 – Um status da segurança da informação detalhado

Introdução
• **Escopo** (estratégia, políticas, normas), **perímetro** (unidades geográficas/organizacionais), **período abrangido** (mês/trimestre/semestre/ano)
Status geral
• **Satisfatório/Ainda não satisfatório/Insatisfatório**
Atualizações (conforme apropriado e relevante)
• **Progressos visando atingir a estratégia de segurança da informação** Elementos concluídos/em andamento/planejados
• **Alterações no sistema de gestão de segurança da informação** Revisão da política do SGSI, estrutura organizacional para implementação do SGSI (incluindo a atribuição de responsabilidades)
• **Progressos no sentido da Certificação** SGSI (re)certificação, certificado de auditorias de segurança da informação
• **Orçamento / pessoal / treinamento** Situação financeira, adequação de número de funcionários, qualificações de segurança da informação
• **Outras atividades de segurança da informação** Envolvimento com a gestão de continuidade de negócios, campanhas de conscientização, auxílio de auditoria interna / externa
Questões significativas (se houver)
• **Resultados de análises críticas de segurança da informação** Recomendações, respostas da gestão, planos de ação, prazos

- **Progresso em relação aos principais relatórios internos/externos de auditoria**

  Recomendações, respostas da gestão, planos de ação, prazos

- **Incidentes de segurança da informação**

  Impacto estimado, planos de ação, prazos

- **(Não) Conformidade com a legislação e regulamentos**

  Impacto estimado, planos de ação, prazos

Decisão(ões) necessária(s) (se houver)

- **Recursos adicionais**

  Para permitir que a segurança da informação apoie iniciativa(s) de negócio

Bibliografia

[1] ABNT NBR ISO/IEC 27001:2005, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos*

[2] ABNT NBR ISO/IEC 27002:2005, *Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação*

[3] ABNT NBR ISO/IEC 27005:2011, *Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação*

[4] ABNT NBR ISO/IEC 38500:2008, *Governança corporativa da tecnologia da informação*

[5] Recomendação ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Tecnologia da informação – Técnicas de segurança – Diretrizes para gestão de segurança da informação em organizações de telecomunicações baseadas em ISO/IEC 27002*

[6] ITGI, *Information Security Governance framework: 2009*

[7] ISF, *Standard of Good Practice for Information Security: 2011*