Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação

APRESENTAÇÃO

1) Este Projeto de Revisão foi elaborado pela Comissão de Estudo de Técnicas de Segurança (CE-21:027.00) do Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), nas reuniões de:

02.07.2013	28.08.2013	

2) Este Projeto de Revisão/Emenda é previsto para cancelar e substituir a edição anterior (ABNT NBR ISO IEC 27002:2005), quando aprovado, sendo que nesse ínterim a referida norma continua em vigor;

3) Previsto para ser equivalente à ABNT NBR ISO/IEC 27002:2013;

4) Não tem valor normativo;

5) Aqueles que tiverem conhecimento de qualquer direito de patente devem apresentar esta informação em seus comentários, com documentação comprobatória;

6) Este Projeto de Norma será diagramado conforme as regras de editoração da ABNT quando de sua publicação como Norma Brasileira.

7) Tomaram parte na elaboração deste Projeto:

Participantes	Representante
BAKERTILLY DO BRASIL	Andréa Thomé
CQSI	Ariosto Farias Jr
SERASA EXPERIAN	Denise Menoncello
USIMINAS	Gilmar Ribeiro
INDIVIDUAL	Lilian Prícola
GETNET	Luciano Domingues
TV GLOBO	Vinícuis Brasileiro
BATORI	Ricardo Kiyoshi Batori
CEMIG	Giovani Davi Silva
CORREIOS	Otávio Quadros
DÍGITRO	Andreia S. G. Da Silva

IPEA-SEG	Carlos Augusto Valim
IPEA-SEG	Vera P. Harger
MICROSOFT	Fernando Gebara
PROXIS	Olympio Neto
RIOSOFT	Gisele Villas Bôas
RSA	Anchises De Paula
SABESP	Claudio Barbosa
SABESP	Marcelo Rezende
SEC4YOU	Luciano M. Kadoya
TIVIT	Luiz Gustavo Ribeiro

Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação

Information technology — Security techniques — Code of practice for information security controls

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.

O Escopo desta Norma Brasileira em inglês é o seguinte:

Scope

This Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

a) select controls within the process of implementing an Information Security Management System based on ABNT NBR ISO/IEC 27001;

b) implement commonly accepted information security controls;

c) develop their own information security management guidelines.

0 Introdução

0.1 Contexto e histórico

Esta Norma é projetada para as organizações usarem como uma referência na seleção de controles dentro do processo de implementação de um sistema de gestão da segurança da informação (SGSI), baseado na ABNT NBR ISO/IEC 27001 ou como um documento de orientação para as organizações implementarem controles de segurança da informação comumente aceitos.

Esta Norma é também usada no desenvolvimento de organizações e indústrias especificas de gerenciamento de segurança da informação, levando em consideração os seus ambientes de risco de segurança da informação específicos.

Organizações de todos os tipos e tamanhos (incluindo o setor privado e público, organizações comerciais e sem fins lucrativos), coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal (por exemplo, conversações e apresentações).

O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requer proteção contra vários riscos.

Ativos são objeto de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes. Mudanças nos processos e sistemas do negócio ou outras mudanças externas (tais como novas leis e regulamentações), podem criar novos riscos de segurança da informação. Desta forma, em função das várias maneiras nas quais as ameaças podem se aproveitarem das vulnerabilidades para causar dano à organização, os riscos de segurança da informação estão sempre presentes. Uma segurança da informação eficaz reduz estes riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos.

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização são atendidos.

Um sistema de gestão da segurança da informação (SGSI), a exemplo do especificado na ABNT NBR ISO/IEC 27001, considera uma visão holística e coordenada dos riscos de segurança da informação da organização, para implementar um conjunto de controles de segurança da informação detalhado, com base na estrutura global de um sistema de gestão coerente.

Muitos sistemas de informação não têm sido projetados para serem seguros, na ótica da ABNT NBR ISO/IEC 27001 e desta Norma. A segurança que pode ser alcançada através de meios técnicos é limitada e está apoiada por procedimentos e gerenciamentos apropriados. A identificação de quais controles devem ser implementados requer planejamento e atenção cuidadosa em nível de detalhes. Um sistema de gestão da segurança da informação bem sucedido requer apoio de todos os funcionários da organização. Isto pode também exigir a participação de acionistas, fornecedores ou outras partes externas. Orientações de especialistas externos podem também ser necessárias.

De um modo geral, uma segurança da informação eficaz também garante à direção e outras partes interessadas que os ativos da organização estão razoavelmente seguros e protegidos contra danos, agindo como um facilitador dos negócios.

0.2 Requisitos de segurança da informação

É essencial que uma organização identifique os seus requisitos de segurança da informação.

Existem três fontes principais de requisitos de segurança da informação.

a) Uma fonte é obtida a partir da avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da avaliação de riscos, são identificadas as ameaças aos ativos, e as vulnerabilidades destes e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.

b) Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.

c) A terceira fonte são os conjuntos particulares de princípios, objetivos e os requisitos do negócio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.

Os recursos empregados na implementação dos controles precisam ser balançeados com base na probabilidade de danos ao negócio, resultado dos problemas de segurança pela ausência desses controles. Os resultados de uma avaliação de risco ajudará a orientar e determinar as ações de gestão apropriadas e as prioridades para gerenciar os riscos de segurança da informação e a implementação dos controles selecionados para proteger contra estes riscos.

A ABNT NBR ISO/IEC 27005 fornece diretrizes sobre gestão de riscos de segurança da informação, incluindo orientações sobre avaliação de riscos, tratamentos de riscos, aceitação de riscos, comunicação de riscos, monitoramento e análise critica dos riscos.

0.3 Seleção de controle

Controles podem ser selecionados desta norma ou de outros conjuntos de controles, ou novos controles podem ser projetados para atender necessidades especificas, conforme apropriado.

A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização, e convém que também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais, relevantes. A seleção de controles também depende da maneira pela qual os controles interagem para prover uma proteção segura.

Alguns dos controles nesta norma podem ser considerados como princípios básicos para a gestão da segurança da informação e podem ser aplicados na maioria das organizações. Os controles são explicados em mais detalhes logo a seguir, no campo diretrizes para implementação.

Mais informações sobre seleção de controles e outras opções para tratamento de riscos podem ser encontradas na ABNT NBR ISO/IEC 27005.

0.4 Desenvolvendo suas próprias diretrizes

Esta Norma pode ser considerada como um ponto de partida para o desenvolvimento de diretrizes específicas para a organização. Nem todos os controles e diretrizes contidos neste código de prática podem ser aplicados. Além disto, controles adicionais e recomendações não incluídas nesta Norma, podem ser necessários. Quando os documentos são desenvolvidos contendo controles ou recomendações adicionais, pode ser útil realizar uma referência cruzada com as seções desta Norma, onde aplicável, para facilitar a verificação da conformidade por auditores e parceiros de negócio.

0.5 Considerações sobre o ciclo de vida

A informação tem um ciclo de vida natural, desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até a sua eventual destruição ou obsolecência. O valor e os riscos aos ativos podem variar durante o tempo de vida da informação (por exemplo, revelação não autorizada ou roubo de balanços financeiros de uma companhia, é muito menos importante depois que elas são formalmente publicadas), porém a segurança da informação permanece importante em algumas etapas de todos os estágios.

Sistemas de informação têm ciclos de vida nos quais eles são concebidos, especificados, projetados, desenvolvidos, testados, implementados, usados, mantidos e, eventualmente, retirados do serviço e descartados. Convém que a segurança da informação seja considerada em cada estágio. Desenvolvimentos de sistemas novos e mudanças nos sistemas existentes são oportunidades para as organizações atualizarem e melhorarem os controles de segurança, levando em conta os incidentes reais e os riscos de segurança da informação, projetados e atuais.

0.6 Normas relacionadas

Enquanto esta Norma oferece uma diretriz em uma ampla gama de controles de segurança da informação, que são normalmente aplicados em muitas organizações diferentes, as outras partes da família de normas ISO/IEC 27000 fornece orientações complementares ou requisitos sobre outros aspectos do processo global de gerenciamento da segurança da informação.

A ISO/IEC 27000 apresenta uma introdução geral de um sistema de gestão da segurança da informação e da família de normas da série 27000. A ISO/IEC 27000 fornece um glossário, contendo definições da maioria dos termos usados em toda a família de normas da série 27000, e descreve o escopo e objetivos para cada membro da família.

1 Escopo

Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

Esta norma é projetada para ser usada por organizações que pretendam:

a) selecionar controles dentro do processo de implementação de um sistema de gestão da segurança da informação baseado na ABNT NBR ISO/IEC 27001;

b) implementar controles de segurança da informação comumente aceitos;

c) desenvolver seus próprios princípios de gestão da segurança da informação.

2 Referências normativas

O documento referenciado a seguir é indispensável à aplicação desta norma. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do referido documento (incluindo emendas).

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

3 Termos e definições

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

4 Estrutura desta Norma

Esta Norma contém 14 seções de controles de segurança da informação, 35 Objetivos de controles e 114 controles.

4.1 Seções

Cada seção definindo os controles de segurança da informação contém um ou mais objetivos de controle.

A ordem em que se encontram as seções não implica nem significa o seu grau de importância.

Dependendo das circunstâncias, os controles de segurança da informação de uma de quaisquer das seções podem ser importantes; assim, convém que cada organização implemente esta Norma identificando quais controles são aplicáveis, quão importantes eles são e qual a aplicação para os processos individuais do negócio. A relação dos controles, portanto, não está em ordem de prioridade.

4.2 Categorias de controles

Cada seção principal contém:

a) um objetivo de controle declarando o que se espera ser alcançado;

b) um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.

As descrições do controle estão estruturadas da seguinte forma:

Controle

Define a declaração específica do controle, para atender ao objetivo de controle.

Diretrizes para implementação

Apresenta informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle. As diretrizes podem não ser totalmente adequada ou suficiente em todas as situações e podem, portanto, não atender completamente os requisitos de controle específicos da organização.

Informações adicionais

Apresenta mais dados que podem ser considerados, como por exemplo, questões legais e referências normativas. Se não existem informações adicionais, esta parte não é mostrada no controle.

5 Políticas de segurança da informação

5.1 Orientação da direção para 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.

5.1.1 Políticas para segurança da informação

Controle

Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

Diretrizes para implementação

Convém que no mais alto nível a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.

Convém que as políticas de segurança da informação contemplem requisitos oriundos da:

a) estratégia do negócio;

b) de regulamentações, legislação e contratos;

c) do ambiente de ameaça da segurança da informação, atual e futuro.

Convém que a política de segurança da informação contenha declarações relativas a:

a) definição da segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;

b) atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;

c) processos para o tratamento dos desvios e exceções.

No nível mais baixo, convém que a política de segurança da informação seja apoiada por políticas de tópicos específicos, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.

São exemplos de políticas com tópicos específicos:

a) controle de acesso (ver 9);

b) classificação e tratamento da informação (ver 8.2);

c) segurança física e do ambiente (ver 11);

d) tópicos orientados aos usuários finais:

   1) uso aceitável dos ativos (ver 8.1.3);

   2) mesa Limpa e Tela Limpa (ver11.2.9);

   3) transferência de informações (ver 13.2.1);

   4) dispositivos móveis e trabalho remoto (ver 6.2);

   5) restrições sobre o uso e instalação de software (ver 12.6.2);

e) backup (ver 12.3);

f) transferência da informação (ver 13.2);

g) proteção contra *códigos maliciosos* (ver 12.2);

h) gerenciamento de vulnerabilidades técnicas (ver 12.6.1);

i) Controles criptográficos (ver 10);

j) segurança nas comunicações (ver 13);

k) proteção e privacidade da informação de identificação pessoal (ver 18.1.4);

l) relacionamento na cadeia de suprimento (ver 15).

Convém que estas políticas sejam comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de um programa de conscientização, educação e treinamento em segurança da informação.

Informações adicionais

A necessidade de políticas internas de segurança da informação varia entre organizações. Políticas internas são especialmente úteis em organizações maiores e mais complexas onde aqueles que definem e aprovam os níveis esperados de controle são segregados daqueles que implementam os controles, ou em situações onde uma política se aplica a muitas pessoas ou funções diferentes na organização. Políticas de segurança da informação podem ser emitidas em um único documento, "política de segurança da informação" ou como um conjunto de documentos individuais, relacionados.

Se qualquer uma das políticas de segurança da informação é distribuída fora da organização, convém que cuidados sejam tomados para não divulgar informações confidenciais.

Algumas organizações usam outros termos para estes documentos da política, como "Normas", "Diretrizes" ou "Regras".

5.1.2 Análise crítica das políticas para segurança da informação

Controle

Convém que as políticas para a segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Diretrizes para implementação

Convém que cada política de segurança da informação tenha um gestor que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação das políticas de segurança da informação. Convém que a análise crítica inclua a avaliação de oportunidades para melhoria da política de segurança da informação da organização e tenha um enfoque para gerenciar a segurança da informação em resposta às mudanças ao ambiente organizacional, às circunstâncias do negócio, às condições legais, ou ao ambiente de tecnologia.

Convém que a análise crítica das políticas de segurança da informação leve em consideração os resultados da análise crítica pela direção.

Convém que seja obtida a aprovação da direção para a política revisada.

6 Organização da segurança da informação

6.1 Organização interna

Objetivo: Estabelecer uma estrutura de gerenciamento, para iniciar e controlar a implementação da segurança da informação dentro da organização.

6.1.1 Responsabilidades e papéis pela segurança da informação

Controle

Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas.

Diretrizes para implementação

Convém que a atribuição das responsabilidades pela segurança da informação seja feita em conformidade com as políticas de segurança da informação (ver 5.1.1). Convém que as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança da informação específicos sejam claramente definidas. Convém que as responsabilidades pelas atividades do gerenciamento dos riscos de segurança da informação e, em particular, pela aceitação dos riscos residuais sejam definidas. Convém que as responsabilidades sejam complementadas, onde necessário, com orientações mais detalhadas para locais específicos e recursos de processamento da informação. Convém que as responsabilidades locais para a proteção dos ativos e para realizar processos de segurança da informação específicos, sejam definidas.

Convém que pessoas com responsabilidades definidas pela segurança da informação delegem as tarefas de segurança da informação para outros usuários. Todavia, eles continuam responsáveis para verificar se as tarefas delegadas estão sendo executadas corretamente.

Convém que as áreas pelas quais as pessoas sejam responsáveis, estejam claramente definidas; em particular recomenda-se que os seguintes itens sejam cumpridos:

a) Convém que os ativos e os processos de segurança da informação sejam identificados e claramente definidos;

b) O gestor responsável por cada ativo ou processo de segurança da informação tenha atribuições definidas e os detalhes dessa responsabilidade sejam documentados (ver 8.1.2);

c) Os níveis de autorização sejam claramente definidos e documentados;

d) As pessoas indicadas sejam competentes e capazes de cumprir com as responsabilidades pela segurança da informação e a elas seja dada a oportunidade de manter-se atualizada com os desenvolvimentos;

e) A coordenação e a visão global dos aspectos de segurança da informação na cadeia de suprimento sejam identificadas e documentadas.

Informações adicionais

Muitas organizações atribuem a um gestor de segurança da informação a responsabilidade global pelo desenvolvimento e implementação da segurança da informação, e para apoiar a identificação de controles.

Entretanto, a responsabilidade por pesquisar e implementar os controles frequentemente permanecerá com os gestores individuais. Uma política comum é a nomeação de um proprietário para cada ativo que, então, se torna responsável por sua proteção no dia-a-dia.

6.1.2 Segregação de funções

Controle

Convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.

Diretrizes para implementação

Convém que sejam tomados certos cuidados para impedir que uma única pessoa possa acessar, modificar ou usar ativos sem a devida autorização ou detecção. Recomenda-se que o início de um evento seja separado de sua autorização. A possibilidade de existência de conluios seja considerada no projeto dos controles.

Pequenas organizações podem encontrar dificuldades em aplicar a segregação de função, mas o princípio deve ser aplicável, tão logo seja possível e praticável. Apesar da dificuldade em segregar, convém considerar outros controles, como, monitoração de atividades, trilhas de auditoria e gerenciamento da supervisão.

Informações adicionais

Segregação de funções é um método para reduzir o risco de mau uso, acidental ou deliberado, dos ativos de uma organização.

6.1.3 Contato com autoridades

Controle

Convém que contatos apropriados com autoridades relevantes sejam mantidos.

Diretrizes para implementação

Convém que a organização tenha procedimentos implementados que especifiquem quando e quais autoridades (por exemplo, obrigações legais, corpo de bombeiros, autoridades fiscalizadoras, entidades regulatórias) serão contactadas e como os incidentes de segurança da informação identificados serão reportados em tempo hábil (por exemplo,no caso de suspeita de que a lei foi violada).

Informações adicionais

Organizações sob ataque da internet podem vir a necessitar que autoridades tomem providências contra a origem dos ataques.

Manter tais contatos pode ser um requisito para apoiar a gestão de incidentes de segurança da informação (ver 16) ou do processo de planejamento da contingência e da continuidade de negócio (ver cláusula 17).Contatos com órgãos regulatórios também são úteis para antecipar-se e preparar-se para futuras alterações em leis ou regulamentos, que terão que ser implementados pela organização. Contatos com outras autoridades incluem serviços de infraestrutura, serviços de emergência, fornecedores de energia, saúde e segurança, por exemplo, corpo de bombeiros (juntamente com continuidade de negócios), fornecedores de telecomunicações (juntamente com rotas de linha e disponibilidade) e fornecedores de água (juntamente com instalação de refrigeração para os equipamentos).

6.1.4 Contato com grupos especiais

Controle

Convém que contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação sejam mantidos.

Diretrizes para implementação

Convém que a associação a grupos especiais ou fóruns sejam considerados como forma de:

a) ampliar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre segurança da informação;

b) assegurar que o entendimento do ambiente de segurança da informação está atual e completo;

c) receber previamente advertências de alertas, aconselhamentos e correções relativos a ataques e vulnerabilidades;

d) conseguir acesso à consultoria especializada em segurança da informação;

e) compartilhar e trocar informações sobre novas tecnologias, produtos, ameaças ou vulnerabilidades;

f) prover relacionamentos adequados quando tratar com incidentes de segurança da informação (ver 16).

Informações adicionais

Acordos de compartilhamento de informações podem ser estabelecidos para melhorar a cooperação e coordenação de assuntos de segurança da informação. Convém que tais acordos identifiquem requisitos para a proteção de informação confidencial.

6.1.5 Segurança da informação no gerenciamento de projetos

Controle

Convém que a segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo do projeto.

Diretrizes para implementação

Convém que a segurança da informação seja integrada nos métodos de gerenciamento de projeto da organização para assegurar que os riscos de segurança da informação estão identificados e considerados como parte de um projeto. Isto se aplica de um modo geral, para qualquer projeto independentemente do seu propósito, por exemplo, se é um projeto para um processo crítico do negócio, um processo de TI, de gerenciamento de recursos ou outro processo de apoio.

Convém que os métodos de gerenciamento de projetos usados requeiram que:

a) os objetivos de segurança da informação sejam contemplados nos objetivos do projeto;

b) uma avaliação dos riscos de segurança da informação seja conduzida em estágios iniciais do projeto para identificar os controles que são necessários;

c) a segurança da informação seja parte integrante de todas as fases da metodologia do projeto.

Convém que as questões de segurança da informação sejam consideradas e analisadas criticamente a intervalos planejados, em todos os projetos. Convém que as responsabilidades pela segurança da informação sejam definidas e alocadas para papéis específicos definidos dos métodos de gerenciamento de projeto.

6.2 Dispositivos móveis e trabalho remoto

Objetivo: Garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.

6.2.1 Política para o uso de dispositivo móvel

Controle

Convém que uma política e medidas que apoiam a segurança da informação seja adotada para gerenciar os riscos decorrentes do uso de dispositivos móveis.

Diretrizes para implementação

Convém que quando se utilizam dispositivos móveis, cuidados especiais sejam tomados para assegurar que as informações do negócio não sejam comprometidas. Convém que a política de dispositivos móveis leve em consideração os riscos de se trabalhar com esses dispositivos móveis em ambientes desprotegidos.

Convém que a política para uso de dispositivos móveis considere:

a) registros dos dispositivos móveis;

b) requisitos para a proteção física;

c) restrições quanto à instalação de *softwares*;

d) requisitos para as versões dos *softwares* e aplicações de *patches*;

e) restrições para conexão aos serviços de informação;

f) controle de acesso;

g) técnicas criptográficas;

h) proteção contra códigos maliciosos;

i) desativação, bloqueio e exclusão de forma remota;

j) *backups*;

k) uso dos serviços *web* e aplicações *web*.

Convém que cuidados sejam tomados ao se utilizarem dispositivos móveis em locais públicos, salas de reuniões e outras áreas desprotegidas. Convém que sejam estabelecidas proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nesses dispositivos, por exemplo, através da utilização de técnicas de criptografia (ver 10) e do uso de informação de autenticação secreta (ver 9.2.3).

Convém que os dispositivos móveis sejam também protegidos fisicamente contra roubo, especialmente quando deixados, por exemplo, em carros ou em outros meios de transporte, quartos de hotéis, centros de conferência e locais de reunião. Convém que seja estabelecido um procedimento específico que leve em consideração requisitos legais, securitários e outros requisitos de segurança da organização para casos de furto, roubo ou perda de dispositivos móveis.

Convém que os dispositivos móveis que contêm informações importantes, sensíveis e/ou críticas para o negócio, não sejam deixados sem observação e, quando possível, estejam fisicamente trancados com o uso de travas especiais, para proteger esses dispositivos móveis.

Convém que seja programado treinamento para as pessoas que usam dispositivos móveis, como forma de aumentar a conscientização quanto aos riscos adicionais decorrentes desta forma de trabalho, e os controles que recomenda-se implementar.

Onde a política de dispositivos móveis permita o uso de dispositivos pessoais, convém que esta política e os controles de segurança relacionados, também considerem:

a) separação do uso do dispositivo para negócio e para fins pessoais, incluindo os *softwares* para apoiar esta separação e proteger os dados do negócio em um dispositivo privado;

b) prover acesso às informações do negócio somente depois que os usuários assinarem o acordo de conhecimento das suas responsabilidades (quanto a proteção física, atualização do *software*, entre outros), renunciando direitos autorais dos dados do negócio, que permita a exclusão remota dos dados pela organização no caso de furto, roubo ou perda do dispositivo móvel ou ainda, quando não mais houver autorização para o uso dos serviços. Esta política precisa levar em consideração a legislação sobre privacidade.

Informações adicionais

Conexões de dispositivos móveis sem fio são similares a outros tipos de conexões de rede, mas possuem diferenças importantes as quais recomenda-se considerar na identificação dos controles. As diferenças típicas são:

a) alguns protocolos de segurança sem fio são imaturos e possuem fraquezas conhecidas;

b) informações armazenadas em dispositivos móveis podem não ser passíveis de cópia de segurança por conta de limitações da largura de banda da rede ou porque dispositivos móveis podem não estar conectados no momento em que a cópia de segurança for agendada.

Dispositivos móveis geralmente compartilham funções comuns, por exemplo: rede, acesso à internet, e-mail e manuseio de arquivos, com uso de dispositivos fixos. Controles de segurança da informação para os dispositivos móveis geralmente consistem naqueles adotados para o uso de dispositivos fixos e aqueles para endereçar ameaças levantadas pelo seu uso fora das instalações da organização.

6.2.2 Trabalho remoto

Controle

Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto

Diretrizes para implementação

Convém que a organização que permita a atividade de trabalho remoto publique uma política que defina as condições e restrições para o uso do trabalho remoto. Quando considerados aplicáveis e permitidos por lei, convém que os seguintes pontos sejam considerados:

a) a segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local;

b) o ambiente físico proposto para o trabalho remoto;

c) os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acessada e trafegada na linha de comunicação e a sensibilidade do sistema interno;

d) a provisão de acesso virtual às estações de trabalho dos usuários, para prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular;

e) a ameaça de acesso não autorizado à informação ou aos recursos de processamento da informação por outras pessoas que utilizam o local, por exemplo familiares e amigos;

f) o uso de redes domésticas e requisitos ou restrições na configuração de serviços de rede sem fio;

g) políticas e procedimentos para evitar disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular;

h) acesso a equipamentos de propriedade particular (para verificar a segurança da máquina ou durante uma investigação), que pode ser proibido legalmente;

i) acordos de licenciamento de *software* que podem tornar as organizações responsáveis pelo licenciamento do *software* cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou terceiros;

j) requisitos de proteção contra vírus e requisitos de *firewall.*

Convém que as diretrizes e providências considerem:

a) a provisão de equipamento e mobília apropriados às atividades de trabalho remoto, onde o uso de equipamentos de propriedade particular que não esteja sob controle da organização não seja permitido;

b) uma definição do trabalho permitido, o período de trabalho, a classificação da informação que pode ser tratada e os sistemas internos e serviços que o usuário do trabalho remoto está autorizado a acessar;

c) provisão de equipamento de comunicação apropriado, incluindo métodos para acesso remoto seguro;

d) segurança física;

e) regras e diretrizes sobre o acesso de familiares e visitantes ao equipamento e à informação;

f) a provisão de suporte e manutenção de *hardware* e *software*;

g) a provisão de seguro;

h) os procedimentos para cópias de segurança e continuidade do negócio;

i) auditoria e monitoramento da segurança;

j) revogação de autoridade e direitos de acesso, e devolução do equipamento quando as atividades de trabalho remoto cessarem.

Informações adicionais

Trabalho remoto refere-se a todas as formas de trabalho fora do escritório, incluindo ambientes de trabalho não tradicionais, como aqueles referidos como: “ambientes de *telecommuting*”, “local de trabalho flexível”, “ trabalho remoto” e “trabalho virtual”.

7 Segurança em recursos humanos

7.1 Antes da contratação

Objetivo: Assegurar que funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados.

7.1.1 Seleção

Controle

Convém que verificações do histórico sejam realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.

Diretrizes para implementação

Convém que as verificações levem em consideração toda a legislação pertinente relativa à privacidade, proteção da informação de identificação pessoal e do emprego e, onde permitido, incluam os seguintes itens:

a) disponibilidade de referências de caráter satisfatórias, por exemplo uma profissional e uma pessoal;

b) uma verificação (da exatidão e completeza) das informações do *curriculum vitae* do candidato;

c) confirmação das qualificações acadêmicas e profissionais;

d) verificação independente da identidade (passaporte ou documento similar);

e) verificações mais detalhadas, tais como verificações financeiras (de crédito) ou verificações de registros criminais**.**

Convém que quando um individuo seja contratado para desempenhar o papel de segurança da informação, a organização certifique-se de que o candidato:

a) tem a competência necessária para executar as atividades de segurança da informação;

b) é suficientemente confiável para desempenhar a sua tarefa, especialmente se a atividade é crítica para a organização.

Onde um trabalho envolver pessoas, tanto por contratação como por promoção, que tenham acesso aos recursos de processamento da informação, em particular aquelas que tratam de informações sensíveis, como informações financeiras ou informações altamente confidenciais, convém que a organização faça verificações mais detalhadas.

Convém que procedimentos definam critérios e limitações para as verificações de controle, por exemplo, quem está qualificado para selecionar as pessoas, e como, quando e por que as verificações de controle são realizadas.

Convém que um processo de seleção também seja feito para fornecedores e partes externas. Nestes casos, convém que o acordo entre a organização e o prestador de serviços especifique as responsabilidades por conduzir e realizar a seleção, bem como os procedimentos de notificação que precisam ser seguidos no caso em que a seleção não tenha sido concluída ou se os resultados gerarem dúvidas ou preocupações.

Convém que as informações sobre todos os candidatos que estão sendo considerados para certas posições dentro da organização, sejam levantadas e tratadas de acordo com a legislação apropriada existente na jurisdição pertinente. Dependendo da legislação aplicável, convém que os candidatos sejam previamente informados sobre as atividades de seleção.

7.1.2 Termos e condições de contratação

Controle

Convém que as obrigações contratuais com funcionários e partes externas, declarem as suas responsabilidades e a da organização para a segurança da informação.

Diretrizes para implementação

Convém que as obrigações contratuais para funcionários e partes externas, reflitam as políticas para segurança da informação da organização, esclarecendo e declarando:

a) que todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento da informação (ver 13.2.4);

b) as responsabilidades legais e direitos dos funcionários e partes externas, e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais e legislação de proteção de dados (ver 18.1.4);

c) as responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização, associados com a informação, com os recursos de processamento da informação e com os serviços de informação conduzidos pelos funcionários, fornecedores ou partes externas (ver 8);

d) as responsabilidades dos funcionários ou partes externas, pelo tratamento da informação recebida de outras companhias ou partes interessadas;

e) ações a serem tomadas no caso de o funcionário ou partes externas, desrespeitar os requisitos de segurança da informação da organização (ver 7.2.3).

Convém que os papéis e responsabilidades pela segurança da informação sejam comunicados para o candidato durante o processo de pré-contratação.

Convém que a organização assegure que os funcionários ou partes externas concordem com os termos e condições relativas à segurança da informação, adequados à natureza e abrangência do

acesso que eles terão aos ativos da organização, associados com os sistemas e serviços de informação.

Onde apropriado, convém que as responsabilidades contidas nos termos e condições de contratação continuem por um período de tempo definido, após o término da contratação (ver 7.3).

Informações adicionais

Um código de conduta pode ser usado para estabelecer as responsabilidades de segurança da informação do funcionário ou parte externa quanto à confidencialidade, proteção de dados, ética, uso apropriado dos equipamentos e recursos da organização, assim como as práticas respeitosas esperadas pela organização. Partes externas com as quais um fornecedor é associado podem ser solicitadas a entrar nos acordos contratuais em nome do indivíduo contratado.

7.2 Durante a contratação

Objetivo: Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.

7.2.1 Responsabilidades da direção

Controle

Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.

Diretrizes para implementação

Convém que as responsabilidades da direção assegurem que os funcionários e partes externas:

a) estão adequadamente instruídos sobre as suas responsabilidades e papéis pela segurança da informação, antes de obter acesso às informações sensíveis ou aos sistemas de informação;

b) recebam diretrizes que definam quais as expectativas sobre a segurança da informação de suas atividades dentro da organização;

c) estão motivados para cumprir com as políticas de segurança da informação da organização;

d) atinjam um nível de conscientização sobre segurança da informação que seja relevante para os seus papéis e responsabilidades dentro da organização (ver 7.2.2);

e) cumpram com os termos e condições de trabalho, que incluam a política de segurança da informação da organização e métodos apropriados de trabalho;

f) tenham as habilidades e qualificações apropriadas e sejam treinados em bases regulares;

g) tenham disponíveis um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação.

É recomendado que a direção demonstre seu apoio às políticas, procedimentos e controles, e aja como tal, de forma exemplar.

Informações adicionais

Se os funcionários e fornecedores não forem conscientizados das suas responsabilidades em segurança da informação, eles podem causar danos consideráveis para uma organização.

Pessoal motivado pode ser mais confiável e causar menos incidentes de segurança da informação.

Uma má gestão pode fazer com que o pessoal se sinta desvalorizado, resultando em impacto negativo na segurança da informação da organização. Por exemplo, uma má gestão pode levar a segurança da informação a ser negligenciada ou a um potencial mau uso dos ativos da organização.

7.2.2 Conscientização, educação e treinamento em segurança da informação

Controle

Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

Diretrizes para implementação

Convém que um programa de conscientização em segurança da informação tenha por objetivo tornar os funcionários e, onde relevante, partes externas, conscientes das suas responsabilidades para a segurança da informação e os meios pelos quais essas responsabilidades são realizadas.

Convém que um programa de conscientização em segurança da informação seja estabelecido alinhado com as políticas e procedimentos relevantes de segurança da informação da organização, levando em consideração as informações da organização a serem protegidas e os controles a serem implementados para proteger a informação.

Convém que o programa de conscientização considere um número de atividades de conscientização, tais como, campanhas (por exemplo, dia da segurança da informação) e a publicação de boletins ou folhetos.

Convém que o programa de conscientização seja planejado levando em consideração os papéis a serem desempenhados na organização pelos funcionários e, onde relevante, as expectativas da organização quanto à conscientização das partes externas. Convém que as atividades do programa de conscientização sejam planejadas ao longo do tempo, preferencialmente de forma regular, de tal modo que as atividades sejam repetidas e contemplem novos funcionários e partes externas.

Convém que o programa de conscientização também seja atualizado regularmente, de modo que ele permaneça alinhado com as políticas e os procedimentos da organização, e seja construídos com base nas lições aprendidas dos incidentes de segurança da informação.

Convém que o treinamento em conscientização seja realizado conforme requerido pelo programa de conscientização em segurança da informação da organização. Convém que o treinamento em consientização use diferentes formas de apresentação, tais como, treinamento presencial, treinamento a distância, treinamento baseado em web, autodidata e outros.

Convém que o treinamento e educação em segurança da informação também contemple aspectos gerais, como:

a) declaração do comprometimento da direção com a segurança da informação em toda a organização;

b) a necessidade de tornar conhecido e estar em conformidade com as obrigações e regras de segurança da informação aplicavéis, conforme definido nas políticas, normas, leis, regulamentações, contratos e acordos.

c) responsabilidade pessoal por seus próprios atos e omissões, e compromissos gerais para manter seguro ou para proteger a informação que pertença a organização e partes externas.

d) procedimentos de segurança da informação básicos (tais como, notificação de incidente de segurança da informação) e controles básicos (tais como, segurança da senha, controles contra *códigos maliciosos* e política de mesa limpa e tela limpa).

e) pontos de contato e recursos para informações adicionais e orientações sobre questões de segurança da informação, incluindo materiais de treinamento e educação em segurança da informação.

Convém que o treinamento e a educação em segurança da informação seja realizado periodicamente. Treinamento e educação iniciais se aplicam aqueles que são transferidos para novas posições ou atribuições com requisitos de segurança da informação completamente diferentes, e não apenas para os novos iniciantes e deve ser realizado antes das pessoas assumirem os seus papéis.

Convém que a organização desenvolva o programa de treinamento e educação com o objetivo de conduzir a educação e treinamento de forma eficaz. Convém que o programa esteja alinhado com as políticas e procedimentos relevantes de segurança da informação da organização, levando em consideração as informações da organização a serem protegidas e os controles que devem ser implementados para proteger a informação. Convém que o programa considere diferentes formas de educação e treinamento, tais como, leituras ou auto-estudos.

Informações adicionais

Ao compor um programa de conscientização, é importante não focar apenas no “o que” e “como”, mas também no “por que”. É importante que os funcionários entendam os objetivos da segurança da informação e o impacto potencial, positivo e negativo, do seu próprio comportamento na organização.

Conscientização, educação e treinamento pode ser parte de, ou conduzido em colaboração com outras atividades de treinamento geral em TI ou treinamento geral em segurança.

Conscientização, educação e atividades de treinamento devem ser ajustáveis e relevantes aos papéis dos indivíduos, responsabilidades e habilidades (ver 7.2.2).

Uma avaliação do entendimento das pessoas pode ser conduzida no final do curso de conscientização, educação ou treinamento para testar a transferência de conhecimento.

7.2.3 Processo disciplinar

Controle

Convém que exista um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.

Diretrizes para implementação

Convém que o processo disciplinar não inice sem uma verificação prévia de que a violação da segurança da informação realmente ocorreu (Ver 16.1.7).

Convém que o processo disciplinar formal assegure um tratamento justo e correto aos funcionários que são suspeitos de cometer violações de segurança da informação. Convém que o processo disciplinar formal apresente uma resposta de forma gradual, que leve em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio, se este é ou não o primeiro delito, se o infrator foi ou não adequadamente treinado, as legislações relevantes, os contratos do negócio e outros fatores conforme requerido.

Convém que o processo disciplinar também seja usado como uma forma de dissuasão, para evitar que os funcionários e partes externas, violem os procedimentos e as políticas de segurança da informação da organização, e quaisquer outras violações na segurança da informação. Violações deliberadas (propositais), podem exigir ações imediatas.

Informações adicionais

O processo disciplinar pode também tornar-se uma motivação ou um incentivo se recompensas positivas forem definidas por comportamento destacável no que se refere à segurança da informação.

7.3 Encerramento e mudança da contratação

Objetivo: Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

7.3.1 Responsabilidades pelo encerramento ou mudança da contratação

Controle

Convém que as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação, sejam definidas, comunicadas aos funcionários ou partes externas e sejam cumpridas.

Diretrizes para implementação

Convém que a comunicação de encerramento de atividades inclua requisitos de segurança da informação e responsabilidades legais existentes e, onde apropriado, responsabilidades contidas em quaisquer acordos de confidencialidade e os termos e condições de trabalho que continuem por um período definido após o fim do trabalho do funcionário ou partes externas.

Convém que as responsabilidades e obrigações contidas nos contratos dos funcionários ou partes externas, permaneçam válidas após o encerramento das atividades.

Convém que as mudanças de responsabilidades ou do trabalho sejam gerenciadas quando do encerramento da responsabilidade ou do trabalho atual, combinado com o início de novas responsabilidades ou trabalho.

Informações adicionais

A função de Recursos Humanos é geralmente responsável por todo processo de demissão e trabalha junto com o gestor da pessoa que está saindo da empresa para gerir os aspectos relevantes dos procedimentos de segurança da informação. No caso de um prestador de serviço fornecido por uma parte externa, este processo é feito pela parte externa de acordo com o contrato entre a organização e a parte externa.

Pode ser necessário informar funcionários, clientes ou fornecedores de alterações de pessoal e acordos operacionais.

8 Gestão de ativos

8.1 Responsabilidade pelos ativos

Objetivo: Identificar os ativos da organização e definir as responsabilidades apropriadas para a proteção dos ativos.

8.1.1 Inventário dos ativos

Controle

Convém que os ativos associados com informação e com os recursos de processamento da informação sejam identificados e um inventário destes ativos seja estruturado e mantido.

Diretrizes para implementação

Convém que a organização identifique os ativos relevantes no ciclo de vida da informação e documente a sua importância. Convém que o ciclo de vida da informação inclua a criação, o processamento, o armazenamento, a transmissão, a exclusão e a sua destruição. Convém que a documentação seja mantida em um inventário existente ou exclusivo, conforme apropriado.

Convém que o inventário de ativos seja completo, atualizado, consistente e alinhado com outros inventários.

Convém que para cada um dos ativos identificados, seja indicado um responsável (ver 8.1.2) e a classificação do ativo a ser identificado (ver 8.2).

Informações adicionais

Os inventários de ativos ajudam a assegurar que a proteção efetiva ocorra, e podem igualmente ser exigidos para outras finalidades, tais como a saúde e segurança, razões de seguro ou financeiras (gestão de ativos).

A ABNT NBR ISO/IEC 27005 fornece exemplos de ativos que podem necessitar serem considerados pela organização na identificação dos ativos. O processo de compilação de um inventário de ativos é um pré-requisito importante da gestão de riscos.

8.1.2 Proprietário dos ativos

Controle

Convém que os ativos mantidos no inventário tenham um proprietário.

Diretrizes para implementação

Convém que as pessoas e outras entidades que tenham responsabilidades aprovadas pela direção para qualificar o ciclo de vida do ativo sejam designadas como o proprietário deste ativo.

Convém que seja implementado um processo para assegurar a atribuição, em tempo hábil, do proprietário de um ativo. Convém que o proprietário seja designado quando os ativos são criados ou quando os ativos são transferidos para a organização. Convém que o proprietário do ativo seja responsável pelo próprio gerenciamento deste ativo ao longo do seu ciclo de vida.

Convém que o proprietário do ativo:

a) assegure que os ativos são inventariados;

b) assegure que os ativos são adequadamente classificados e protegidos;

c) defina e periodicamente analise criticamente as classificações e restrições ao acesso aos ativos importantes, levando em conta as políticas de controle de acesso aplicáveis;

d) assegure um adequado tratamento quando o ativo é excluído ou destruído.

Informações adicionais

O proprietário identificado pode ser um indivíduo ou uma entidade que aprovou a responsabilidade pela gestão, para controlar todo o ciclo de vida de um ativo. O proprietário identificado não tem necessariamente quaisquer direitos de propriedade sobre o ativo.

As tarefas de rotina podem ser delegadas, por exemplo, para um custodiante cuidar dos ativos no dia-a-dia, mas a responsabilidade permanece com o proprietário.

Em sistemas de informação complexos, pode ser útil definir grupos de ativos que atuem juntos para fornecer um serviço particular. Neste caso, o proprietário deste serviço é responsável pela entrega do serviço, incluindo a operação dos ativos envolvidos.

8.1.3 Uso aceitável dos ativos

Controle

Convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação, sejam identificadas, documentadas e implementadas.

Diretrizes para implementação

Convém que funcionários e partes externas que usam ou têm acesso aos ativos da organização estejam conscientes dos requisitos de segurança da informação dos ativos da organização, associados com a informação e os recursos e instalações de processamento da informação. Convém que eles sejam responsáveis pelo seu uso de qualquer recurso de processamento da informação e tal uso seja realizado sob sua responsabilidade

8.1.4 Devolução de ativos

Controle

Convém que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

Diretrizes para implementação

Convém que o processo de encerramento de atividades seja formalizado para contemplar a devolução de todos os equipamentos físico e eletronico, de propriedade da organização.

Convém que no caso em que um funcionário ou partes externas, compre o equipamento da organização ou use o seu próprio equipamento pessoal, procedimentos sejam adotados para assegurar que toda a informação relevante seja transferida para a organização e que seja apagada de forma segura do equipamento (Ver 11.2.7).

Convém que nos casos em que o funcionário ou partes externas, tenham conhecimento de que seu trabalho é importante para as atividades que são executadas, esta informação seja documentada e transferida para a organização.

Convém que durante o período de encerramento, a organização monitore possíveis cópias de informações relevantes (por exemplo, propriedade intelectual) pelos funcionários ou partes externas que estão saindo da organização.

8.2 Classificação da informação

Objetivo: Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

8.2.1 Classificação da informação

Controle

Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

Diretrizes para implementação

Convém que a classificação e os controles de proteção, associados para a informação, leve em consideração as necessidades do negócio para compartilhar ou restrigir a informação bem como os requisitos legais. Convém que outros ativos além dos ativos de informação também sejam classificados de acordo com a classificação da informação armazenada, processada, manuseada ou protegida pelo ativo.

Convém que os proprietários de ativos de informação sejam responsáveis por sua classificação.

Convém que o esquema de classificação inclua convenções para classificação e critérios para análise crítica da classificação ao longo do tempo. Convém que o nível de proteção seja avaliado por meio da análise da confidencialidade, integridade e disponibilidade e quaisquer requisitos considerados para a informação.

Convém que o esquema esteja alinhado com a política de controle de acesso (Ver 9.1.1).

Convém que a cada nível seja dado um nome que faça sentido no contexto do esquema de classificação.

Convém que o esquema seja consistente em toda a organização de forma que cada pessoa possa classificar a informação e os ativos relacionados da mesma forma, e tenham um entendimento comum dos requisitos de proteção e apliquem a proteção apropriada.

Convém que a classificação seja incluída nos processos da organização e seja consistente e coerente em toda a organização. Convém que os resultados da classificação indiquem o valor dos ativos em função da sua sensibilidade e criticidade para a organização, em termos da confidencialidade, integridade e disponibilidade. Convém que os resultados da classificação sejam atualizados de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida.

Informações adicionais

A Classificação fornece às pessoas que lidam com informações uma indicação concisa de como tratar e proteger a informação. A criação de grupos de informação com necessidades de proteção semelhantes e especificação dos procedimentos de segurança da informação que se aplicam a todas as informações de cada grupo, é um facilitador. Esta abordagem reduz a necessidade de avaliação de risco e a customização personalizada de controles caso a caso.

A informação pode deixar de ser sensível ou crítica após certo período de tempo, por exemplo, quando a informação se torna pública. Convém que estes aspectos sejam levados em consideração, pois uma classificação superestimada pode levar à implementação de controles desnecessários, resultando em despesas adicionais ou, pelo contrário, classificações subestimada podem pôr em perigo o alcance dos objetivos de negócio.

Um exemplo de um esquema de classificação de confidencialidade da informação poderia ser baseado em quatro níveis, a seguir:

a) quando sua divulgação não causa nenhum dano;

b) quando a divulgação causa constrangimento menor ou inconveniência operacional menor;

c) quando a divulgação tem um pequeno impacto significativo nas operações ou objetivos táticos;

d) quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

8.2.2 Rótulos e tratamento da informação

Controle

Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.

Diretrizes para implementação

Convém que procedimentos para a rotulação da informação abranjam a informação e os seus ativos relacionados, nos formatos físico e eletrônico. A rotulação pode refletir o esquema de classificação estabelecido em 8.2.1. Convém que os rótulos sejam facilmente reconhecidos.

Convém que o procedimento oriente sobre onde e como os rótulos devem ser colocados, levando-se em conta como a informação é acessada ou os ativos são manuseados, em função dos tipos de mídias.

O procedimento pode definir uma situação onde a rotulação é omitida, por exemplo, rotulação de informação não confidencial, para reduzir a carga de trabalho. Convém que os funcionários e partes externas estejam conscientes do procedimento de classificação da informação.

Convém que os resultados de sistemas que contém informações classificadas como críticas ou sensíveis tenham um nível de classificação apropriado.

Informações adicionais

A rotulação de informações classificadas é um requisito chave para acordos de compartilhamento de informações. Rótulos físicos e metadados são uma forma comum de rotulagem.

A rotulação de informação e de ativos relacionados podem às vezes ter efeitos negativos. Ativos classificados são mais fáceis de identificar e, consequentemente, roubados por pessoas internas ou externas.

8.2.3 Tratamento dos ativos

Controle

Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotada pela organização.

Diretrizes para implementação

Convém que procedimentos sejam estabelecidos para o tratamento, processamento, armazenamento e a transmissão da informação, de acordo com a sua classificação (Ver 8.2.1).

Convém que os seguintes itens sejam considerados:

a) Restrições de acesso para apoiar os requisitos de proteção para cada nível de classificação;

b) Manutenção de um registro formal dos destinatários de ativos autorizados;

c) Armazenamento dos ativos de TI de acordo com as especificações dos fabricantes;

d) Identificação eficaz de todas as cópias das mídias, para chamar a atenção dos destinatários autorizados.

O esquema de classificação usado na organização pode não ser equivalente aos esquemas usados por outras organizações, mesmo se os nomes dos níveis são similares;

Adicionalmente, uma informação que transita entre organizações pode variar a sua classificação dependendo do contexto da informação em cada organização, mesmo se os esquemas de classifcação são idênticos.

Convém que acordos com outras organizações que incluam o compartilhamento de informação, contemplem procedimento para identificar a classificação daquela informação e interpretar os rótulos de classificação de outras organizações.

8.3 Tratamento de mídias

Objetivo: Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.

8.3.1 Gerenciamento de mídias removíveis

Controle

Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.

Diretrizes para implementação

Convém que as seguintes diretrizes para o gerenciamento de mídias removíveis sejam consideradas:

a) quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável seja destruído, caso venha a ser retirado da organização;

b) quando necessário e prático, seja requerida a autorização para remoção de qualquer mídia da organização e mantido o registro dessa remoção como trilha de auditoria;

c) toda mídia seja guardada de forma segura em um ambiente protegido, de acordo com as especificações do fabricante;

d) convém que sejam usadas, no caso em que a integridade ou confidencialidade dos dados sejam considerações importantes, técnicas de criptografia, para proteger os dados na mídia removível;

e) para mitigar o risco de degradar a mídia enquanto os dados armazenados ainda são necessários, convém que os dados sejam transferidos para uma mídia nova antes de se tornar ilegíveis;

f) cópias múltiplas de dados valiosos sejam armazenadas em mídias separadas para reduzir riscos futuros de perda ou dano, que ocorram por coincidência nessas mídias;

g) as mídias removíveis sejam registradas para limitar a oportunidade de perda de dados;

h) as unidades de mídia removíveis sejam habilitadas somente se houver uma necessidade do negócio;

i) onde houver a necessidade para o uso de mídia removível, a transferência da informação contida na mídia seja monitorada.

Convém que procedimentos e níveis de autorização sejam documentados.

8.3.2 Descarte de mídias

Controle

Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.

Diretrizes para implementação

Convém que procedimentos formais para o descarte seguro das mídias sejam definidos para minimizar o risco de vazamento de informações sensíveis para pessoas não autorizadas. Os procedimentos para o descarte seguro das mídias, contendo informações confidenciais, sejam proporcionais á sensibilidade das informações. Recomenda-se que os itens abaixo sejam considerados:

a) convém que mídias contendo informações confidenciais sejam guardadas e destruídas de forma segura e protegida, como por exemplo, através de incineração ou trituração, ou da remoção dos dados para uso por outra aplicação dentro da organização;

b) procedimentos sejam implementados para identificar os itens que requerem descarte seguro;

c) pode ser mais fácil implementar a coleta e descarte seguro de todas as mídias a serem inutilizadas do que tentar separar apenas aquelas contendo informações sensíveis;

d) muitas organizações oferecem serviços de coleta e descarte de mídia; convém que sejam tomados cuidados na seleção de um fornecedor com experiência e controles adequados;

e) convém que o descarte de itens sensíveis sejam registrados, sempre que possível, para se manter uma trilha de auditoria.

Quando da acumulação de mídias para descarte, seja levada em consideração o efeito proveniente do acúmulo, o que pode fazer com que uma grande quantidade de informação não sensível, torna-se sensível.

Informações adicionais

Equipamentos danificados contendo dados sensíveis podem exigir uma avaliação de riscos para determinar se é recomendado que os itens sejam destruídos fisicamente ao invés de serem enviados para conserto ou descartados (ver 11.2.7).

8.3.3 Transferência física de mídias

Controle

Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte..

Diretrizes para implementação

Convém que as seguintes recomendações sejam consideradas, para proteger as mídias que contém informações, quando transportadas:

a) o meio de transporte ou o serviço de mensageiros sejam confiáveis;

b) seja definida uma relação de portadores autorizados em concordância com o gestor;

c) seja estabelecido procedimento para a verificação da identificação dos transportadores;

d) a embalagem seja suficiente para proteger o conteúdo contra qualquer dano físico, como os que podem ocorrer durante o transporte, e que seja feita de acordo com as especificações dos fabricantes (como no caso de *softwares*), por exemplo, protegendo contra fatores ambientais que possam reduzir a possibilidade de restauração dos dados como a exposição ao calor, umidade ou campos eletromagnéticos;

e) registros (*logs*) sejam guardados, identificando o conteúdo da mídia, a proteção aplicada, bem como os registros dos tempos de transferência no trânsito entre o custodiante e o destino final.

Informações adicionais

Informações podem ser vulneráveis a acesso não autorizado, uso indevido ou corrupção durante o transporte físico, por exemplo, quando o envio de mídia através do serviço postal ou via correio. Neste controle, incluem-se mídias de documentos em papel.

Quando a informação confidencial não é criptografada na mídia, convém que seja considerada a proteção física adicional desta mídia.

9 Controle de acesso

9.1 Requisitos do negócio para controle de acesso

Objetivo: Limitar o acesso à informação e aos recursos de processamento da informação.

9.1.1 Política de controle de acesso

Controle

Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.

Diretrizes para implementação

Convém que os proprietários dos ativos determinem regras apropriadas do controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem seus ativos, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança da informação associados.

Convém que sejam considerados os controles de acesso lógico e físico (Ver 11) de forma conjunta. Convém que uma declaração nítida dos requisitos do negócio a serem atendidos pelo controle de acesso, seja fornecida aos usuários e provedores de serviços.

Convém que a política leve em consideração os seguintes itens:

a) requisitos de segurança de aplicações de negócios individuais;

b) política para disseminação e autorização da informação, por exemplo, o princípio “necessidade de conhecer” e níveis de segurança e a classificação das informações (ver 8.2);

c) consistência entre os direitos de acesso e as políticas de classificação da informação em diferentes sistemas e redes;

d) legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços (ver 18.1);

e) gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis;

f) segregação de funções de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso;

g) requisitos para autorização formal de pedidos de acesso (ver 9.2.1);

h) requisitos para análise crítica periódica de direitos de acesso (ver 9.2.5);

i) remoção de direitos de acesso (ver 9.2.6);

j) arquivo dos registros de todos os eventos significantes, relativos ao uso e gerenciamento das identidades do usuário e da informação de autenticação secreta;

k) regras para o acesso privilegiado (ver 9.2.3).

Informações adicionais

Convém que sejam tomados cuidados na especificação de regras de controle de acesso quando se considerar o seguinte:

a) estabelecer regra baseada na premissa de que “Tudo é proibido a menos que expressamente permitido" em lugar da regra mais fraca que "Tudo é permitido, a menos que expressamente proibido";

b) mudanças em rótulos de informação (ver 8.2.2) que são iniciadas automaticamente através de recursos de processamento da informação e aquelas iniciadas pela observação de um usuário;

c) mudanças em permissões de usuário que são iniciadas automaticamente pelo sistema de informação e os que iniciaram por um administrador;

d) regras que requerem aprovação específica antes de um decreto ou lei e as que não necessitam. Convém que as regras para controle de acesso sejam apoiadas por procedimentos formais (ver 9.2, 9.3 e 9.4) e responsabilidades claramente definidas (ver 6.1.1, 9.2, e 15.1).

As regras baseadas em controles de acesso é uma abordagem usada com sucesso por muitas organizações para relacionar os direitos de acesso com as atividades do negócio.

Dois dos frequentes princípios que orientam a política de controle de acesso são:

a) necessidade de conhecer: você somente tem permissão para acessar informação que você necessita para desempenhar suas tarefas (tarefas e atribuições diferentes significam diferentes necessidades de conhecer e diferentes perfis de acesso);

b) necessidade de uso: você somente tem permissão para acessar os recursos de processamento da informação (equipamentos de TI, aplicações, procedimentos, salas), que você necessita para desempenhar a sua tarefa/função/papel.

9.1.2 Acesso às redes e aos serviços de rede

Controle

Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

Diretrizes para implementação

Convém que uma política seja formulada com relação ao uso de redes e serviços de rede. Convém que esta política inclua:

a) redes e serviços de redes que são permitidos de serem acessados;

b) procedimentos de autorização para determinar quem tem permissão para acessar quais redes e serviços de redes;

c) procedimentos e controles de gerenciamento para proteger o acesso a conexões e serviços de redes;

d) os meios usados para acessar redes e serviços de rede (por exemplo, uso de VPN ou redes sem fio);

e) requisitos de autenticação do usuário para acessar vários serviços de rede;

f) monitoramento do uso dos serviços de rede.

Convém que a política do uso de serviço de rede seja consistente com a política de controle de acesso da organização (ver 9.1.1).

Informações adicionais

Conexões sem autorização e inseguras nos serviços de rede podem afetar toda organização. Este controle é particularmente importante para conexões de redes sensíveis ou aplicações de negócios críticos ou para usuários em locais de alto risco, por exemplo, áreas públicas ou externas que estão fora da administração e controle da segurança da organização.

9.2 Gerenciamento de acesso do usuário

Objetivo: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.

9.2.1 Registro e cancelamento de usuário

Controle

Convém que um processo formal de registro e cancelamento de usuário seja implementado para permitir atribuição de direitos de acesso.

Diretrizes para implementação

Convém que o processo para gerenciar o identificador de usuário (ID de usuário) inclua:

a) o uso de um ID de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações; o uso compartilhado de ID de usuário somente será permitido, onde eles são necessários por razões operacionais ou de negócios e convém que seja aprovado e documentado;

b) a imediata remoção ou desabilitação do ID de usuário que tenha deixado a organização (ver 9.2.5);

c) a remoção e identificação, de forma periódica, ou a desabilitação de usuários redundantes com ID;

d) a garantia de que o ID de usuário redundante não é emitido para outros usuários;

Informações adicionais

Fornecer ou revogar o acesso à informação ou aos recursos de processamento da informação, normalmente é um procedimento de duas etapas:

a) atribuir e permitir, ou revogar, um ID de um usuário;

b) fornecer, ou revogar, os direitos de acesso para este usuário de ID (ver 9.2.2)

9.2.2 Provisionamento para acesso de usuário

Controle

Convém que um processo formal de provisionamento de acesso do usuário seja implementado para conceder ou revogar os direitos de acesso do usuário para todos os tipos de usuários em todos os tipos de sistemas e serviços.

Diretrizes para implementação

Convém que o processo de provisionamento para atribuir ou revogar os direitos de acesso concedidos ao ID de usuário inclua:

a) obtenção de autorização do proprietário do sistema ou do serviço da informação para o uso do serviço ou sistema da informação (ver 8.1.2); aprovações separadas para os direitos de acesso da direção também pode ser recomendada;

b) verificação de que o nível de acesso concedido é apropriado ás políticas de acesso (ver 9.1) e é consistente com outros requisitos, tais como, segregação de funções(ver 6.1.2);

c) garantia de que os direitos de acesso não estão ativados (por exemplo, por provedores de serviços) antes que o procedimento de autorização esteja completo;

d) manutenção de um registro central de direitos de acesso concedido ao ID de usuário para acessar serviços e sistemas de informação;

e) adaptação dos direitos de acesso dos usuários que tenham mudado de função ou de atividades, e imediata remoção ou bloqueio dos direitos de acesso dos usuários que deixaram a organização;

f) direitos de acesso analisados criticamente a intervalos regulares com os proprietários dos serviços ou sistemas de informação (ver 9.2.4)

Informações adicionais

Convém que consideração seja dada para estabelecer as regras de acesso do usuário baseadas nos requisitos do negócio que resumam um número de direitos de acesso em um perfil típico de acesso do usuário. Solicitações de acesso e análises críticas (ver 9.2.4), são facilmente gerenciadas no nível de tais papéis do que no nível de direitos particulares.

Convém que consideração seja dada para incluir cláusulas nos contratos de pessoas e nos contratos de serviços, que especifiquem sanções no caso de tentativa de acesso não autorizado pelas pessoas ou pelas partes externas (ver 7.1.2, 7.2.3,13.2.4 e 15.1.2)

9.2.3 Gerenciamento de direitos de acesso privilegiados

Controle

Convém que a concessão e uso de direitos de acesso privilegiado sejam restritos e controlados.

Diretrizes para implementação

Convém que a alocação de direitos de acesso privilegiado seja controlada por meio de um processo de autorização formal, de acordo com a política de controle de acesso pertinente (ver 9.1.1).

Convém que os seguintes passos sejam considerados:

a) os direitos de acesso privilegiados, associados a cada sistema ou processo, por exemplo, sistema operacional, sistemas de gerenciamento de banco de dados e cada aplicação, e de categorias de usuários para os quais estes necessitam ser concedido, sejam identificados;

b) os direitos de acesso privilegiado sejam concedidos a usuários conforme a necessidade de uso e com base em eventos alinhados com a política de controle de acesso (ver 9.1.1), baseado nos requisitos mínimos para sua função;

c) um processo de autorização e um registro de todos os privilégios concedidos sejam mantidos. direitos de acesso privilegiados não sejam concedidos até que todo o processo de autorização esteja finalizado;

d) requisitos para expirar os direitos de acesso privilegiado sejam definidos;

e) os direitos de acesso privilegiados sejam atribuídos a um ID de usuário diferente daqueles usados nas atividades normais do negócio. As atividades normais do negócio não sejam desempenhadas usando contas privilegiadas;

f) as competências dos usuários com direitos de acesso privilegiado sejam analisadas criticamente a intervalos regulares, para verificar se eles estão alinhados com as suas obrigações;

g) procedimentos específicos sejam estabelecidos e mantidos para evitar o uso não autorizado de ID de usuário de administrador genérico, de acordo com as capacidades de configuração dos sistemas;

h) para o ID de usuário de administrador genérico, a confidencialidade da informação de autenticação secreta seja mantida quando for compartilhada (por exemplo, mudanças de senhas com frequência e tão logo quanto possível, quando um usuário privilegiado deixa a organização ou muda de função, comunicação entre os usuários privilegiados por meio de mecanismos apropriados).

Informações adicionais

Uso inapropriado de privilégios de administrador de sistemas (qualquer característica ou recursos de sistemas de informação que habilitam usuários a exceder o controle de sistemas ou aplicações) pode ser um grande fator de contribuição para falhas ou violações de sistemas.

9.2.4 Gerenciamento da informação de autenticação secreta de usuários

Controle

Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal.

Diretrizes para implementação

Convém que o processo inclua os seguintes requisitos:

a) solicitar aos usuários a assinatura de uma declaração, para manter a confidencialidade da informação de autenticação secreta e manter as senhas de grupos de trabalho, exclusivamente com os membros do grupo; esta declaração assinada pode ser incluída nos termos e condições da contratação (ver 7.1.2);

b) garantir, onde os usuários necessitam manter suas próprias informações de autenticação secreta, que lhes sejam fornecidas uma informação de autenticação secreta temporária, as quais o usuário é obrigado a alterá-la no primeiro uso;

c) procedimentos sejam estabelecidos para verificar a identidade de um usuário antes de fornecer uma informação de autenticação secreta, temporária, de substituição ou nova;

d) fornecer informação de autenticação secreta temporárias aos usuários de maneira segura; o uso de mensagens de correio eletrônico de terceiros ou desprotegido (texto claro) seja evitado;

e) Informação de autenticação secreta temporária seja única para uma pessoa e que não seja fácil de ser advinhada;

f) os usuários acusem o recebimento da informação de autenticação secreta;

g) as informações de autenticações secretas padrão sejam alteradas logo após a instalação de sistemas ou *software*.

Informações adicionais

Senhas são normalmente usadas como um tipo de informação de autenticação secreta, e é uma forma comum de verificar a identidade de um usuário. Outros tipos de informação de autenticação secreta são chaves criptográficas e outros dados armazenados em tokens (por exemplo, smart cards), que produzem códigos de autenticação.

9.2.5 Análise crítica dos direitos de acesso de usuário

Controle

Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.

Diretrizes para implementação

Convém que a análise crítica dos direitos de acesso considerem as seguintes orientações:

a) os direitos de acesso de usuários sejam revisados em intervalos regulares e depois de quaisquer mudanças, como promoção, remanejamento ou encerramento do contrato (ver 7);

b) os direitos de acesso de usuários sejam analisados criticamente e realocados quando movidos de um tipo de atividade para outra na mesma organização;

c) autorizações para direitos de acesso privilegiado especial sejam revisadas em intervalos mais frequentes.

d) as alocações de privilégios sejam verificadas em intervalo de tempo regular para garantir que privilégios não autorizados não foram obtidos;

e) as modificações para contas privilegadas sejam registradas para análise crítica periódica.

Informações adicionais

Este controle compensa possíveis vulnerabilidades na execução dos controles 9.2.1, 9.2.2 e 9.2.6.

9.2.6 Retirada ou ajuste de direitos de acesso

Controle

Convém que os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades.

Diretrizes para implementação

Convém que, após o encerramento das atividades, os direitos de acesso da pessoa aos ativos associados com os sistemas de informação e serviços sejam removidos ou suspensos. Isto irá determinar se é necessário retirar os direitos de acesso.

As mudanças de uma atividade podem refletir na retirada de todos os direitos de acesso que não foram aprovados para o novo trabalho. Convém que os direitos de acesso que sejam retirados ou adaptados, incluam o acesso lógico e físico.

A remoção ou o ajuste pode ser feito por meio da remoção, revogação ou substituição de chaves, cartões de identificação, recursos de processamento da informação ou subscrições.

Convém que qualquer documentação que identifique os direitos de acesso de funcionários e partes externas reflita a remoção ou ajuste dos direitos de acesso.

Caso o funcionário, fornecedor ou terceiro que esteja saindo tenha conhecimento de senhas de contas que permanecem ativas, convém que estas sejam alteradas após um encerramento das atividades, mudança do trabalho, contrato ou acordo.

Convém que os direitos de acesso aos ativos de informação e aos recursos de processamento da informação sejam reduzidos ou retirados antes que a atividade se encerre ou altere, dependendo da avaliação de fatores de risco, como:

a) se o encerramento da atividade ou a mudança é iniciada pelo funcionário, parte externa ou pelo gestor e a razão do encerramento da atividade;

b) as responsabilidades atuais do funcionário, parte externa ou qualquer outro usuário;

c) o valor dos ativos atualmente acessíveis.

Informações adicionais

Em certas circunstâncias os direitos de acesso podem ser alocados com base no que está sendo disponibilizado para mais pessoas do que as que estão saindo (funcionário, fornecedor ou terceiro), como, por exemplo, grupos de ID. Em tais casos, convém que as pessoas que estão saindo da organização sejam retiradas de quaisquer listas de grupos de acesso e que sejam tomadas providências para avisar aos outros funcionários, fornecedores e terceiros envolvidos para não mais compartilhar esta informação com a pessoa que está saindo.

Nos casos em que o encerramento da atividade seja da iniciativa do gestor, os funcionários, fornecedores ou terceiros descontentes podem deliberadamente corromper a informação ou sabotar os recursos de processamento da informação. No caso de pessoas demitidas ou exoneradas, elas podem ser tentadas a coletar informações para uso futuro.

9.3 Responsabilidades dos usuários

Objetivo: Tornar os usuários responsáveis pela proteção das suas informações de autenticação.

9.3.1 Uso da informação de autenticação secreta

Controle

Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.

Diretrizes para implementação

Convém que todos os usuários sejam informados para:

a) manter a confidencialidade da informação de autenticação secreta, garantindo que ela não é divulgada para quaisquer outras partes, incluindo autoridades e lideranças;

b) evitar manter anotadas a informação de autenticação secreta (por exemplo, papel, arquivos ou dispositivos móveis), a menos que elas possam ser armazenadas de forma segura e o método de armazenamento esteja aprovado (por exemplo, sistema de gerenciamento de senha;

c) alterar a informação de autenticação secreta, sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;

d) Quando as senhas são usadas como informação de autenticação secreta, selecione senhas de qualidade com um tamanho mínimo que sejam:

   1) fáceis de lembrar;

   2) não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;

   3) não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras inclusas no dicionário);

   4) isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;

   5) caso a senha seja temporária, ela deve ser mudada no primeiro acesso (*log-on*)

e) não compartilhar a informação de autenticação secreta de usuários individuais;

f) garantir adequada proteção de senhas quando as senhas são usadas como informação de autenticação secreta em procedimentos automáticos de acesso (*log-on)* e são armazenadas;

g) não utilizar a mesma informação de autenticação secreta para uso com finalidades profissionais e pessoais.

Informações adicionais

O fornecimento de um Simples *Sign On* (SSO) ou outras ferramentas de gerenciamento de informação de autenticação secreta reduz o número de informação de autenticação secreta que os usuários são solicitados a proteger, aumentando dessa forma a eficácia desse controle. Entretanto, estas ferramentas podem também aumentar o impacto da revelação da informação de autenticação secreta.

9.4 Controle de acesso ao sistema e à aplicação

Objetivo: Prevenir o acesso não autorizado aos sistemas e aplicações.

9.4.1 Restrição de acesso à informação

Controle

Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso.

Diretrizes para implementação

Convém que restrições para o acesso sejam baseadas nos requisitos das aplicações individuais do negócio e de acordo com a política de controle de acesso definida.

Convém que os seguintes controles sejam considerados de forma a apoiar os requisitos de restrição de acesso:

a) fornecer *menus* para controlar o acesso às funções dos sistemas de aplicação;

b) controlar quais dados podem ser acessados por um usuário em particular;

c) controlar os direitos de acesso dos usuários, por exemplo, ler, escrever, excluir e executar;

d) controlar os direitos de acesso de outras aplicações;

e) limitar a informação contidas nas saídas;

f) prover controles de acesso lógico ou fisico para o isolamento de aplicações sensíveis, dados de aplicação ou sistemas.

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

Controle

Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema *(log-on*).

Diretrizes para implementação

Convém que uma técnica de autenticação adequada seja escolhida para validar a identificação alegada de um usuário.

Onde é requerida a verificação de identidade e uma forte autenticação, métodos alternativos de autenticação para as senhas, tais como, meios criptográficos, *smart cards*, *tokens* ou biometria, sejam usados.

Convém que o procedimento para entrada no sistema operacional seja configurado para minimizar a oportunidade de acessos não autorizados. Convém que o procedimento de entrada (*log-on*) revele o mínimo de informações sobre o sistema ou aplicação, de forma a evitar o fornecimento de informações desnecessárias a um usuário não autorizado.

Convém que um bom procedimento de entrada no sistema (*log-on*):

a) não mostre identificadores de sistema ou de aplicação até que o processo tenha sido concluído com sucesso;

b) mostre um aviso geral informando que o computador seja acessado somente por usuários autorizados;

c) não forneça mensagens de ajuda durante o procedimento de entrada (*log-on*) que poderiam auxiliar um usuário não autorizado;

d) valide informações de entrada no sistema somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não indique qual parte do dado de entrada está correto ou incorreto;

e) proteja contra tentativas forçadas de entrada no sistema (*log-on*);

f) registre tentativas de acesso ao sistema, sem sucesso e bem sucedida;

g) comunique um evento de segurança caso uma tentativa potencial ou uma violação bem sucedida de entrada no sistema (*log-on*), seja detectada;

h) mostre as seguintes informações quando o procedimento de entrada no sistema (*log-on*) finalizar com sucesso:

   1) data e hora da última entrada no sistema (*log-on*) com sucesso;

   2) detalhes de qualquer tentativa sem sucesso de entrada no sistema (*log-on*) desde o último acesso com sucesso;

i) não mostre a senha que está sendo informada;

j) não transmita senhas em texto claro pela rede;

k) encerre sessões inativas após um período definido de inatividade, especialmente em locais de alto risco, tais como, locais públicos, ou àreas externas ao gerenciamento de segurança da organização ou quando do uso de dispositivos móveis;

l) restrinja os tempos de conexão para fornecer segurança adicional nas aplicações de alto risco e reduzir a janela de oportunidade para acesso não autorizado.

Informações adicionais

Senhas representam uma forma comum de prover identificação e autenticação baseado no segredo de que somente o usuário é quem conhece. Isto também pode ser obtido com protocolos de autenticação e meios criptográficos. Convém que a complexidade de autenticação do usuário seja apropriada para a classificação da informação a ser acessada.

Se as senhas forem transmitidas em texto claro durante o procedimento de entrada no sistema (*log-on*) pela rede, elas podem ser capturadas por um programa de *sniffer* de rede, instalado nela.

9.4.3 Sistema de gerenciamento de senha

Controle

Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.

Diretrizes para implementação

Convém que o sistema de gerenciamento de senha:

a) obrigue o uso individual de ID de usuário e senha para manter responsabilidades;

b) permita que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

c) obrigue a escolha de senhas de qualidade;

d) obrigue os usuários a mudarem as suas senhas temporárias no primeiro acesso ao sistema;

e) force as mudanças de senha a intervalos regulares, conforme necessário;

f) mantenha um registro das senhas anteriores utilizadas e bloquei a reutilização;

g) não mostre as senhas na tela quando forem digitadas;

h) armazene os arquivos de senha separadamente dos dados do sistema da aplicação;

i) armazene e transmita as senhas de forma protegida.

Informações adicionais

Algumas aplicações requerem que senhas de usuário sejam atribuídas por uma autoridade independente. Em alguns casos, as alíneas b), d) e e) das diretrizes acima não se aplicam. Na maioria dos casos, as senhas são selecionadas e mantidas pelos usuários.

9.4.4 Uso de programas utilitários privilegiados

Controle

Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações sejam restrito e estritamente controlado.

Diretrizes para implementação

Convém que as seguintes diretrizes para o uso de utilitários de programa que possam ser capazes de sobrepor os controles dos sistemas e as aplicações, sejam consideradas:

a) uso de procedimentos de identificação, autenticação e autorização para programas utilitários de sistema;

b) segregação de programas utilitários dos *softwares* de aplicação;

c) limitação do uso de programas utilitários a um número mínimo de usuários confiáveis e autorizados (ver 9.2.2);

d) autorização para uso programas utilitários não previstos;

e) limitação da disponibilidade dos programas utilitários, por exemplo para a duração de uma modificação autorizada;

f) registro de todo o uso de programas utilitários;

g) definição e documentação dos níveis de autorização para os programas utilitários;

h) remoção ou desabilitação de todos os programas utilitários desnecessários;

i) não deixar programas utilitários disponíveis para usuários que têm acesso às aplicações nos sistemas onde a segregação de funções é requerida.

Informações adicionais

A maioria das instalações de computadores tem um ou mais programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações.

9.4.5 Controle de acesso ao código-fonte de programas

Controle

Convém que o acesso ao código-fonte de programa seja restrito.

Diretrizes para implementação

Convém que o acesso ao código-fonte de programas e de itens associados (como desenhos, especificações, planos de verificação e de validação) sejam estritamente controlados, com a finalidade de prevenir a introdução de funcionalidade não autorizada e para evitar mudanças não intencionais, bem como para manter a confidencialidade de propriedade intelectual valiosa.

Para os códigos-fonte de programas, este controle pode ser obtido com a guarda centralizada do código, de preferência utilizando bibliotecas de programa-fonte.

É conveniente que as seguintes orientações sejam consideradas para o controle de acesso às bibliotecas de programa-fonte, com a finalidade de reduzir o risco de corrupção de programas de computador:

a) quando possível, convém que seja evitado manter as bibliotecas de programa-fonte no mesmo ambiente dos sistemas operacionais.

b) convém que seja implementado o controle do código-fonte de programa e das bibliotecas de programa-fonte, conforme procedimentos estabelecidos;

c) convém que o pessoal de suporte não tenha acesso irrestrito às bibliotecas de programa-fonte;

d) convém que a atualização das bibliotecas de programa-fonte e itens associados, e a entrega de fontes de programas a programadores seja apenas efetuada após o recebimento da autorização pertinente;

e) As listagens dos programas sejam mantidas num ambiente seguro;

f) convém que seja mantido um registro de auditoria de todos os acessos a código-fonte de programas;

g) convém que a manutenção e a cópia das bibliotecas de programa-fonte estejam sujeitas a procedimentos estritos de controles de mudanças (ver 14.2.2);

Se o código do programa-fonte pretende ser publicado, controles adicionais, para ajudar a garantir a sua integridade (por exemplo, assinatura digital), deve ser considerada.

10 Criptografia

10.1 Controles criptográficos

Objetivo: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

10.1.1 Política para o uso de controles criptográficos

Controle

Convém que seja desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.

Diretrizes para implementação

Quando do desenvolvimento de uma política para criptografia, convém que sejam considerados:

a) a abordagem gerencial quanto ao uso de controles criptográficos em toda a organização, incluindo os princípios gerais sob os quais as informações de negócio sejam protegidas;

b) a identificação do nível requerido de proteção com base em uma avaliação de risco, levando em consideração o tipo, a força e a qualidade do algoritmo de criptografia requerido;

c) o uso de criptografia para a proteção de informações sensíveis transportadas em dispositivos móveis, mídias removiveis ou através de linhas de comunicação;

d) a abordagem do gerenciamento de chaves, incluindo métodos para lidar com a proteção das chaves criptográficas e a recuperação de informações cifradas, no caso de chaves perdidas, comprometidas ou danificadas;

e) papéis e responsabilidades, por exemplo, de quem for responsável:

   1) pela implementação da política;

   2) pelo gerenciamento de chaves, incluindo sua geração (Ver 10.1.2).

f) os padrões a serem adotados para a efetiva implementação ao longo de toda a organização (qual solução é usada para quais processos de negócios);

g) o impacto do uso de informações cifradas em controles que dependem da inspeção de conteúdos (por exemplo, detecção de *códigos maliciosos*).

Convém que sejam consideradas na implementação da política criptográfica da organização, as leis ou regulamentações e restrições nacionais aplicáveis ao uso de técnicas criptográficas, nas diferentes partes do mundo, e das questões relativas ao fluxo transfronteiras de informações cifradas (ver 18.1.5).

Controles criptográficos podem ser usados para alcançar diferentes objetivos de segurança, como por exemplo:

a) confidencialidade: usando a criptografia da informação para proteger informações sensíveis ou críticas, armazenadas ou transmitidas;

b) integridade/autenticidade: usando assinaturas digitais ou códigos de autenticação de mensagens (MAC) para verificar a autenticidade ou integridade de informações sensíveis ou críticas, armazenadas ou transmitidas;

c) não-repúdio: usando técnicas de criptografia para obter evidência da ocorrência ou não ocorrência de um evento ou ação.

d) autenticação: usando técnicas criptográficas para autenticar usuários e outros sistemas que requeiram acesso para transações com usuários de sistemas, entidades e recursos.

Informações adicionais

Convém que a tomada de decisão quanto a uma solução de criptografia ser apropriada, seja vista como parte de processos mais amplos de avaliação de riscos e seleção de controles. Essa avaliação pode, então, ser usada para determinar se um controle criptográfico é apropriado, que tipo de controle convém ser aplicado e para qual propósito e processos de negócio.

Uma política sobre o uso de controles criptográficos é necessária para maximizar os benefícios, minimizar os riscos do uso de técnicas criptográficas e para evitar o uso incorreto ou inapropriado.

Convém que seja buscada a opinião de um especialista para identificar os controles criptográficos adequados para atender os objetivos da Política de Segurança da Informação.

10.1.2 Gerenciamento de chaves

Controle

Convém que uma política sobre o uso, proteção e ciclo de vida das chaves criptográficas, seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.

Diretrizes para implementação

Convém que a política inclua requisitos para o gerenciamento de chaves criptográficas ao longo de todo o seu ciclo de vida incluindo, a geração, armazenagem, arquivo, recuperação, distribuição, retirada e destruição das chaves.

Algoritmos criptográficos, tamanho de chaves e práticas usuais sejam selecionados de acordo com as melhores práticas.

Todas as chaves criptográficas sejam protegidas contra modificação e perda. Adicionalmente, chaves secretas e privadas necessitam de proteção contra o uso ou a divulgação não autorizada.

É recomendável que os equipamentos utilizados para gerar, armazenar e guardar as chaves sejam fisicamente protegidos.

Convém que um sistema de gerenciamento de chaves seja baseado em um conjunto estabelecido de normas, procedimentos e métodos seguros para:

a) gerar chaves para diferentes sistemas criptográficos e diferentes aplicações;

b) gerar e obter certificados de chaves públicas;

c) distribuir chaves para os usuários devidos, incluindo a forma como as chaves são ativadas, quando recebidas;

d) armazenar chaves, incluindo a forma como os usuários autorizados obtêm acesso a elas;

e) mudar ou atualizar chaves, incluindo regras quando as chaves são mudadas e como isto deve ser conduzido;

f) lidar com chaves comprometidas;

g) revogar chaves, incluindo regras de como elas são retiradas ou desativadas, por exemplo quando chaves tiverem sido comprometidas ou quando um usuário deixa a organização (é recomendável, também neste caso, que as chaves sejam guardadas);

h) recuperar chaves perdidas ou corrompidas;

i) realizar cópias de segurança ou guardar as chaves;

j) destruir chaves;

k) manter registro e auditoria das atividades relacionadas com o gerenciamento de chaves;

Para reduzir a possibilidade de comprometimento, convém que as datas de ativação e desativação de chaves sejam definidas de forma que possam ser utilizadas apenas por um período de tempo definido na política de gerenciamento de chaves.

Além do gerenciamento seguro de chaves secretas e privadas, convém que a autenticidade de chaves públicas seja considerada.

Este processo de autenticação pode ser conduzido utilizando-se certificados de chaves públicas que são normalmente emitidos por uma autoridade certificadora, a qual recomenda-se que seja uma organização reconhecida, com controles adequados e procedimentos implantados com o objetivo de garantir o requerido nível de confiança.

Convém que o conteúdo dos termos dos acordos de nível de serviço ou contratos com fornecedores externos de serviços criptográficos, como por exemplo, com uma autoridade certificadora, cubram

aspectos como responsabilidades, confiabilidade dos serviços e tempos de resposta para a execução dos serviços contratados (ver 15.2) .

Informações adicionais

A gestão de chaves criptográficas é essencial para o uso eficaz de técnicas criptográficas. A ISO/IEC 11770 fornece informação adicional sobre a gestão de chaves.

Técnicas criptográficas podem ser também utilizadas para proteger chaves criptográficas. Pode ser necessário o estabelecimento de procedimentos para o manuseio de solicitações legais para acesso a chaves criptográficas, por exemplo, a disponibilização de informação cifrada pode ser requerida em sua forma decifrada para uso como evidência em um processo judicial.

11 Segurança física e do ambiente

11.1 Áreas seguras

Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.

11.1.1 Perímetro de segurança física

Controle

Convém que perímetros de segurança sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis.

Diretrizes para implementação

Convém que as seguintes diretrizes sejam consideradas e implementadas, onde apropriado, para os perímetros de segurança física:

a) convém que os perímetros de segurança sejam claramente definidos e que a localização e a capacidade de resistência de cada perímetro dependam dos requisitos de segurança dos ativos existentes no interior do perímetro, e dos resultados da avaliação de riscos;

b) convém que os perímetros de um edifício ou de um local que contenha as instalações de processamento da informação sejam fisicamente sólidos (ou seja, o perímetro não deve ter brechas nem pontos onde poderia ocorrer facilmente uma invasão); as paredes externas do local devem ser de construção robusta e todas as portas externas sejam adequadamente protegidas contra acesso não autorizado por meio de mecanismos de controle, por exemplo, barras, alarmes, fechaduras etc.; as portas e janelas sejam trancadas quando estiverem sem monitoração, e que uma proteção externa para as janelas seja considerada, principalmente para as que estiverem situadas no andar térreo;

c) convém que seja implantada uma área de recepção, ou um outro meio para controlar o acesso físico ao local ou ao edifício; o acesso aos locais ou edifícios deve ficar restrito somente ao pessoal autorizado;

d) convém que sejam construídas barreiras físicas, onde aplicável, para impedir o acesso físico não autorizado e a contaminação do meio ambiente;

e) convém que todas as portas corta-fogo do perímetro de segurança sejam providas de alarme, monitoradas e testadas juntamente com as paredes, para estabelecer o nível de resistência exigido, de acordo com normas regionais, nacionais e internacionais aceitáveis; elas devem funcionar de acordo com os códigos locais de prevenção de incêndios e prevenção de falhas;

f) convém que sistemas adequados de detecção de intrusos, de acordo com normas regionais, nacionais e internacionais sejam instalados e testados em intervalos regulares, e cubram todas as portas externas e janelas acessíveis; as áreas não ocupadas sejam protegidas por alarmes o tempo todo; também seja dada proteção a outras áreas, por exemplo, salas de computadores ou salas de comunicações;

g) convém que as instalações de processamento da informação gerenciadas pela organização fiquem fisicamente separadas daquelas que são gerenciadas por partes externas.

Informações adicionais

Pode-se obter proteção física criando uma ou mais barreiras físicas ao redor das instalações e dos recursos de processamento da informação da organização. O uso de barreiras múltiplas proporciona uma proteção adicional, uma vez que neste caso a falha de uma das barreiras não significa que a segurança fique comprometida imediatamente.

Uma área segura pode ser um escritório trancável ou um conjunto de salas rodeado por uma barreira física interna contínua de segurança. Pode haver necessidade de barreiras e perímetros adicionais para o controle do acesso físico, quando existem áreas com requisitos diferentes de segurança dentro do perímetro de segurança.

Convém que sejam tomadas precauções especiais para a segurança do acesso físico no caso de edifícios que alojam diversas organizações.

Convém que a aplicação de controles físicos, especialmente para as áreas seguras sejam adaptadas para as circunstâncias técnicas e econoômicas da organização, como definido na avaliação de riscos.

11.1.2 Controles de entrada física

Controle

Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.

Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes:

a) convém que a data e hora da entrada e saída de visitantes sejam registradas, e todos os visitantes sejam supervisionados, a não ser que o seu acesso tenha sido previamente aprovado; as permissões de acesso só sejam concedidas para finalidades específicas e autorizadas, e sejam emitidas com instruções sobre os requisitos de segurança da área e os procedimentos de emergência. A identidade dos visitantes seja autenticada por meios apropriados;

b) convém que o acesso às áreas em que são processadas ou armazenadas informações sensíveis seja restrito apenas ao pessoal autorizado pela implementação de controles de acesso

apropriados, por exemplo, mecanismos de autenticação de dois fatores, como, cartões de controle de acesso e PIN *(personal identification number);*

c) convém que uma trilha de auditoria eletrônica ou um livro de registro físico de todos os acessos seja mantida e monitorada de forma segura;

d) convém que seja exigido que todos os funcionários, fornecedores e partes externas, e todos os visitantes, tenham alguma forma visível de identificação, e que eles avisem imediatamente ao pessoal de segurança, caso encontrem visitantes não acompanhados ou qualquer pessoa que não esteja usando uma identificação visível;

e) Às partes externas que realizam serviços de suporte, convém que seja concedido acesso restrito às áreas seguras ou as instalações de processamento da informação sensíveis, somente quando necessário; este acesso seja autorizado e monitorado;

f) convém que os direitos de acesso a áreas seguras sejam revistos e atualizados em intervalos regulares, e revogados quando necessário (ver 9.2.4 e 9.2.5).

11.1.3 Segurança em escritórios, salas e instalações

Controle

Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.

Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes para proteger escritórios, salas e instalações:

a) convém que as instalações-chave sejam localizadas de maneira a evitar o acesso do público;

b) quando for aplicável, convém que os edifícios sejam discretos com a menor indicação possível da sua finalidade, sem letreiros evidentes, fora ou dentro do edifício, que identifiquem a presença de atividades de processamento de informações;

c) convém que as instalações sejam projetadas para evitar que as informações confidenciais ou as atividades sejam visíveis e possam ser ouvidas da parte externa. Proteção eletromagnética também seja considerado, conforme apropriado.

d) convém que as listas de funcionários e guias telefônicos internos, que identifiquem a localização das instalações que processam informações sensíveis, não fiquem facilmente acessíveis a qualquer pessoal não autorizada.

11.1.4 Proteção contra ameaças externas e do meio-ambiente

Controle

Convém que sejam projetadas e aplicadas proteção física contra desastres naturais, ataques maliciosos ou acidentes.

Diretrizes para implementação

Convém que orientações de especialistas sejam obtidas sobre como evitar danos oriundos de fogo, inundação, terremoto, explosão, manifestações civis e outras formas de desastre natural ou provocado pela natureza.

11.1.5 Trabalhando em áreas seguras

Controle

Convém que seja projetado e aplicado procedimentos para o trabalho em áreas seguras.

Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes:

a) o pessoal só tenha conhecimento da existência de áreas seguras ou das atividades nelas realizadas, apenas se for necessário;

b) seja evitado o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para prevenir as atividades mal intencionadas;

c) as áreas seguras, não ocupadas, sejam fisicamente trancadas e periodicamente verificadas;

d) não seja permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado.

As normas para o trabalho em áreas seguras incluam o controle dos funcionários, fornecedores e partes externas que trabalham em tais áreas, cubram todas as atividades nestas áreas.

11.1.6 Áreas de entrega e de carregamento

Controle

Convém que pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.

Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes:

a) convém que o acesso a uma área de entrega e carregamento a partir do exterior do prédio fique restrito ao pessoal identificado e autorizado;

b) convém que as áreas de entrega e carregamento sejam projetadas de tal maneira que seja possível carregar e descarregar suprimentos sem que os entregadores tenham acesso a outras partes do edifício;

c) convém que as portas externas de uma área de entrega e carregamento sejam protegidas enquanto as portas internas estiverem abertas;

d) Os materiais entregues sejam inspecionados e examinados para detectar a presença de explosivos, materiais químicos ou outros materiais perigosos, antes de serem transportados da área de entrega e carregamento para o local de utilização;

e) convém que os materiais entregues sejam registrados de acordo com os procedimentos de gerenciamento de ativos, por ocasião da sua entrada no local (ver 8);

f) convém que as remessas entregues sejam segregadas fisicamente das remessas que saem, sempre que possível;

g) convém que os materiais entregues sejam inspecionados para evidenciar alteração indevida. Caso alguma alteração indevida seja descoberta, ela deve ser imediatamente notificado ao pessoal da segurança.

11.2 Equipamentos

Objetivo: Impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das operações da organização.

11.2.1 Escolha do local e proteção do equipamento

Controle

Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado.

Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes para proteger os equipamentos:

a) convém que os equipamentos sejam colocados no local, a fim de minimizar o acesso desnecessário às áreas de trabalho;

b) convém que as instalações de processamento da informação que manuseiam dados sensíveis sejam posicionadas cuidadosamente para reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante a sua utilização;

c) convém que as instalações de armazenagem sejam protegidas de forma segura para evitar acesso não autorizado;

d) convém que os itens que exigem proteção especial sejam protegidos para reduzir o nível geral de proteção necessário;

e) convém que sejam adotados controles para minimizar o risco de ameaças físicas potenciais e ambientais, tais como furto, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;

f) convém que sejam estabelecidas diretrizes quanto a comer, beber e fumar nas proximidades das instalações de processamento da informação;

g) convém que as condições ambientais, como temperatura e umidade, sejam monitoradas para a detecção de condições que possam afetar negativamente as instalações de processamento da informação;

h) convém que todos os edifícios sejam dotados de proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;

i) para equipamentos em ambientes industriais, é recomendado considerar o uso de métodos especiais de proteção, como membranas para teclados;

j) convém que os equipamentos que processam informações sensíveis sejam protegidos, a fim de minimizar o risco de vazamento de informações em decorrência de emanações eletromagnéticas.

11.2.2 Utilidades

Controle

Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

Diretrizes para implementação

Convém que todas as utilidades (como suprimento de energia elétrica, telecomunicações, suprimento de água, gás, esgoto, calefação/ventilação e ar-condicionado) :

a) estejam em conformidade com as especificações do fabricante do equipamento e com os requisitos legais da localidade;

b) sejam avaliadas regularmente quanto á sua capacidade para atender ao crescimento do negócio e ás interações com outras utilidades;

c) sejam inspecionadas e testadas regularmente para assegurar o seu adequado funcionamento;

d) seja alarmada para detectar mau funcionamento, quando necessário;

e) tenham múltiplas alimentações com rotas físicas diferentes;

Convém que seja providenciada iluminação e comunicação de emergência. As chaves de emergência (*switches*) e válvulas para o corte de energia, água, gás ou outras utilidades, sejam localizadas próximo das saídas de emergência ou salas de equipamentos.

Informações adicionais

Redundância adicional para conectividade em rede pode ser obtida por meio de múltiplas rotas de mais de um provedor de utilidades.

11.2.3 Segurança do cabeamento

Controle

Convém que o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos.

Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes para a segurança do cabeamento:

a) convém que as linhas de energia e de telecomunicações que entram nas instalações de processamento da informação sejam subterrâneas (ou fiquem abaixo do piso) sempre que possível, ou recebam uma proteção alternativa adequada;

b) convém que os cabos de energia sejam segregados dos cabos de comunicações, para evitar interferências;

c) para sistemas sensíveis ou críticos, convém que os seguintes controles adicionais, sejam considerados:

   1) instalação de conduítes blindados e salas ou caixas trancadas em pontos de inspeção e pontos terminais;

   2) utilização de blindagem eletromagnética para a proteção dos cabos;

   3) realização de varreduras técnicas e inspeções físicas para detectar a presença de dispositivos não autorizados conectados aos cabos;

   4) acesso controlado aos painéis de conexões e às salas de cabos.

11.2.4 Manutenção dos equipamentos

Controle

Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente.

Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes para a manutenção dos equipamentos:

a) convém que a manutenção dos equipamentos seja realizada nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações;

b) convém que a manutenção e os consertos dos equipamentos só sejam realizados por pessoal de manutenção autorizado;

c) convém que sejam mantidos registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas;

d) convém que sejam implementados controles apropriados, na época programada para a manutenção do equipamento, dependendo da manutenção ser realizada pelo pessoal local ou por pessoal externo à organização; onde necessário, informações sensíveis sejam eliminadas do equipamento, ou o pessoal de manutenção seja de absoluta confiança;

e) convém que sejam atendidas todas as exigências de manutenção estabelecidas nas apólices de seguro;

f) antes de colocar o equipamento em operação, após a sua manutenção, convém que ele seja inspecionado para garantir que o equipamento não foi alterado indevidamente e que não está em mau funcionamento.

11.2.5 Remoção de ativos

Controle

Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.

Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes:

a) convém que sejam claramente identificados os funcionários, fornecedores e partes externas que tenham autoridade para permitir a remoção de ativos para fora do local;

b) convém que sejam estabelecidos limites de tempo para a retirada de equipamentos do local, e a devolução seja controlada;

c) Sempre que necessário ou apropriado, é recomendado que seja feito um registro da retirada e da devolução de ativos, quando do seu retorno;

d) convém que a identidade, atribuição e função de qualquer pessoa que manuseia ou utiliza os ativos estejam documentados, e que esta documentação seja devolvida com o equipamento, a informação ou *software*.

Informações adicionais

Podem ser feitas inspeções aleatórias para detectar a retirada não autorizada de ativos e a existência de equipamentos de gravação não autorizados, armas etc., e impedir sua entrada e saída do local. Convém que tais inspeções aleatórias sejam feitas de acordo com a legislação e as normas aplicáveis. Convém que as pessoas sejam avisadas da realização das inspeções, e elas só possam ser feitas com a devida autorização, levando em conta as exigências legais e regulamentares.

11.2.6 Segurança de equipamentos e ativos fora das dependências da organização

Controle

Convém que sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

Diretrizes para implementação

Convém que o uso de qualquer equipamento de processamento e armazenamento de informações fora das dependências da organização seja autorizado pela gerência. Isto se aplica aos próprios equipamentos da organização e aos equipamentos pessoais, usados em nome da organização.

Convém que as seguintes diretrizes sejam adotadas para a proteção de equipamentos usados fora das dependências da organização:

a) convém que os equipamentos e mídias removidos das dependências da organização não fiquem sem supervisão em lugares públicos;

b) convém que sejam observadas a qualquer tempo as instruções do fabricante para a proteção do equipamento, por exemplo, proteção contra a exposição a campos eletromagnéticos intensos;

c) convém que os controles para as localidades fora das dependências da organização, como, o trabalho em casa e localidades remotas e temporárias, sejam determinados por uma avaliação de riscos, devendo ser aplicados controles adequados para cada caso, por exemplo, arquivos trancáveis, política de "mesa limpa", controles de acesso a computadores, e comunicação segura com o escritório (ver também ISO/IEC 27033);

d) quando o equipamento fora das dependências da organização é transferido entre diferentes pessoas ou partes externas, convém que seja mantido um registro para definir a cadeia de custodia do equipamento, incluindo pelo menos os nomes e organizações daqueles que são responsáveis pelo equipamento.

Os riscos de segurança, por exemplo, de danos, furto ou espionagem, podem variar consideravelmente de um local para outro, e convém que sejam levados em conta para determinar os controles mais apropriados.

Informações adicionais

Os equipamentos de armazenagem e processamento de informações incluem todas as formas de computadores pessoais, agendas eletrônicas, telefones celulares, cartões inteligentes, papéis e outros tipos, utilizados no trabalho em casa, ou que são removidos do local normal de trabalho.

Informações adicionais sobre outros aspectos da proteção de dispositivos móveis podem ser encontradas em 6.2.

Recomenda-se evitar o risco, desencorajando os funcionários de trabalharem fora das instalações da organização, ou restringindo o uso de dispositivos móveis.

11.2.7 Reutilização e alienação segura de equipamentos

Controle

Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre-gravados com segurança, antes do descarte ou do seu uso.

Diretrizes para implementação

Convém que os equipamentos sejam inspecionados para verificar se a mídia está ou não armazenada, antes do descarte ou reutilização.

Convém que as mídias de armazenamento que contém informações confidenciais ou de direitos autorais sejam destruídas fisicamente, ou as informações sejam destruídas, apagadas ou sobre-gravadas por meio de técnicas que tornem as informações originais irrecuperáveis, em vez de se usarem as funções-padrão de apagar ou formatar.

Informações adicionais

No caso de dispositivos defeituosos que contenham informações sensíveis, pode ser necessária uma avaliação de riscos para determinar se convém destruir fisicamente o dispositivo em vez de mandá-lo para o conserto ou descartá-lo.

As informações podem ser comprometidas por um descarte feito sem os devidos cuidados ou pela reutilização do equipamento.

Adicionalmente à remoção segura das informações contidas no disco, a encriptação completa do disco reduz o risco de revelação de informação confidencial quando o equipamento é descartado ou reparado considerando que:

a) o processo de encriptação é suficientemente robusto e cobre o disco por completo (incluindo *slack space, swap files*, etc)

b) as chaves criptográficas são de um tamanho considerável para resistir um ataque de força bruta;

c) as chaves criptográficas são guardadas de forma confidencial (por exemplo, nunca armazenada no mesmo disco).

Para orientações adicionais sobre criptografia ver seção 10.

Técnicas para sobregravar de forma segura as mídias armazenadas, diferem em função da tecnologia usada para armazenar a mídia. Convém que ferramentas usadas para sobregravar sejam analisadas criticamente para assegurar que elas são aplicáveis à tecnologia usada para o armazenamento da mídia.

11.2.8 Equipamento de usuário sem monitoração

Controle

Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.

Diretrizes para implementação

Convém que todos os usuários estejam cientes dos requisitos de segurança da informação e procedimentos para proteger equipamentos desacompanhados, assim como suas responsabilidades por implementar estas proteções.

Convém que os usuários sejam informados para:

a) encerrar as sessões ativas, a menos que elas possam ser protegidas por meio de um mecanismo de bloqueio, por exemplo tela de proteção com senha;

b) efetuar a desconexão de serviços de rede ou aplicações, quando não for mais necessário;

c) proteger os computadores ou dispositivos móveis contra uso não autorizado através de tecla de bloqueio ou outro controle equivalente, por exemplo, senha de acesso, quando não estiver em uso.

11.2.9 Política de mesa limpa e tela limpa

Controle

Convém que seja 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..

Diretrizes para implementação

Convém que uma política de mesa limpa e tela protegida leve em consideração a classificação da informação, requisitos contratuais e legais, e o risco correspondente e aspectos culturais da organização. Convém que as seguintes diretrizes sejam consideradas:

a) convém que as informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas, sejam guardadas em lugar seguro (idealmente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando o escritório está desocupado;

b) convém que os computadores e terminais sejam mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por senha, *token* ou mecanismo de autenticação similar quando sem monitoração e protegida por tecla de bloqueio, senhas ou outros controles, quando não usados;

c) convém que sejam evitados o uso não autorizado de fotocopiadoras e outra tecnologia de reprodução (por exemplo, *scanners*, máquinas fotográficas digitais);

d) convém que os documentos que contêm informação sensível ou classificada sejam removidos de impressoras imediatamente.

Informações adicionais

Uma política de mesa limpa e tela protegida reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho. Cofres e outras formas de recursos de armazenamento seguro também podem proteger informações armazenadas contra desastres como incêndio, terremotos, enchentes ou explosão.

Considerar o uso de impressoras com função de código PIN, permitindo dessa forma que os requerentes sejam os únicos que podem pegar suas impressões, e apenas quando estiverem próximas às impressoras.

12 Segurança nas operações

12.1 Responsabilidades e procedimentos operacionais

Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.

12.1.1 Documentação dos procedimentos de operação

Controle

Convém que os procedimentos de operação sejam documentados e disponibilizados a todos os usuários que necessitem deles.

Diretrizes para implementação

Convém que os procedimentos documentados sejam preparados para as atividades operacionais associadas a recursos de processamento de comunicação e informações, tais como procedimentos de inicialização e desligamento de computadores, geração de cópias de segurança (backup), manutenção de equipamentos, tratamento de mídias, segurança e gestão do tratamento das correspondências e das salas de computadores.

É conveniente que os procedimentos de operação especifiquem as instruções, incluindo:

a) a instalação e configuração de sistemas;

b) processamento e tratamento da informação, tanto automática como manual;

c) cópias de segurança (*backup)* (ver 12.3);

d) requisitos de agendamento, incluindo interdependências com outros sistemas, a primeira hora para início da tarefa e a última hora para o término da tarefa;

e) instruções para tratamento de erros ou outras condições excepcionais, que possam ocorrer durante a execução de uma tarefa, incluindo restrições de uso dos utilitários do sistema (ver 9.4.4);

f) contatos para suporte e escalação, incluindo contatos de suporte externos, para o caso de eventos operacionais inesperados ou dificuldades técnicas;

g) instruções quanto ao manuseio de mídias e saídas especiais, tais como o uso de formulários especiais ou o gerenciamento de dados confidenciais, incluindo procedimentos para o descarte seguro de resultados provenientes de rotinas com falhas (ver 8.3 e11.2.7);

h) procedimento para o reinício e recuperação em caso de falha do sistema;

i) gerenciamento de trilhas de auditoria e informações de registros (*logs*) de sistemas (ver 12.4);

j) procedimentos de monitoramento (ver 12.4).

Convém que os procedimentos operacionais e os procedimentos documentados para atividades de sistemas sejam tratados como documentos formais e as mudanças sejam autorizadas pela direção. Quando tecnicamente possível, sistemas de informação sejam gerenciados uniformemente, usando os mesmos procedimentos, ferramentas e utilitários.

12.1.2 Gestão de mudanças

Controle

Convém que mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas.

Diretrizes para implementação

Convém que os seguintes itens em particular, sejam considerados:

a) identificação e registro das mudanças significativas;

b) planejamento e testes das mudanças;

c) avaliação de impactos potenciais, incluindo impactos de segurança da informação, de tais mudanças;

d) procedimento formal de aprovação das mudanças propostas;

e) verificação de que os requisitos de segurança da informação foram atendidos;

f) comunicação dos detalhes das mudanças para todas as pessoas relevantes;

g) procedimentos de recuperação, incluindo procedimentos e responsabilidades para interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

h) provisão de um processo emergencial de mudança para permitir uma implementação rápida e controlada de mudanças, necessárias para resolver um incidente (ver 16.1).

Convém que sejam estabelecidos procedimentos e responsabilidades de gestão formais para garantir que haja um controle satisfatório de todas as mudanças. Quando mudanças forem realizadas, é conveniente manter um registro de auditoria contendo todas as informações relevantes.

Informações adicionais

O controle inadequado de modificações nos sistemas e nos recursos de processamento das informações é uma causa comum de falhas de segurança ou de sistema. Mudanças em ambientes operacionais, especialmente quando da transferência de um sistema em desenvolvimento para o estágio operacional, podem trazer impactos à confiabilidade de aplicações (ver 14.2.2).

12.1.3 Gestão de capacidade

Controle

Convém que a utilização dos recursos seja monitorada e ajustada e as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.

Diretrizes para implementação

Convém que requisitos de capacidade sejam identificados levando-se em conta a criticidade do negócio do sistema em questão. Que o ajuste e monitoramento dos sistemas sejam aplicados para garantir e, quando necessário, melhorar a disponibilidade e eficiência dos sistemas. É recomendável que os controles detectivos sejam implantados para identificar problemas em tempo hábil. É conveniente que projeções de capacidade futura levem em consideração os requisitos de novos

negócios e sistemas e as tendências atuais e projetadas de capacidade de processamento de informação da organização.

Atenção particular precisa ser dada a qualquer recurso que possua um ciclo de renovação longo ou custos alto, sendo responsabilidade dos gestores monitorar a utilização dos recursos-chave dos sistemas. Convém que eles identifiquem as tendências de utilização, particularmente em relação às aplicações do negócio ou às ferramentas de gestão de sistemas de informação.

Convém que os gestores utilizem essas informações para identificar e evitar os potenciais gargalos e a dependência em pessoas-chave que possam representar ameaças à segurança dos sistemas ou aos serviços, e planejar ação apropriada.

O fornecimento de capacidade suficiente pode ser obtido por meio do aumento de capacidade ou pela redução da demanda. Exemplos de gerenciamento da demanda de capacidade incluem:

a) exclusão de dados obsoletos (espaço em disco);

b) desativação de aplicações, sistemas, bases de dados ou ambientes;

c) otimização das programações e dos processos de lote;

d) otimização da lógica de aplicação ou das consultas à base de dados;

e) negar ou restringir a largura da banda para serviços que demandam muitos recursos se estes não são críticos ao negócio (por exemplo *streaming* de vídeo).

Um plano documentado da gestão de capacidade convém ser considerado para os sistemas de missão crítica.

Informações adicionais

Este controle também considera a capacidade dos recursos humanos, bem como dos escritórios e instalações.

12.1.4 Separação dos ambientes de desenvolvimento, teste e de produção

Controle

Convém que ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

Diretrizes para implementação

Convém que o nível de separação dos ambientes de produção, testes e desenvolvimento, que é necessário para prevenir problemas operacionais, seja identificado e os controles apropriados sejam implementados.

Convém que os seguintes itens sejam considerados:

a) convém que as regras para a transferência de *software* do ambiente de desenvolvimento para o de produção sejam definidas e documentadas;

b) convém que o *software* em desenvolvimento e o *software* em produção sejam, sempre que possível, executados em diferentes sistemas ou processadores e em diferentes domínios ou diretórios;

c) convém que as mudanças nas aplicações e nos sistemas operacionais sejam testadas em um ambiente de teste ou projeto piloto, antes de ser aplicado aos sistemas operacionais.

d) convém que os testes não sejam realizados nos sistemas operacionais, exceto em circunstâncias excepcionais;

e) convém que os compiladores, editores e outras ferramentas de desenvolvimento ou utilitários de sistemas não sejam acessíveis aos sistemas operacionais, quando não for necessário;

f) convém que os usuários tenham diferentes perfis para sistemas em testes e em produção, e que os *menus* mostrem mensagens apropriadas de identificação para reduzir o risco de erro;

g) convém que os dados sensíveis não sejam copiados para os ambientes de testes, a menos que controles equivalentes sejam fornecidos para o sistema de teste (ver 14.3).

Informações adicionais

As atividades de desenvolvimento e teste podem causar sérios problemas, como, por exemplo, modificações inesperadas em arquivos ou no ambiente dos sistemas, ou falhas de sistemas. Nesse caso, é necessária a manutenção de um ambiente conhecido e estável, no qual possam ser executados testes significativos e que seja capaz de prevenir o acesso indevido do pessoal de desenvolvimento ao ambiente operacional.

Quando o pessoal de desenvolvimento e teste possui acesso ao sistema operacional e suas informações, estes podem introduzir códigos não autorizados e não testados, ou mesmo alterar os dados de produção. Em alguns sistemas essa capacidade pode ser mau utilizada para a execução de fraudes ou introdução de códigos maliciosos ou não testados, que podem causar sérios problemas operacionais.

O pessoal de desenvolvimento e testes também representa uma ameaça à confidencialidade das informações de produção. As atividades de desenvolvimento e teste podem causar modificações não intencionais no *software* ou nas informações se eles compartilharem o mesmo ambiente computacional. A separação dos ambientes de desenvolvimento, teste e produção é, portanto, desejável para reduzir o risco de modificações acidentais ou acessos não autorizados aos sistemas operacionais e aos dados do negócio (ver 14.3 para a proteção de dados de teste).

12.2 Proteção contra códigos maliciosos

Objetivo: Assegurar que as informações e os recursos de processamento da informação estão protegidos contra códigos maliciosos.

12.2.1 Controles contra códigos maliciosos

Controle

Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário.

Diretrizes para implementação

Convém que a proteção contra códigos maliciosos seja baseada em *softwares* de detecção e resposta a códigos maliciosos, na conscientização da segurança da informação, no controle de acesso adequado e nos controles de gerenciamento de mudanças. Recomenda-se que os seguintes controles sejam considerados:

a) estabelecer uma política formal proibindo o uso de *softwares* não autorizados (ver 12.6.2 e 14.2);

b) implementar controles para prevenir ou detectar o uso de *softwares* não autorizado (por exemplo *whitelisting*, ou seja, uma lista de softwares permitidos a acessar o sistema);

c) implementar controles para prevenir ou detectar o uso de websites maliciosos, suspeitos ou conhecidos (por exemplo *blacklisting*, ou seja, uma lista de softwares permitidos a acessar o sistema);

d) estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e *softwares*, seja de redes externas, ou por qualquer outro meio, indicando as medidas preventivas a serem adotadas;

e) reduzir vulnerabilidades que possam ser exploradas por códigos maliciosos, por exemplo por meio do gerenciamento de vulnerabilidades técnicas (ver 12.6);

f) conduzir análises críticas regulares dos *softwares* e dados dos sistemas que suportam processos críticos de negócio; convém que a presença de quaisquer arquivos não aprovados ou atualização não autorizada seja formalmente investigada;

g) instalar e atualizar regularmente *softwares* de detecção e remoção de códigos maliciosos para o exame de computadores e mídias magnéticas, de forma preventiva ou de forma rotineira; convém que as verificações realizadas incluam:

   1) varredura, antes do uso, da existência de códigos maliciosos nos arquivos recebidos por meio de redes ou em qualquer mídia de armazenamento;

   2) verificação, antes do uso, da existência de *software* malicioso em qualquer arquivo recebido através de correio eletrônico ou importado (*download*). Essa avaliação pode ser feita em diversos locais, como, por exemplo, nos servidores de correio eletrônico, nos computadores pessoais ou quando da sua entrada na rede da organização;

   3) verificação da existência de códigos maliciosos em páginas *web*;

h) definir procedimentos e responsabilidades para tratar da proteção de código malicioso nos sistemas, treinamento nesses procedimentos, reporte e recuperação de ataques de códigos maliciosos (*códigos maliciosos*);

i) preparar planos de continuidade do negócio adequados para a recuperação em caso de ataques por códigos maliciosos, incluindo todos os procedimentos necessários para recuperação e cópia dos dados e *softwares* (ver 12.3);

j) implementar procedimentos para coletar regularmente informações, através por exemplo, de assinaturas de listas de discussão e visitas a *sites* informativos sobre novos códigos maliciosos;

k) implementar procedimentos para verificar a informação relacionada a códigos maliciosos e garantir que os boletins com alertas sejam precisos e informativos; Convém que os gestores garantam que fontes qualificadas, como, por exemplo, jornais com reputação idônea, *sites* confiáveis ou fornecedores de *software* de proteção contra códigos maliciosos, sejam utilizadas para diferenciar boatos de notícias reais sobre códigos maliciosos; convém que todos os usuários estejam cientes dos problemas decorrentes de boatos e estejam capacitados a lidar com eles;

l) isolar os ambientes onde impactos catastróficos possam ser gerados.

Informações adicionais

A utilização de dois ou mais tipos de *software* de controle contra códigos maliciosos de diferentes fornecedores e tecnologias no ambiente de processamento da informação pode aumentar a eficácia na proteção contra códigos maliciosos.

Convém que seja tomado cuidado para proteção contra a introdução de códigos maliciosos durante manutenções e procedimentos de emergência, os quais podem ultrapassar os controles comuns de proteção contra códigos maliciosos.

Sob certas condições, a proteção contra códigos maliciosos pode causar perturbação nas operações.

O uso isolado de *softwares* de reparação e detecção contra códigos maliciosos não é usualmente adequado e geralmente necessita ser acompanhado de procedimentos operacionais que previnam a introdução de códigos maliciosos.

12.3 Cópias de segurança

Objetivo: Proteger contra a perda de dados.

12.3.1 Cópias de segurança das informações

Controle

Convém que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

Diretrizes para implementação

Convém que a política de *backup* seja estabelecida para definir os requisitos da organização relativos às cópias de segurança das informações, dos softwares e dos sistemas.

Convém que a política de *backup* defina os requisitos para proteção e retenção.

Convém que os recursos adequados para a geração de cópias de segurança sejam disponibilizados para garantir que toda informação e *software* essenciais possam ser recuperados após um desastre ou a falha de uma mídia.

Quando da elaboração de um plano de *backup*, convém que os seguintes itens sejam levados em consideração:

a) registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação, os quais convém que sejam produzidos;

b) a abrangência (por exemplo, completa ou diferencial) e a freqüência da geração das cópias de segurança reflitam os requisitos de negócio da organização, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização;

c) convém que as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;

d) convém que seja dado um nível apropriado de proteção física e ambiental das informações das cópias de segurança (ver 11), consistentes com as normas aplicadas na instalação principal;

e) convém que as mídias de *backup* sejam regularmente testadas para garantir que elas são confiáveis no caso do uso emergencial; Convém que isto seja combinado com um teste de restauração e checado contra o tempo de restauração requerido. Convém que os testes da capacidade para restaurar os dados copiados sejam realizados em uma mídia de teste dedicada, não sobrepondo a mídia original, no caso em que o processo de restauração ou *backup* falhe e cause irreparável dano ou perda dos dados;

f) em situações onde a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Convém que cópias de segurança de sistemas e serviços específicos sejam testadas regularmente para garantir que elas estão aderentes aos requisitos definidos nos planos de continuidade do negócio. Para serviços e sistemas críticos, convém que sejam criados mecanismos de geração de cópias de segurança que abranjam todos os sistemas de informação, aplicações e dados necessários para a completa recuperação do sistema em um evento de desastre.

O período de retenção para informações essenciais ao negócio e também qualquer requisito para que cópias de arquivo sejam permanentemente retidas, coném que seja determinado.

12.4 Registros e monitoramento

Objetivo: Registrar eventos e gerar evidências.

12.4.1 Registros de eventos

Controle

Convém que registros *(log*) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.

Diretrizes para implementação

Convém que os registros *(log)* de eventos incluam, quando relevante:

a) identificação dos usuários (ID);

b) atividades do sistema;

c) datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (*log-on*) e saída (*log-off*) no sistema;

d) identidade do dispositivo ou sua localização quando possível e o identificador do sistema;

e) registros das tentativas de acesso ao sistema, aceitas e rejeitadas;

f) registros das tentativas de acesso a outros recursos e dados, aceitos e rejeitados;

g) alterações na configuração do sistema;

h) uso de privilégios;

i) Uso de aplicações e utilitários do sistema;

j) arquivos acessados e o tipo de acesso;

k) endereços e protocolos de rede;

l) alarmes provocados pelo sistema de controle de acesso;

m) ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção de intrusos;

n) registros de transações executadas pelos usuários nas aplicações.

Os registros de eventos estabelecem o fundamento para os sistemas de monitoramento automáticos, os quais são capazes de gerar relatórios consolidados e alertas na segurança do sistema.

Informações adicionais

Os registros (*log*) de eventos podem conter dados confidenciais e informação de identificação pessoal. Convém que medidas apropriadas de proteção de privacidade sejam tomadas (ver 18.1.4).

Quando possível, convém que os administradores de sistemas não tenham permissão de exclusão ou desativação dos registros (*log*) de suas próprias atividades (ver 12.4.3).

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

Controle

Convém que as informações dos registros de eventos (log) e seus recursos sejam protegidas contra acesso não autorizado e adulteração.

Diretrizes para implementação

Convém que os controles implementados objetivem a proteção contra modificações não autorizadas às informações dos (logs) e problemas operacionais com os recursos dos registros (log), tais como:

a) alterações dos tipos de mensagens que são gravadas;

b) arquivos de registros (*log*) sendo editados ou excluídos;

c) capacidade de armazenamento da mídia magnética do arquivo de registros (*log*) excedida, resultando em falhas no registro de eventos ou sobreposição do registro de evento anterior.

Alguns registros (*log*) de auditoria podem ser guardados como parte da política de retenção de registros ou devido aos requisitos para a coleta e retenção de evidência (ver 16.1.7).

Informações adicionais

Registros (*logs*) de sistema frequentemente contêm um grande volume de informações, muitas das quais não dizem respeito ao monitoramento de segurança da informação. Para ajudar a identificar eventos significativos para o propósito de monitoramento de segurança da informação, convém considerar que seja feita a cópia automática dos tipos apropriados de mensagens para um segundo registro, ou que sejam utilizados utilitários de sistemas adequados ou ferramentas de auditoria para realizar a racionalização e investigação do arquivo.

Registros (*log*) de sistema precisam ser protegidos, porque se os dados forem modificados ou excluídos, a sua existência pode gerar a falsa sensação de segurança. A cópia de registros em tempo real para um sistema fora do controle do administrador ou operador do sistema pode ser utilizada como salvaguarda para os registros.

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

Controle

Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares.

Diretrizes para implementação

As pessoas que possuem conta de usuário privilegiado podem ser capazes de manipular os registros (logs) nos recursos de processamento da informação que estão sob o seu controle direto, sendo portanto necessário proteger e analisar criticamente os registros (logs) para manter o controle dos usuários privilegiados.

Informações adicionais

Um sistema de detecção de intrusos gerenciado fora do controle dos administradores de rede e de sistemas pode ser utilizado para monitorar a conformidade das atividades dos administradores dos sistemas e de rede.

12.4.4 Sincronização dos relógios

Controle

Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa.

Diretrizes para implementação

Convém que requisitos internos e externos relativos à exatidão, sincronização e tempo de representação sejam documentados. Tais requisitos podem ser legais, regulatórios, contratuais de

conformidade com normas ou requisitos para monitoramento interno. Um tempo padrão de referência para uso dentro da organização, pode ser definido.

Convém que a abordagem da organização para obter o tempo de referência de uma fonte externa e, como sincronizar, de forma confiável os relógios internos, seja documentada e implementada.

Informações adicionais

O ajuste correto dos relógios dos computadores é importante para garantir a exatidão dos registros (*log*) de auditoria, que podem ser requeridos para investigações ou como evidências em casos legais ou disciplinares. Registros (*log*) de auditoria incorretos podem dificultar tais investigações e causar danos à credibilidade dessas evidências. Um relógio interno ligado ao relógio atômico nacional via transmissão de rádio pode ser utilizado como relógio principal para os sistemas de registros (*logging*). O protocolo de hora da rede pode ser utilizado para sincronizar todos os relógios dos servidores com o relógio principal.

12.5 Controle de software operacional

Objetivo: Assegurar a integridade dos sistemas operacionais.

12.5.1 Instalação de software nos sistemas operacionais

Controle

Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados.

Diretrizes para implementação

Convém que as seguintes diretrizes sejam consideradas para controlar as mudanças de *software* em sistemas operacionais:

a) convém que as atualizações do *software* operacional, aplicativos e bibliotecas de programas sejam executadas por administradores treinados e com autorização gerencial apropriada (ver 9.4.5);

b) convém que os sistemas operacionais somente contenham código executável e aprovado, e não contenham códigos em desenvolvimento ou compiladores;

c) convém que sistemas operacionais e aplicativos somente sejam implementados após testes extensivos e bem sucedidos; é recomendável que os testes incluam testes sobre uso, segurança, efeitos sobre outros sistemas como também sobre uso amigável, e sejam realizados em sistemas separados (ver 12.1.4); Convém que seja assegurado que todas as bibliotecas de código fonte dos programas correspondentes tenham sido atualizadas;

d) convém que um sistema de controle de configuração seja utilizado para manter controle da implementação do *software* assim como da documentação do sistema;

e) convém que uma estratégia de retorno às condições anteriores seja disponibilizada antes que mudanças sejam implementadas no sistema;

f) convém que um registro de auditoria seja mantido para todas as atualizações das bibliotecas dos programas operacionais;

g) convém que versões anteriores dos *softwares* aplicativos sejam mantidas como medida de contingência;

h) convém que versões antigas de *software* sejam arquivadas, junto com todas as informações e parâmetros requeridos, procedimentos, detalhes de configurações, e *software* de suporte durante um prazo igual ao prazo de retenção dos dados;

É recomendável que *software* adquirido de fornecedores e utilizado em sistemas operacionais seja mantido em um nível apoiado pelo fornecedor. Ao transcorrer o tempo, fornecedores de *software* cessam o apoio às versões antigas do *software*. É recomendado que a organização considere os riscos associados à dependência de *software* sem suporte.

Convém que qualquer decisão de atualização para uma nova versão considere os requisitos do negócio para a mudança, e da segurança associada por exemplo,a introdução de uma nova funcionalidade de segurança da informação ou a quantidade e a gravidade dos problemas de segurança da informação associados a esta versão.

Convém que os pacotes de correções de *software* sejam aplicados quando puderem remover ou reduzir as vulnerabilidades de segurança da informação (ver 12.6).

É recomendado que acessos físicos e lógicos sejam concedidos a fornecedores, somente quando necessário, com a finalidade de suporte e com aprovação gerencial. Convém que as atividades do fornecedor sejam monitoradas (ver 15.2.1).

Softwares para computadores podem depender de outros *softwares* e módulos fornecidos externamente, os quais convém que sejam monitorados e controlados para evitar mudanças não autorizadas, que podem introduzir fragilidades na segurança.

12.6 Gestão de vulnerabilidades técnicas

Objetivo: Prevenir a exploração de vulnerabilidades técnicas.

12.6.1 Gestão de vulnerabilidades técnicas

Controle

Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.

Diretrizes para implementação

Um inventário completo e atualizado dos ativos de informação (ver 8) é um pré-requisito para uma gestão efetiva de vulnerabilidade técnica. Informação especifica para o apoio à gestão de vulnerabilidade técnica inclui o fornecedor de *software*, o número da versão, o status atual de desenvolvimento (por exemplo, quais *softwares* estão instalados e em quais sistemas), e a(s) pessoa(s) na organização responsável (is) pelos *softwares*.

Convém que seja tomada ação apropriada, no devido tempo, como resposta às potenciais vulnerabilidades técnicas identificadas. É recomendável que as seguintes diretrizes sejam seguidas para o estabelecimento de um processo de gestão efetivo de vulnerabilidades técnicas:

a) convém que a organização defina e estabeleça as funções e responsabilidades associadas na gestão de vulnerabilidades técnicas, incluindo o monitoramento de vulnerabilidades, a avaliação de risco de vulnerabilidades, correções, acompanhamento dos ativos e qualquer responsabilidade de coordenação requerida;

b) convém que os recursos de informação a serem usados para identificar vulnerabilidades técnicas relevantes e para manter a conscientização sobre os mesmos, sejam identificados, para *softwares* e outras tecnologias (baseado na lista de inventário dos ativos, ver 8.1.1); convém que esses recursos de informação sejam mantidos atualizados com base nas mudanças no inventário de ativos, ou quando outros recursos novos ou úteis sejam encontrados;

c) convém que seja definido um prazo para a reação a notificações de potenciais vulnerabilidades técnicas relevantes;

d) uma vez que uma vulnerabilidade técnica potencial tenha sido identificada, convém que a organização avalie os riscos associados e as ações a serem tomadas; tais ações podem requerer o uso de emendas de correções (*patches*) nos sistemas vulneráveis e/ou a aplicação de outros controles;

e) dependendo da urgência exigida para tratar uma vulnerabilidade técnica, convém que a ação a ser tomada esteja em acordo com os controles relacionados com a gestão de mudanças (ver 12.1.2) ou que sejam seguidos os procedimentos de resposta a incidentes de segurança da informação (ver 16.1.5).

f) se uma correção é disponibilizada, convém que sejam avaliados os riscos associados à sua instalação (convém que os riscos associados à vulnerabilidade sejam comparados com os riscos de instalação da correção);

g) convém que as emendas (*patches*) sejam testadas e avaliadas antes de serem instaladas para assegurar a efetividade e que não tragam efeitos que não possam ser tolerados; quando não existir a disponibilidade de uma emenda de correção, convém considerar o uso de outros controles, como:

   1) a desativação de serviços ou potencialidades relacionadas à vulnerabilidade;

   2) a adaptação ou a agregação de controles de acesso, por exemplo *firewalls* nas fronteiras da rede (ver 13.1);

   3) o aumento do monitoramento para detectar ou prevenir ataques reais;

   4) o aumento da conscientização sobre a vulnerabilidade.

h) convém que seja mantido um registro de auditoria de todos os procedimentos realizados;

i) com a finalidade de assegurar a eficácia e a eficiência, convém que processo de gestão de vulnerabilidades técnicas seja monitorado e avaliado regularmente;

j) recomenda-se contemplar em primeiro lugar os sistemas com altos riscos;

k) convém que um processo de gestão de vulnerabilidade técnica eficaz esteja alinhado com as atividades de gestão de incidentes, para comunicar dados sobre as vulnerabilidades, às funções de resposta a incidentes e fornecer procedimentos técnicos no caso em que ocorra um incidente.

l) convém que seja definido um procedimento para contemplar a situação onde uma vulnerabilidade tenha sido identificada e não existam controles adequados. Nesta situação, convém que a organização avalie os riscos relativos à vulnerabilidade conhecida e defina correções e ações corretivas apropriadas.

Informações adicionais

A gestão de vulnerabilidades técnicas pode ser vista como uma subfunção da gestão de mudanças e, como tal, pode aproveitar os procedimentos e processos da gestão de mudanças (ver 12.1.2 e 14.2.2).

Fornecedores estão frequentemente sob grande pressão para liberar correções o mais breve possível. Portanto, existe a possibilidade de uma correção não resolver o problema adequadamente e causar efeitos colaterais negativos. Também, em alguns casos, a desinstalação de uma correção pode não ser facilmente obtida após sua instalação.

Quando testes adequados de correção não forem possíveis, por exemplo, devido a custos ou falta de recursos, um atraso na aplicação da correção pode ser considerado para avaliar os riscos associados, baseados nas experiências relatadas por outros usuários. O uso da ISO/IEC 27031 pode ser benéfico.

12.6.2 Restrições quanto à instalação de software

Controle

Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de *software* pelos usuários.

Diretrizes para implementação

Convém que a organização defina e crie uma política mandatória e restrita, sobre quais os tipos de software os usuários podem instalar.

Convém que o princípio do privilégio mínimo seja aplicado. Se certos privilégios são concedidos, os usuários podem ter a capacidade de instalar *software.*

Convém que a organização identifique quais os tipos de *software* são permitidos instalar (por exemplo, atualização e segurança de patches ao *software* existente), e quais tipos de instalações são proibidas (por exemplo, *software* que é usado somente para fins pessoais e *software* cuja possibilidade de ser potencialmente malicioso, é desconhecida ou suspeita).

Convém que estes privilégios sejam concedidos aos usuários pertinentes.

Informações adicionais

A instalação de *software* não controlada em dispositivos computadorizados pode introduzir vulnerabilidades e em seguida gerar o vazamento de informações, perda de integridade ou outros incidentes de Segurança da Informação além da violação de direitos de propriedade intelectual.

12.7 Considerações quanto à auditoria de sistemas de informação

Objetivo: Minimizar o impacto das atividades de auditoria nos sistemas operacionais.

12.7.1 Controles de auditoria de sistemas de informação

Controle

Convém que os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.

Diretrizes para implementação

Convém que as seguintes diretrizes sejam observadas:

a) convém que os requisitos de auditoria para acesso aos sistemas e dados sejam acordados com o nível apropriado da gerência;

b) convém que o escopo dos testes técnicos da auditoria seja acordado e controlado;

c) convém que os testes de auditoria sejam limitados ao acesso somente para leitura de *software* e dados;

d) convém que os outros acessos diferentes de apenas leitura sejam permitidos somente através de cópias isoladas dos arquivos do sistema, as quais recomenda-se que sejam apagadas ao final da auditoria, ou dada proteção apropriada quando existir uma obrigação para guardar tais arquivos como requisitos da documentação da auditoria;

e) convém que os requisitos para processamento adicional ou especial sejam identificados e acordados; os testes de auditoria que possam afetar a disponibilidade do sistema seja realizado fora do horário normal de trabalho;

f) convém que todo o acesso seja monitorado e registrado de forma a produzir uma trilha de referência.

13 Segurança nas comunicações

13.1 Gerenciamento da segurança em redes

Objetivo: Garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.

13.1.1 Controles de redes

Controle

Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

Diretrizes para implementação

Convém que controles sejam implementados para garantir a segurança da informação nestas redes, e a proteção dos serviços a elas conectadas, de acesso não autorizado. Em particular, convém que os seguintes itens sejam considerados:

a) convém que responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede sejam estabelecidos;

b) convém que a responsabilidade operacional pelas redes seja separada da operação dos recursos computacionais, onde apropriado (ver 6.1.1);

c) convém que controles especiais sejam estabelecidos para proteção da confidencialidade e integridade dos dados que trafegam sobre redes públicas ou sobre as redes sem fio (*wireless*) e proteger os sistemas e aplicações a elas conectadas (ver 10 e 13.2); controles especiais podem também ser requeridos para manter a disponibilidade dos serviços e computadores conectados;

d) convém que sejam aplicados mecanismos apropriados de registro e monitoração para habilitar a gravação e detecção de ações que possam afetar, ou ser relevante para a segurança da informação;

e) convém que atividades de gerenciamento sejam coordenadas para otimizar os serviços para a organização e assegurar que os controles estão aplicados de forma consistente sobre toda a infraestrutura de processamento da informação;

f) convém que sistemas sobre as redes sejam autenticados;

g) convém que a conexão de sistemas à rede seja restrita.

Informações adicionais

Informações adicionais sobre segurança em rede pode ser encontrada na ISO / IEC 27033.

13.1.2 Segurança dos serviços de rede

Controle

Convém que mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede, sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.

Diretrizes para implementação

Convém que a capacidade do provedor dos serviços de rede para gerenciar os serviços acordados de maneira segura, seja determinada e monitorados regularmente, bem como o direito de auditá-los seja acordado.

É conveniente que as definições de segurança necessárias para serviços específicos, como características de segurança, níveis de serviço e requisitos de gerenciamento sejam identificadas. Convém que a organização assegure que os provedores dos serviços de rede implementam estas medidas.

Informações adicionais

Serviços de rede incluem o fornecimento de conexões, serviços de rede privados, redes de valor agregado e soluções de segurança de rede gerenciadas como *firewalls* e sistemas de detecção de intrusos.

Estes serviços podem abranger desde o simples fornecimento de banda de rede não gerenciada até complexas ofertas de soluções de valor agregado.

Funcionalidades de segurança de serviços de rede podem ser:

a) tecnologias aplicadas para segurança de serviços de redes como autenticação, encriptação e controles de conexões de rede;

b) parâmetros técnicos requeridos para uma conexão segura com os serviços de rede de acordo com as regras de conexão de redes e segurança;

c) procedimentos para o uso de serviços de rede para restringir o acesso a serviços de rede ou aplicações, onde for necessário.

13.1.3 Segregação de redes

Controle

Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.

Diretrizes para implementação

Um método de controlar a segurança da informação em grandes redes é dividir em diferentes domínios de redes. Os domínios podem ser escolhidos baseado no nível de confiança (por exemplo, domínio de acesso público, domínio de estação de trabalho, domínio de servidor), em todas as áreas da organização (por exemplo, RH, financeiro, marketing). A segregação pode ser feita, tanto usando diferentes redes físicas ou usando diferentes redes lógicas (por exemplo, VPN).

Convém que o perímetro de cada domínio seja bem definido. O acesso entre os domínios de rede é permitido, porém é recomendado que seja controlado no perímetro por meio do uso de um *gateway* (por exemplo, *firewall*, roteador de filtro). Convém que o critério para segregação de redes em domínios e o acesso permitido através dos *gateways* seja baseado em uma avaliação dos requisitos de segurança da informação de cada domínio.

Convém que a avaliação seja feita de acordo com a política de controle de acesso (ver 9.1.1), os requisitos de acesso, o valor e a classificação da informação processada, e que leve em conta o impacto no desempenho e no custo da incorporação da tecnologia *gateway*, adequada.

Redes *wireless* requerem tratamento especial devido ao perímetro de rede definido ser fraco. Convém que, para ambientes sensíveis, consideração seja dada para tratar todos os acessos *wireless* como conexão externa (ver 9.4.2) e segregar esse acesso das redes internas, até que o acesso tenha passado por um *gateway,* baseado na política de controle de redes (ver 13.1.1), antes de conceder o acesso aos sistemas internos.

Autenticação, encriptação e as normas modernas de tecnologia de níveis de controle de acesso do usuário a rede, baseadas nas redes *wireless* podem ser suficientes para controlar a conexão com a rede interna da organização, quando implementado adequadamente.

Informações adicionais

Redes estão sendo progressivamente estendidas além dos limites organizacionais tradicionais, tendo em vista as parcerias de negócio que são formadas e que podem requerer a interconexão ou compartilhamento de processamento de informação e recursos de rede. Tais extensões podem aumentar o risco de acesso não autorizado aos sistemas de informação existentes que usam a rede, e alguns dos quais podem requerer proteção de outros usuários de rede por causa da sensibilidade ou criticidade.

13.2 Transferência de informação

Objetivo: Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

13.2.1 Políticas e procedimentos para transferência de informações

Controle

Convém que políticas, procedimentos e controles de transferências formais, sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.

Diretrizes para implementação

Convém que procedimentos e controles estabelecidos para a troca de informações em recursos eletrônicos de comunicação considerem os tópicos a seguir:

a) procedimentos para proteger a informação transferida contra interceptação, cópia, modificação, desvio e destruição;

b) procedimentos para detecção e proteção contra código malicioso que pode ser transmitido através do uso de recursos eletrônicos de comunicação (ver 12.2.1);

c) procedimentos para proteção de informações eletrônicas sensíveis que sejam transmitidas na forma de anexos;

d) política ou diretrizes que especifiquem o uso aceitável dos recursos eletrônicos de comunicação (ver 8.1.3);

e) que as responsabilidades de funcionários, fornecedores e partes externas possam comprometer a organização através de, por exemplo, difamação, assédio, falsa identidade, retransmissão de "correntes", compras não autorizadas etc.;

f) uso de técnicas de criptografia para, por exemplo, proteger a confidencialidade, a integridade e a autenticidade das informações (ver 10);

g) diretrizes de retenção e descarte para toda a correspondência de negócios, incluindo mensagens, de acordo com regulamentações e legislação locais e nacionais, relevantes.

h) controles e restrições associados à retransmissão em recursos de comunicação como, por exemplo, a retransmissão automática de mensagens eletrônicas (*e-mails*) para endereços externos;

i) orientar as pessoas para adotar precauções apropriadas não revelando informações confidenciais;

j) não deixar informações críticas ou sensíveis em secretárias eletrônicas uma vez que elas podem ser acessadas por pessoas não autorizadas, armazenadas em sistemas comuns ou armazenadas de forma incorreta, por engano;

k) lembrar as pessoas sobre os problemas do uso de aparelhos de fax, como:

   1) acesso não autorizado a dispositivos para recuperação de mensagens;

   2) programação de aparelhos, de forma deliberada ou acidental, para enviar mensagens para números específicos determinados;

   3) envio de documentos e mensagens para número errado, seja por falha na discagem ou uso de número armazenado errado.

Adicionalmente, convém que as pessoas sejam lembradas de que não devem manter conversas confidenciais em locais públicos, escritórios abertos, canais de comunicação inseguros e locais de reunião.

Convém que os serviços de transferência de informações estejam de acordo com os requisitos legais pertinentes (ver 18.1).

Informações adicionais

A transferência de informações pode ocorrer através do uso de vários tipos diferentes de recursos de comunicação, incluindo mensagens eletrônicas *(e-mails)*, voz, fax e vídeo.

A transferência de *softwares* pode ocorrer de diferentes formas, incluindo a baixa (*download*) da *internet* e a aquisição junto a fornecedores que vendem produtos em série.

Convém que sejam considerados os controles para os requisitos e as possíveis implicações nos negócios, nos aspectos legais e na segurança, relacionadas com a troca eletrônica de dados, com o comércio eletrônico e com o correio eletrônico.

13.2.2 Acordos para transferência de informações

Controle

Convém que sejam estabelecidos acordos para transferência segura de informações do negócio entre a organização e partes externas.

Diretrizes para implementação

Convém que os acordos de transferência de informações incorporem as seguintes condições:

a) responsabilidades do gestor pelo controle e notificação de transmissões, expedições e recepções;

b) procedimentos para assegurar a rastreabilidade dos eventos e o não-repúdio.

c) padrões técnicos mínimos para embalagem e transmissão;

d) acordos para procedimentos de custódia;

e) normas para identificação de portadores;

f) responsabilidades e obrigações na ocorrência de incidentes de segurança da informação, como perda de dados.

g) utilização de um sistema acordado de identificação para informações críticas e sensíveis, garantindo que o significado dos rótulos seja imediatamente entendido e que a informação esteja devidamente protegida (ver 8.2).

h) normas técnicas para a gravação e leitura de informações e *softwares*;

i) quaisquer controles especiais que possam ser necessários para proteção de itens sensíveis, tais como chaves criptográficas (ver 10);

j) manutenção de uma cadeia de custódia enquanto a informação encontra-se em trânsito;

k) níveis aceitáveis de controle de acesso.

Convém que políticas, procedimentos e normas para proteger as informações e as mídias em trânsito (ver 8.3.3) sejam estabelecidos e mantidos, além de serem referenciados nos mencionados acordos para transferência de informações.

É recomendado que os aspectos de segurança da informação contidos nos acordos reflitam a sensibilidade das informações envolvidas no negócio.

Informações adicionais

Os acordos podem ser eletrônicos ou manuais, e podem estar no formato de contratos formais. Para informações sensíveis, convém que os mecanismos específicos, usados para a transferência de tais informações, sejam consistentes com todas as organizações e tipos de acordos.

13.2.3 Mensagens eletrônicas

Controle

Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.

Diretrizes para implementação

Convém que as considerações de segurança da informação sobre as mensagens eletrônicas incluam o seguinte:

a) proteção das mensagens contra acesso não autorizado, modificação ou negação de serviço, combinado com o esquema de classificação adotado pela organização;

b) assegurar que o endereçamento e o transporte da mensagem estejam corretos;

c) confiabilidade e disponibilidade do serviço;

d) aspectos legais, como, por exemplo, requisitos de assinaturas eletrônicas;

e) aprovação prévia para o uso de serviços públicos externos tais como sistemas de mensagens instantâneas, redes sociais e compartilhamento de arquivos;

f) níveis mais altos de autenticação para controlar o acesso a partir de redes públicas.

Informações adicionais

Existem muitos tipos de mensagem eletrônica, como, *e-mails*, *Eletronic Data Interchange* (EDI), e redes sociais que cumprem um papel importante nas comunicações do negócio.

13.2.4 Acordos de confidencialidade e não divulgação

Controle

Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados.

Diretrizes para implementação

Convém que os acordos de confidencialidade e de não divulgação considerem os requisitos para proteger as informações confidenciais, usando termos que são obrigados do ponto de vista legal. Acordos de confidencialidade ou não divulgação são aplicaveis as partes externas ou aos funcionários da organização.

Convém que os elementos sejam selecionados ou acrescentados considerando-se o tipo do acesso permitido para a outra parte, ou para o tratamento da informação confidencial. Para identificar os requisitos para os acordos de confidencialidade ou de não divulgação, convém que os seguintes elementos sejam considerados:

a) uma definição da informação a ser protegida (por exemplo, informação confidencial);

b) o tempo de duração esperado de um acordo, incluindo situações onde a confidencialidade tenha que ser mantida indefinidamente;

c) ações requeridas quando um acordo está encerrado;

d) responsabilidades e ações dos signatários para evitar a divulgação não autorizada da informação;

e) o proprietário da informação, segredos comerciais e de propriedade intelectual, e como isto se relaciona com a proteção da informação confidencial;

f) o uso permitido da informação confidencial, e os direitos do signatário para usar a informação;

g) o direito de auditar e monitorar as atividades que envolvem as informações confidenciais;

h) o processo para notificação e relato de divulgação não autorizada ou vazamento das informações confidenciais;

i) termos para a informação ser retornada ou destruída quando do término do acordo;

j) ações esperadas a serem tomadas no caso de uma violação deste acordo.

Baseado nos requisitos de segurança da informação da organização, outros elementos podem ser necessários em um acordo de confidencialidade ou de não divulgação.

Convém que os acordos de confidencialidade e de não divulgação estejam em conformidade com todas as leis e regulamentações aplicáveis na jurisdição para a qual eles se aplicam (ver 18.1).

Convém que os requisitos para os acordos de confidencialidade e de não divulgação, sejam analisados criticamente de forma periódica e quando mudanças ocorrerem que influenciem estes requisitos.

Informações adicionais

Acordos de confidencialidade e de não divulgação protegem as informações da organização e informam aos signatários das suas responsabilidades, para proteger, usar e divulgar a informação de maneira responsável e autorizada.

Pode haver uma necessidade de uma organização usar diferentes formas de acordos de confidencialidade ou de não divulgação, em diferentes circunstâncias.

14 Aquisição, desenvolvimento e manutenção de sistemas

14.1 Requisitos de segurança de sistemas de informação

Objetivo: Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.

14.1.1 Análise e especificação dos requisitos de segurança da informação

Controle

Convém que os requisitos relacionados com segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

Diretrizes para implementação

Convém que os requisitos de segurança da informação sejam identificados usando vários métodos, como, requisitos de conformidade oriundos de política e regulamentações, modelos de ameaças, análises críticas de incidentes ou o uso de limiares de vulnerabilidade. Convém que os resultados da identificação sejam documentados e analisados criticamente por todas as partes interessadas.

Convém que os controles e requisitos de segurança da informação reflitam o valor da informação envolvida para o negócio (ver 8.2) e o seu potencial impacto negativo, que possa resultar de uma falha da segurança da informação.

Convém que a identificação e a gestão dos requisitos de segurança da informação e os processos associados sejam integrados nos estágios iniciais dos projetos de sistemas de informação. Considerações iniciais dos requisitos de segurança da informação, por exemplo, na fase do projeto podem conduzir a uma solução de custo mais eficiente e eficaz.

Convém que os requisitos de segurança da informação também considerem:

a) o nível de confiança exigido para as identidades alegadas dos usuários para determinar requisitos de autenticação do usuário;

b) os processos de autorização e provisionamento de acessos, para usuários técnicos ou com acessos privilegiados;

c) informar os usuários e operadores quanto às suas obrigações e responsabilidades;

d) as necessidades de proteção requerida dos ativos envolvidos, em particular com relação a disponibilidade, confidencialidade e integridade.

e) requisitos derivados dos processos do negócio, tais como registros de transações, monitoramento e requisitos de não repúdio;

f) requisitos mandatórios de outros controles de segurança, por exemplo interfaces para registro e monitoramento ou sistemas de detecção de vazamento de dados.

Convém que para aplicações que fornecem serviços sobre as redes públicas ou que implementam transações sejam considerados os controles dedicados 14.1.2 e 14.1.3.

Se produtos são adquiridos, convém que um processo formal de aquisição e teste seja seguido. Convém que os contratos com os fornecedores enderecem os requisitos de segurança identificados. Onde a funcionalidade segurança em um produto proposto não atenda ao requisito especificado, convém que o risco introduzido e os controles associados sejam reconsiderados antes da compra do produto.

Convém que as orientações para as configurações de segurança do produto estejam disponíveis e o alinhamento com a o software final seja avaliado e implementado.

Convém que critérios para aceitação de produtos sejam definidos, por exemplo em termos da sua funcionalidade, o qual dará garantia de que os requisitos de segurança identificados são atendidos. Convém que os produtos sejam avaliados com base nesses critérios, antes da sua aquisição. Convém que funcionalidades adicionais sejam analisadas criticamente para assegurar que ela não introduz riscos adicionais inaceitáveis.

Informações adicionais

A ABNT NBR ISO IEC 27005 e a ABNT NBR ISO 31000 fornecem diretrizes sobre o uso de processos de gestão de riscos, para identificar controles que atendam os requisitos de segurança da informação.

14.1.2 Serviços de aplicação seguros em redes públicas

Controle

Convém que as informações envolvidas nos serviços de aplicação que transitam sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.

Diretrizes para implementação

Convém que as considerações de segurança da informação para serviços de aplicação que transitam sobre redes públicas, considerem os seguintes itens:

a) o nível de confiança que cada parte requer na identidade alegada, como por exemplo, através de autenticação;

b) processos de autorização associados com quem pode aprovar conteúdos, publicar ou assinar documentos transacionais chave;

c) garantia de que os parceiros de comunicação estão completamente informados de suas autorizações para o fornecimento ou uso do serviço;

d) determinar e atender aos requisitos de confidencialidade, integridade, evidências de emissão e recebimento de documentos-chave e o não-repúdio de contratos, como por exemplo, os associados aos processos de licitação e contratos;

e) o nível de confiança requerido na integridade dos documentos chave;

f) os requisitos de proteção de quaisquer informações confidenciais;

g) a confidencialidade e integridade de quaisquer transações de pedidos, informações de pagamento, detalhes de endereço de entrega e confirmações de recebimentos;

h) o grau de investigação apropriado para a verificação de informações de pagamento fornecidas por um cliente;

i) seleção das formas mais apropriadas de pagamento para proteção contra fraudes;

j) o nível de proteção requerida para manter a confidencialidade e integridade das informações de pedidos;

k) prevenção contra perda ou duplicação de informação de transação;

l) responsabilidades associados com quaisquer transações fraudulentas;

m) requisitos de apólice de seguro.

Muitas das considerações acima podem ser endereçadas pela aplicação de controles criptográficos (ver 10), levando-se em conta a conformidade com requisitos legais (ver 18, especificamente o item 18.1.5 para legislação de criptografia).

Convém que os acordos de serviços de aplicação entre parceiros sejam apoiados por um acordo formal que comprometa ambas as partes com os termos de serviço acordados, incluindo detalhes de autorização (ver item b) acima).

Convém que requisitos de resiliência contra ataques sejam considerados, os quais podem incluir requisitos para a proteção dos servidores da aplicação envolvidos, ou garantir a disponibilidade da interconexão de redes, necessárias para a entrega do serviço.

Informações adicionais

Aplicações acessadas através de redes públicas são suscetíveis a uma variedade de ameaças de rede, tais como: atividades fraudulentas, disputas contratuais ou divulgação de informação para o público. Por estes motivos, uma avaliação de riscos detalhada e uma seleção de controles apropriada são indispensáveis. Os controles requeridos sempre incluem: métodos de criptografia para autenticação e segurança na transferência dos dados.

Serviços de aplicação podem fazer uso de métodos de autenticação segura, por exemplo: usando chave pública criptografada e assinaturas digitais (veja 10), para reduzir os riscos. Além disso, confiança em terceiros pode ser utilizada, onde tais serviços são necessários.

14.1.3 Protegendo as transações nos aplicativos de serviços

Controle

Convém que informações envolvidas em transações nos aplicativos de serviços sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada.

Diretrizes para implementação

Convém que as considerações de segurança da informação para transações nos aplicativos de serviços incluam os seguintes itens:

a) o uso de assinaturas eletrônicas para cada uma das partes envolvidas na transação;

b) todos os aspectos da transação, ou seja, garantindo que:

   1) informação de autenticação secreta de usuário são válidas e verificadas para todas as partes;

   2) a transação permaneça confidencial;

   3) a privacidade de todas as partes envolvidas seja mantida;

c) o caminho de comunicação entre todas as partes envolvidas é criptografado;

d) protocolos usados para comunicações entre todas as partes envolvidas é seguro;

e) garantir que o armazenamento dos detalhes da transação está localizado fora de qualquer ambiente publicamente acessível, como por exemplo, em uma plataforma de armazenamento existente na Intranet da organização, e não retida e exposta em um meio de armazenamento acessível diretamente pela Internet;

f) onde uma autoridade confiável é utilizada (como por exemplo, para propósitos de emissão e manutenção de assinaturas e/ou certificados digitais) a segurança é integrada ao longo de todo o processo de gestão dos certificados/ assinaturas.

Informações adicionais

A abrangência dos controles adotados, precisa ser compatível com o nível de risco associado a cada tipo de transação do serviço da aplicação.

Transações podem precisar de conformidade com requisitos legais e regulamentares na jurisdição nas quais as transações foram geradas, processadas, finalizadas ou armazenadas.

14.2 Segurança em processos de desenvolvimento e de suporte

Objetivo: Garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação.

14.2.1 Política de desenvolvimento seguro

Controle

Convém que regras para o desenvolvimento de sistemas e *software* sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.

Diretrizes para implementação

Desenvolvimento seguro é um requisito para construir um serviço, uma arquitetura, um *software* e um sistema seguro. Dentro de uma política de desenvolvimento seguro, convém que os seguintes aspectos sejam considerados:

a) segurança do ambiente de desenvolvimento;

b) orientações sobre a segurança no ciclo de vida do desenvolvimento do *software:*

   1) segurança na metodologia de desenvolvimento do *software*;

   2) diretrizes de códigos seguro para cada linguagem de programação usada.

c) requisitos de segurança na fase do projeto;

d) pontos de verificação de segurança no cronograma do projeto;

e) repositórios seguros;

f) segurança no controle de versões;

g) necessários conhecimentos de segurança de aplicações;

h) capacidade dos desenvolvedores de evitar, encontrar e corrigir vulnerabilidades.

Convém que as técnicas de programação seguras sejam usadas tanto para novos desenvolvimentos como para cenários de reuso dos códigos, onde as normas aplicadas ao desenvolvimento podem não ser conhecidas ou não estarem consistentes com as melhores práticas atuais. Convém que Normas de códigos seguro sejam consideradas e, onde relevante, seja exigido o seu uso.

Convém que os desenvolvedores sejam treinados no uso das técnicas de programação segura, e os testes e as análises críticas de código verifiquem a necessidade de uso dessas técnicas.

Quando o desenvolvimento é terceirizado, convém que a organização obtenha garantia de que a parte externa está em conformidade com essas regras para o desenvolvimento seguro (ver 14.2.7).

Informações adicionais

O desenvolvimento também pode ocorrer dentro das aplicações, como as aplicações para escritório, scripts, navegadores e banco de dados.

14.2.2 Procedimentos para controle de mudanças de sistemas

Controle

Convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças.

Diretrizes para implementação

Convém que os procedimentos de controle de mudanças sejam documentados e reforçados para assegurar a integridade do sistema, das aplicações e produtos, nos estágios iniciais dos projetos, através de um subsequente esquema de manutenção.

Convém que a introdução de novos sistemas e mudanças maiores em sistemas existentes, siga um processo formal de documentação, especificação, teste, controle da qualidade e gestão da implementação.

Convém que este processo inclua uma avaliação de riscos, análise do impacto das mudanças e a especificação dos controles de segurança requeridos. Convém que este processo também assegure que a segurança e os procedimentos de controle atuais não sejam comprometidos, que os programadores de suporte tenham acesso somente às partes do sistema necessárias para o cumprimento das tarefas e que sejam obtidas concordância e aprovação formal para qualquer mudança obtida.

Quando aplicável, convém que os procedimentos de controle de mudanças operacional e de aplicação sejam integrados (ver 12.1.2).

Convém que os procedimentos de controle de mudanças incluam, porém não se limitem a:

a) a manutenção de um registro dos níveis acordados de autorização;

b) a garantia de que as mudanças sejam submetidas por usuários autorizados;

c) a análise crítica dos procedimentos de controle e integridade para assegurar que as mudanças não os comprometam;

d) a identificação de todo *software*, informação, entidades em bancos de dados e hardware que precisam correções;

e) a identificação e a verificação do código crítico de segurança para minimizar a probabilidade da ocorrência de fragilidades de segurança conhecidas;

f) a obtenção de aprovação formal para propostas detalhadas antes do início dos trabalhos;

g) a garantia de que os usuários autorizados aceitam as mudanças antes da implementação;

h) a garantia da atualização da documentação do sistema após conclusão de cada mudança e de que a documentação antiga seja arquivada ou descartada;

i) a manutenção de um controle de versão para todas as atualizações de *software*;

j) a manutenção de uma trilha de auditoria de todas as mudanças solicitadas;

k) a garantia de que toda a documentação operacional (ver 12.1.1), e procedimentos dos usuários sejam alterados conforme necessário para se manter adequado;

l) a garantia de que as mudanças sejam implementadas em horários apropriados e não perturbe os processos de negócio envolvidos.

Informações adicionais

Mudanças em *software* podem impactar no ambiente operacional e vice versa.

Boas práticas incluem os testes de novo *software* em um ambiente segregado dos ambientes de produção e desenvolvimento (ver 12.1.4). Isto proporciona formas de ter controle sobre o novo *software* e permite proteção adicional das informações operacionais que são usadas para fins de teste. Convém que isto inclua correções, pacotes de serviço, entre outras atualizações.

Onde atualizações automáticas são consideradas, convém que o risco para a integridade e disponibilidade do sistema seja avaliada contra os benefícios da rápida implantação da atualização. Não é recomendada a utilização de atualizações automáticas em sistemas críticos visto que algumas atualizações podem causar falhas em aplicações críticas.

14.2.3 Análise crítica técnica das aplicações após mudanças nas plataformas operacionais

Controle

Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para assegurar que não ocorreu nenhum impacto adverso nas operações da organização ou na segurança.

Diretrizes para implementação

Convém que este processo compreenda:

a) a análise crítica dos controles da aplicação e dos procedimentos de integridade para assegurar que eles não foram comprometidos pelas mudanças na plataforma operacional;

b) a garantia de que as mudanças previstas na plataforma operacional sejam comunicadas em tempo hábil para permitir os testes e análises críticas antes da implementação;

c) a garantia de que as mudanças necessárias sejam incluídas nos planos de continuidade de negócios (ver 17).

Informações adicionais

Plataformas operacionais incluem sistemas operacionais, banco de dados e plataformas intermediárias. Convém que os controles também sejam aplicados para mudanças em aplicações.

14.2.4 Restrições sobre mudanças em pacotes de Software

Controle

Convém que modificações em pacotes de *software* sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas.

Diretrizes para implementação

Convém que quando possível e praticável, os pacotes de *softwares* providos pelos fornecedores sejam utilizados sem modificações. Quando um pacote de *software r*equer modificação, convém que sejam considerados os seguintes itens:

a) o risco de que controles e processos de integridade embutidos no *software s*ejam comprometidos;

b) a obtenção do consentimento do fornecedor;

c) a possibilidade de obtenção junto ao fornecedor das mudanças necessárias como atualização padrão do programa;

d) o impacto resultante quando a organização passa a ser responsável para a manutenção futura do *software* como resultado das mudanças;

e) a compatibilidade com outros *softwares* em uso;

Se mudanças forem necessárias, convém que o *software* original seja retido e as mudanças aplicadas em uma cópia. Convém que um processo de gestão da atualização de *software* seja implementado para assegurar que as atualizações das aplicações e os pacotes mais atualizados sejam instalados para todos os *softwares* autorizados (ver 12.6.1). Convém que todas as mudanças sejam totalmente testadas e documentadas, para que elas possam ser reaplicadas, se necessário, para futuras atualizações do *software.* Se requerido, convém que as modificações sejam testadas e validadas por um organismo independente de avaliação.

14.2.5 Princípios para projetar sistemas seguros

Controle

Convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.

Diretrizes para implementação

Convém que procedimentos para projetar sistemas de informação seguros, baseados nos princípios da engenharia de segurança sejam estabelecidos, documentados e aplicados nas atividades internas de engenharia de sistemas de informação da organização.

Convém que a segurança seja projetada em todas as camadas da arquitetura (negócios, dados, aplicações e tecnologia), realizando o balanceamento entre a necessidade da segurança da informação com a necessidade de acessibilidade. Convém que novas tecnologias sejam analisadas quanto aos riscos de segurança e o projeto seja analisado criticamente com base em modelos de ataque conhecidos.

Convém que estes princípios e os procedimentos de engenharia estabelecidos sejam analisados criticamente a intervalos regulares, para assegurar que eles estão contribuindo de forma eficaz para melhorar as normas de segurança no processo da engenharia. Convém que eles também analisem criticamente, a intervalos regulares, para garantir que eles permanecem atualizados para combater quaisquer novas ameaças potenciais e permanecer aplicável aos avanços das soluções e tecnologias a serem implementadas.

Convém que o estabelecimento dos princípios de engenharia de segurança seja aplicado onde pertinente, para sistemas de informação terceirizados, por meio de contratos e outras formas de acordos entre a organização e o fornecedor para o qual a organização terceirizou. Convém que a organização confirme que o rigor dos princípios de engenharia de segurança do fornecedor é comparável com seu próprio princípio.

Informações adicionais

Convém que procedimentos de desenvolvimento de aplicações implementem técnicas de engenharia seguras no desenvolvimento de aplicações que possuem interfaces de entrada e saída. Técnicas de engenharia seguras provêm guias sobre técnicas de autenticação de usuários, controle de sessões seguras e validação de dados, higienização e eliminação de depuração de códigos.

14.2.6 Ambiente seguro para desenvolvimento

Controle

Convém que as organizações estabeleçam e protejam adequadamente ambientes de desenvolvimento seguros para os esforços de desenvolvimento e integração de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema.

Diretrizes para implementação

Um ambiente de desenvolvimento seguro inclui pessoas, processos e tecnologia, associados com a integração e o desenvolvimento de sistemas.

Convém que as organizações avaliem os riscos associados com os esforços de desenvolvimento de sistemas individuais e estabeleçam ambientes de desenvolvimento seguro, para esforços de desenvolvimento de sistemas específicos, considerando:

a) a sensibilidade dos dados a serem processados, armazenados e transmitidos pelo sistema;

b) requisitos internos e externos aplicáveis, por exemplo, oriundos de políticas ou regulamentações;

c) controles de segurança já implementados pela organização, que suportam o desenvolvimento de sistemas;

d) confiabilidade das pessoas que trabalham no ambiente (ver 7.1.1);

e) o grau de terceirização associado com o desenvolvimento do sistema;

f) a necessidade de segregação entre os diferentes ambientes de desenvolvimento;

g) controle de acesso ao ambiente de desenvolvimento;

h) monitoramento de mudanças ao ambiente e do código armazenado no ambiente;

i) os *backups* armazenados em locais seguros externos à organização.

Uma vez que o nível de proteção seja determinado para um especifico ambiente de desenvolvimento, convém que a organização documente os processos correspondentes em procedimentos de desenvolvimento seguro, e forneça esses procedimentos a todos os indivíduos que deles necessitam.

14.2.7 Desenvolvimento terceirizado

Controle

Convém que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizado.

Diretrizes para implementação

Quando o desenvolvimento de sistemas for terceirizado, convém que os seguintes pontos sejam considerados ao longo de toda a cadeia de suprimento externo da organização:

a) acordos de licença, propriedade do código e direitos de propriedade intelectual relacionado com o conteúdo terceirizado (ver 18.1.2);

b) requisitos contratuais para um projeto seguro, práticas de código e teste (ver 14.2.1);

c) fornecimento de um modelo de ameaça aprovado para o desenvolvedor externo;

d) teste de aceitação relativos à qualidade e exatidão dos itens entregues;

e) fornecimento de evidência de que os princípios de segurança foram usados para estabelecer um nível mínimo de segurança aceitável e a qualidade da privacidade;

f) fornecimento de evidências de que testes suficientes foram realizados para proteger contra a ausência de conteúdo malicioso, tanto intencional e não intencional no momento da entrega;

g) fornecimento de evidências de que testes suficientes foram aplicados para proteger contra a presença de vulnerabilidades conhecidas;

h) acordos de garantia, por exemplo se o código fonte não está mais disponível;

i) direitos contratuais para auditar os controles e processos de desenvolvimento;

j) documentação efetiva da construção do ambiente usado para realizar as entregas;

k) a organização permanece responsável pela conformidade com as leis aplicáveis e a verificação da eficácia dos controles.

Informações adicionais

Mais informações sobre as relações com fornecedores podem ser encontradas em ISO/IEC 27036.

14.2.8 Teste de segurança do sistema

Controle

Convém que os testes de funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas.

Diretrizes para implementação

Sistemas novos e atualizados requerem verificação e testes completos, durante o processo de desenvolvimento, incluindo a preparação de uma programação de atividades detalhada, com testes de entrada e saída esperadas sob determinadas condições. Para o desenvolvimento interno, convém que tais testes sejam inicialmente realizados pela equipe de desenvolvimento.

Convém que testes de aceitação independente, também sejam realizados (tanto para desenvolvimento interno como para desenvolvimento terceirizado), para assegurar que o sistema trabalha conforme esperado e apenas como previsto em 14.1.1 e 14.1.2. Convém que a abrangência do teste seja proporcional à importância e natureza do sistema.

14.2.9 Teste de aceitação de sistemas

Controle

Convém que programas de testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões.

Diretrizes para implementação

Convém que testes de aceitação de sistemas incluam testes de requisitos de segurança da informação (ver 14.1.1 e 14.1.2) e aderência às práticas de desenvolvimento seguro de sistemas (ver 14.2.1). Convém que os testes também sejam realizados nos componentes recebidos e nos sistemas integrados. As organizações podem aproveitar as ferramentas automatizadas, como ferramentas de

análise de códigos ou *scanners* de vulnerabilidade, para verificar a correção dos defeitos relacionados à segurança.

Convém que os testes sejam realizados em um ambiente de teste realístico para assegurar que o sistema não introduzirá vulnerabilidades ao ambiente da organização e que os testes são confiáveis.

14.3 Dados para teste

Objetivo: Assegurar a proteção dos dados usados para teste.

14.3.1 Proteção dos dados para teste

Controle

Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados.

Diretrizes para implementação

Convém que seja evitado, para propósitos de teste, o uso de bancos de dados operacionais que contenham informação de identificação pessoal ou qualquer outra informação confidencial.

Se a informação de identificação pessoal ou outras informações sensíveis forem utilizadas com o propósito de teste, convém que todos os detalhes e conteúdos sejam protegidos contra remoção ou modificação (ver ISO/IEC 29101).

Convém que as seguintes orientações sejam aplicadas para a proteção de dados operacionais, quando utilizados para fins de teste:

a) convém que os procedimentos de controle de acesso, aplicáveis aos sistemas de aplicações operacionais, sejam também aplicados aos sistemas de aplicações em teste;

b) convém que seja obtida autorização cada vez que for utilizada uma cópia da informação operacional para uso em ambiente de teste;

c) convém que a informação operacional seja apagada do ambiente de teste, imediatamente após finalizar os testes;

d) convém que a cópia e o uso de informação operacional sejam registrados de forma a prover uma trilha para auditoria;

Informações adicionais

O sistema e o teste de aceitação geralmente requerem um volume substancial de dados para teste, o mais próximo possível dos dados operacionais.

15 Relacionamento na cadeia de suprimento

15.1 Segurança da informação na cadeia de suprimento.

Objetivo: Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores

15.1.1 Política de segurança da informação no relacionamento com os fornecedores

Controle

Convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor e documentados.

Diretrizes para implementação

Convém que a organização identifique e exija os controles de segurança da informação para tratar, especificamente, do acesso do fornecedor as informações da organização, através de uma política.

Convém que estes controles considerem os procedimentos e processos a serem implementados pela organização, bem como aqueles processos e procedimentos que a organização requeira do fornecedor a sua implementação, incluindo:

a) identificação e documentação dos tipos de fornecedores, por exemplo, serviços de TI, utilidades, serviços financeiros, componentes de infraestrutura de TI, aos quais a organização permitirá acessar suas informações;

b) um processo padronizado e o ciclo de vida para gerenciar as relações com o fornecedor;

c) definição dos tipos de acesso à informação que diferentes tipos de fornecedores terão permissão, o monitoramento e o controle do acesso;

d) requisitos mínimos de segurança da informação para cada tipo de acesso e tipo de informação, para servir como base para acordos individuais com o fornecedor, baseados nos perfis de risco, requisitos e necessidades de negócio;

e) procedimentos e processos para monitorar a aderência dos requisitos de segurança da informação estabelecidos para cada tipo de acesso e tipo de fornecedor, incluindo análise crítica da parte externa e a validação do produto;

f) completeza e exatidão dos controles para assegurar a integridade da informação ou o processamento da informação provido pelas partes;

g) tipos de obrigações aplicáveis aos fornecedores para proteger as informações da organização;

h) tratamentos de incidentes e contingências associados com o acesso do fornecedor incluindo responsabilidades, tanto da organização como dos fornecedores;

i) resiliência e, quando necessário, acordos de contingência e recuperação para assegurar a disponibilidade da informação ou o processamento da informação fornecido pelas partes;

j) treinamento de conscientização para o pessoal da organização envolvido com aquisição, relativo aos procedimentos, processos e políticas aplicáveis;

k) treinamento de conscientização para o pessoal da organização que interage com o pessoal do fornecedor, relativo às regras apropriadas de interação e comportamento baseado no tipo do fornecedor e no nível de acesso do fornecedor às informações e sistemas da organização;

l) condições sob as quais os controles e requisitos de segurança da informação serão documentados em um acordo, assinado por ambas as partes;

m) o gerenciamento da transição necessária da informação, dos recursos de processamento da informação e de qualquer coisa que necessite ser transferido, e a garantia de que a segurança da informação está mantida ao longo de todo o período de transição.

Informações adicionais

As informações podem ser colocadas em risco por fornecedores com a gestão da segurança da informação inadequada. Convém que controles sejam identificados e aplicados para administrar os acessos dos fornecedores aos recursos de processamento da informação. Por exemplo: se existir uma necessidade especial de confidencialidade da informação, acordos de não divulgação podem ser utilizados. Outro exemplo são os riscos de proteção dos dados quando os acordos com fornecedores envolvem a transferência ou acesso a informação através das barreiras. A organização precisa estar ciente de que as responsabilidades contratuais e legais para proteger a informação permanecem com a organização.

15.1.2 Identificando segurança da informação nos acordos com fornecedores

Controle

Convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar, ou prover componentes de infraestrutura de TI para as informações da organização.

Diretrizes para implementação

Convém que os acordos com fornecedores sejam estabelecidos e documentados para assegurar que não existem desentendimentos entre a organização e o fornecedor, com relação à obrigação de ambas as partes com o cumprimento dos requisitos de segurança da informação relevantes.

Convém que os seguintes termos sejam considerados para inclusão nos acordos visando atender aos requisitos da segurança da informação identificados:

a) descrição da informação a ser acessada/fornecida e os métodos de acesso a informação;

b) classificação da informação de acordo com o esquema de classificação da organização (ver 8.2); quando necessário, mapeamento do esquema de classificação da organização com o esquema de classificação do fornecedor;

c) requisitos regulamentares e legais, incluindo a proteção de dados, os direitos de propriedade intelectual e direitos autorais, e uma descrição sobre como isto será assegurado que os fornecedores cumprirão.

d) obrigação de cada parte contratual para implementar o conjunto de controles acordados, incluindo o controle de acesso, a análise crítica do desempenho, o monitoramento, o reporte e a auditoria;

e) regras de uso aceitável da informação, incluindo o uso inaceitável, se necessário;

f) uma lista explícita do pessoal do fornecedor autorizado a acessar ou receber as informações da organização ou as condições e procedimentos para autorização e remoção do pessoal do fornecedor para acessar ou receber as informações da organização;

g) políticas de segurança da informação relevantes para o contrato específico;

h) procedimentos e requisitos de gestão de incidentes (especialmente para notificação e colaboração durante a correção de um incidente);

i) requisitos de treinamento e conscientização para procedimentos específicos e requisitos de segurança da informação, por exemplo, resposta a incidentes, procedimentos de autorização;

j) regulamentações relevantes para subcontratação, incluindo os controles que precisam ser implementados;

k) acordos relevantes com parceiros, incluindo um contato pessoal para as questões de segurança da informação;

l) requisitos de seleção, se necessário para o pessoal do fornecedor, incluindo responsabilidades por realizar a verificação e procedimentos de notificação caso a verificação não tenha sido concluída ou se os resultados apresentados causem dúvidas ou preocupações;

m) direito de auditar os processos do fornecedor e os controles relacionados ao acordo;

n) processos para resolução de defeitos e de conflitos;

o) obrigações do fornecedor para, periodicamente, apresentar um relatório independente da eficácia dos controles e um acordo das correções em tempo hábil, das questões relevantes apresentadas no relatório;

p) obrigações do fornecedor de cumprir com os requisitos de segurança da informação da organização.

Informações adicionais

Os acordos podem variar consideravelmente para diferentes organizações e entre os diferentes tipos de fornecedores. Por este motivo, convém tomar cuidados para incluir todos os requisitos e riscos de segurança da informação relevantes. Acordos com fornecedores podem também envolver outras partes (por exemplo: sub-fornecedores).

Convém que sejam considerados nos acordos procedimentos para continuidade nos casos em que o fornecedor se torne incapaz de fornecer seus produtos ou serviços, para evitar qualquer atraso nos acordos de substituição de produtos ou serviços.

15.1.3 Cadeia de suprimento na tecnologia da comunicação e informação

Controle

Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia das comunicações e informação.

Diretrizes para implementação

Convém que os seguintes tópicos sejam considerados para inclusão nos acordos com fornecedores na segurança da cadeia de suprimento:

a) definição dos requisitos de segurança da informação aplicáveis na aquisição de serviços ou produtos de tecnologia da comunicação e informação, em acréscimo aos requisitos de segurança da informação gerais, na relação com os fornecedores.

b) para os serviços de tecnologia da comunicação e informação, exigir que os fornecedores divulgue os requisitos de segurança da informação da organização em toda a cadeia de suprimento, caso os sub-fornecedores sejam parte do serviço de tecnologia da comunicação e informação a ser fornecido para a organização;

c) para produtos de tecnologia de comunicação e informação, exigir que os fornecedores divulguem as práticas de segurança da informação apropriadas ao longo de toda a cadeia de suprimento, caso esses produtos incluam componentes comprados de outros fornecedores;

d) implementação de um processo de monitoramento e métodos aceitáveis para validação dos serviços e produtos de tecnologia da comunicação e informação entregues estão aderentes aos requisitos de segurança da informação estabelecidos;

e) implementação de um processo para identificação dos componentes do serviço ou produto que são críticos para manter a funcionalidade e, portanto, requer uma maior atenção e verificação quando construído fora da organização, especialmente se o fornecedor principal terceiriza partes dos componentes do serviço ou produto com outros fornecedores;

f) obtenção de garantia de que os componentes críticos e as suas origens podem ser rastreadas ao longo de toda a cadeia de suprimento;

g) obtenção de garantia de que os produtos de tecnologia da comunicação e informação entregues estão funcionando conforme esperado, sem quaisquer características não desejadas ou não esperadas;

h) definição de regras para compartilhamento da informação com relação a cadeia de suprimento e quaisquer questões potenciais e compromissos assumidos entre a organização e os fornecedores;

i) a implementação de processos específicos para gerenciar os riscos de segurança associados, a disponibilidade e os componentes do ciclo de vida da tecnologia da comunicação e informação. isto inclui a gestão dos riscos de componentes quando não estiverem mais disponíveis, devido ao fornecedor não estar mais no negócio ou o fornecedor não mais fornecer esses componentes devido aos avanços da tecnologia.

Informações adicionais

Práticas de gestão de riscos específicas para a cadeia de suprimento de tecnologia da comunicação e informação são construídas sobre as práticas de segurança da informação, qualidade, gestão de projetos e engenharia de sistemas, mas não as substituem.

As organizações são aconselhadas para trabalhar com fornecedores que entendam da cadeia de suprimento de tecnologia da comunicação e informação e quaisquer questões que tenham impacto

relevante sobre os produtos e serviços que estão sendo fornecidos. As organizações podem influenciar as práticas de segurança da informação da cadeia de suprimento da tecnologia da comunicação e informação, deixando claro nos acordos com seus fornecedores os assuntos que devem ser abordados por outros fornecedores da cadeia de fornecimento de tecnologia da comunicação e informação.

A cadeia de suprimento de tecnologia da comunicação e informação aqui abordada inclui os serviços de computação na nuvem.

15.2 Gerenciamento da entrega do serviço do fornecedor

Objetivo: Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

15.2.1 Monitoramento e análise crítica de serviços com fornecedores

Controle

Convém que a organização monitore, analise criticamente e audite a intervalos regulares, a entrega dos serviços executados pelos fornecedores.

Diretrizes para implementação

Convém que a monitoração e a análise crítica dos serviços fornecidos garantam que os termos e condições dos acordos de segurança de informação sejam cumpridos e que os incidentes e problemas de segurança da informação sejam gerenciados de forma apropriada. Convém que envolva um processo de gestão do relacionamento dos serviços entre a organização e o fornecedor para:

a) monitorar os níveis de desempenho de serviço para verificar aderência aos acordos;

b) analisar criticamente os relatórios de serviços produzidos por fornecedores e agendamento de reuniões de progresso conforme requerido pelos acordos;

c) realizar auditorias nos fornecedores, em conjunto com a análise crítica dos relatórios de auditoria independente, quando disponíveis, bem como o acompanhamento das questões identificadas;

d) fornecer informações sobre incidentes de segurança de informação e analisar criticamente tais informações, conforme requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apoiem;

e) analisar criticamente as trilhas de auditoria do fornecedor e registros de eventos de segurança da informação, problemas operacionais, falhas, investigação de falhas e interrupções relativas ao serviço entregue;

f) resolver e gerenciar quaisquer problemas identificados;

g) analisar criticamente os aspectos de segurança da informação na relação dos fornecedores com seus próprios fornecedores;

h) garantir que o fornecedor mantém capacidade de serviço suficiente em conjunto com planos de trabalho desenhados para assegurar que os níveis de continuidade do serviço acordados são mantidos, no caso de um desastre ou falha dos serviços principais (ver 17).

Convém que a responsabilidade sobre o gerenciamento de relacionamento com o fornecedor seja atribuída a um indivíduo designado ou para a equipe de gerenciamento de serviço.

Adicionalmente, convém que a organização assegure que o fornecedor atribua responsabilidades pela verificação de conformidade e reforce os requisitos dos acordos.

Convém que habilidades técnicas suficientes e recursos sejam disponibilizados para monitorar os requisitos dos acordos, em particular os requisitos de segurança de informação foram atendidos. Convém que ações apropriadas sejam tomadas quando deficiências na entrega dos serviços são observadas.

Convém que a organização mantenha controles gerais suficientes e visibilidade de todos os aspectos de segurança para as informações sensíveis ou críticas ou para os recursos de processamento da informação acessados, processados ou gerenciado por um fornecedor.

Convém que a organização mantenha visibilidade sobre as atividades de segurança, como o gerenciamento de mudanças, a identificação de vulnerabilidades, os relatórios e respostas de incidentes de segurança da informação, através de um processo definido de notificação.

15.2.2 Gerenciamento de mudanças para serviços com fornecedores

Controle

Convém que mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, sejam gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos, e a reavaliação de riscos.

Diretrizes para implementação

Convém que os seguintes aspectos sejam levados em consideração:

a) mudanças nos acordos com o fornecedor;

b) mudanças feitas pela organização para implementar:

   1) melhorias dos serviços atualmente oferecidos;

   2) desenvolvimento de quaisquer novas aplicações e sistemas;

   3) modificações ou atualizações das políticas e procedimentos da organização;

   4) controles novos ou modificados para resolver os incidentes de segurança de informação e para melhorar a segurança da informação;

c) mudanças nos serviços de fornecedores para implementar:

   1) mudanças e melhorias em redes;

   2) uso de novas tecnologias;

   3) adoção de novos produtos ou novas versões;

4) novas ferramentas e ambientes de desenvolvimento;

5) mudanças de localização física dos recursos de serviços;

6) mudanças de fornecedores;

7) subcontratação com outro fornecedor.

16 Gestão de incidentes de segurança da informação

16.1 Gestão de incidentes de segurança da informação e melhorias

Objetivo: Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

16.1.1 Responsabilidades e procedimentos

Controle

Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

Diretrizes para implementação

Convém que as seguintes diretrizes para o gerenciamento de responsabilidades e procedimentos com relação à gestão de incidentes de segurança da informação sejam consideradas:

a) responsabilidades pelo gerenciamento sejam estabelecidas para assegurar que os seguintes procedimentos são desenvolvidos e comunicados, de forma adequada, dentro da organização:

   1) procedimentos para preparação e planejamento a respostas a incidentes;

   2) procedimentos para monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação;

   3) procedimentos pra registros das atividades de gerenciamento de incidentes;

   4) procedimentos para tratamento para evidências forenses;

   5) procedimentos para avaliação e decisão dos eventos de segurança da informação e avaliação de fragilidades de segurança da informação;

   6) procedimentos para resposta, incluindo aquelas relativas a escalação, recuperação controlada de um incidente e comunicação as pessoas ou organizações relevantes, internas e externas.

b) procedimentos estabelecidos assegurem que:

1) pessoal competente trata as questões relativas a incidentes de segurança dentro da organização;

2) um ponto de contato para notificação e detecção de incidentes de segurança está implementado;

3) contatos apropriados são mantidos com autoridades, grupos de interesses externos ou fóruns que tratam de questões relativas a incidentes de segurança da informação.

c) convém que procedimentos de notificação incluam:

1) preparação de formulários de notificação de evento de segurança da informação para apoiar as ações de notificação e ajudar a pessoa que está notificando, lembrando de todas as ações necessárias no caso de um evento de segurança da informação;

2) o procedimento a ser realizado no caso de um evento de segurança da informação, por exemplo relatar todos os detalhes (tipo de não conformidade ou violação, mau funcionamento, mensagens na tela, comportamento estranho) imediatamente; e não tomar nenhuma ação sozinho, porém notificar imediatamente ao ponto de contato, tomando apenas ações coordenadas;

3) referência a um processo disciplinar formal estabelecido para tratar com funcionários que cometam violações de segurança da informação;

4) processo de realimentação adequado para assegurar que aquelas pessoas que notificaram um evento de segurança da informação são informadas dos resultados após o assunto ter sido tratado e encerrado.

Convém que os objetos para a gestão de incidentes de segurança da informação sejam acordados com a direção e garantam que as pessoas responsáveis pela gestão dos incidentes de segurança da informação entendem as prioridades da organização para tratar com os incidentes de segurança da informação.

Informações adicionais

Incidentes de segurança da informação podem transcender os limites organizacionais e nacionais. Para responder tais incidentes existe uma crescente necessidade de coordenar resposta e compartilhar informação sobre esses incidentes com organizações externas, quando apropriado.

Diretriz detalhada em gestão de incidentes de segurança da informação é fornecida em ISO/IEC 27035.

16.1.2 Notificação de eventos de segurança da informação

Controle

Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.

Diretrizes para implementação

Convém que todos os funcionários e partes externas sejam alertados sobre sua responsabilidade de notificar qualquer evento de segurança da informação o mais rapidamente possível. Convém que eles também estejam cientes do procedimento para notificar os eventos de segurança da informação e do ponto de contato, ao qual os eventos devem ser notificados.

Situações a serem consideradas para notificar um evento de segurança da informação incluem:

a) controle de segurança ineficaz;

b) violação da disponibilidade, confidencialidade e integridade da informação;

c) erros humanos;

d) não-conformidade com políticas ou diretrizes;

e) violações de procedimentos de segurança física;

f) mudanças descontroladas de sistemas;

g) mau funcionamento de *software* ou *hardware*;

h) violação de acesso.

Informações adicionais

Mau funcionamento ou outro comportamento anômalo do sistema pode ser um indicador de um ataque de segurança ou violação na segurança atual e, portanto, convém que sempre seja reportado como um evento de segurança da informação.

16.1.3 Notificando fragilidades de segurança da informação

Controle

Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização, sejam instruídos a registrar e notificar quaisquer fragilidades de segurança da informação, suspeita ou observada, nos sistemas ou serviços.

Diretrizes para implementação

Convém que todos os funcionários e partes externas notifiquem essas questões para o ponto de contato, o mais rápido possivel, de forma a prevenir incidentes de segurança da informação. O mecanismo de notificação deve ser fácil, acessivel e disponível, sempre que possível.

Informações adicionais

Convém que funcionários e fornecedores sejam avisados a não tentar provar suspeitas de fraquezas de segurança. Testar fraquezas pode ser interpretado como potencial mau uso do sistema e pode também causar danos ao serviço ou sistema de informação e resultar em responsabilidade legal para o indivíduo que executou o teste.

16.1.4 Avaliação e decisão dos eventos de segurança da informação

Controle

Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.

Diretrizes para implementação

Convém que o ponto de contato avalie cada evento de segurança da informação usando uma escala de classificação de incidentes e eventos de segurança da informação, para decidir se é recomendado que o evento seja classificado como um incidente de segurança da informação. A priorização e a classificação de incidentes pode ajudar a identificar o impacto e a abrangência de um incidente.

Em casos onde a organização tenha uma equipe de resposta a incidentes de segurança da informação, a avaliação e decisão seja encaminhada para a equipe, para confirmação ou reavaliação.

Convém que os resultados da avaliação e decisão sejam registrados em detalhes, para o propósito de verificação e referência futura.

16.1.5 Resposta aos incidentes de segurança da informação

Controle

Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados.

Diretrizes para implementação

Convém que incidentes de segurança da informação sejam reportados para um ponto de contato definido e outras pessoas relevantes da organização, ou ainda, partes externas (ver 16.1.1).

Convém que a notificação inclua os seguintes itens:

a) coleta de evidências, tão rápido quanto possível, logo após a ocorrência;

b) realização de análise forense de segurança da informação, conforme requerido (ver 16.1.7);

c) escalação, conforme requerido;

d) garantia de que todas as atividades de respostas envolvidas são adequadamente registradas para análise futura;

e) comunicação da existência de incidente de segurança da informação ou qualquer detalhe relevante para pessoas internas ou externas, ou organizações que precisam tomar conhecimento;

f) tratamento com as fragilidades de segurança da informação encontradas que causem ou contribuam para o incidente;

g) uma vez que o incidente foi, de forma bem sucedida, formalmente tratado, encerrar o incidente e registra-lo.

Convém que análises pós-incidente sejam realizadas, se necessário, para identificar a fonte do incidente.

Informações adicionais

O primeiro objetivo de resposta a incidente é “voltar ao nível de segurança normal” e então iniciar a recuperação necessária.

16.1.6 Aprendendo com os incidentes de segurança da informação

Controle

Convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.

Diretrizes para implementação

Convém que haja um mecanismo implementado para permitir monitorar e quantificar os tipo, volumes e custos de incidentes de segurança da informação. Convém que a informação resultante da análise de incidentes de segurança da informação seja usada para identificar incidentes recorrentes ou de alto impacto.

Informações adicionais

A avaliação de incidentes de segurança da informação pode indicar a necessidade de melhoria ou controles adicionais para diminuir a frequência, dano e custo de futuras ocorrências ou ser levado em conta no processo de análise crítica da política de segurança (ver 5.1.2).

Com o devido cuidado aos aspectos de confidencialidade, estórias de incidentes atuais de segurança da informação podem ser usadas em treinamentos de conscientizações de usuários (ver 7.2.2) como exemplos do que pode acontecer, como responder a tais incidentes e como evita-los no futuro.

16.1.7 Coleta de evidências

Controle

Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.

Diretrizes para implementação

Convém que procedimentos internos sejam desenvolvidos e seguidos quando tratando de obter evidências para os propósitos de ações legais ou disciplinares.

Geralmente os procedimentos para evidência fornecem processos de identificação, coleta, aquisição e preservação de evidências, de acordo com diferentes tipos de mídia, dispositivos e situação dos dispositivos, por exemplo, se estão ligados ou desligados. Convém que os procedimentos levem em conta:

a) a cadeia de custodia;

b) a segurança da evidência;

c) a segurança das pessoas;

d) papéis e responsabilidades das pessoas envolvidas;

e) competência do pessoal;

f) documentação;

g) resumo do incidente.

Quando disponível, certificações ou outros meios de qualificação de pessoal e ferramentas são buscados, para aumentar o valor da evidência preservada.

Evidência forense pode ir além dos limites da organização ou da jurisdição. Em tais casos, convém que seja assegurado que a organização tem direito de coletar as informações requeridas como evidência forense. Os requisitos de diferentes jurisdições podem ser considerados para maxmizar as chances de admissão ao longo das jurisdições relevantes.

Informações adicionais

Identificação é o processo envolvendo a busca, reconhecimento e documentação de potencial evidência. Coleta é o processo de levantamento de itens físicos que podem conter potencial evidência. Aquisição é o processo de criação de uma cópia dos dados dentro de um cenário definido. Preservação é o processo para manter e proteger a integridade e condição original da potencial evidência.

Logo quando um evento de segurança da informação é detectado pode não ser óbvio se o evento resultará em uma ação judicial ou não. Portanto, existe o perigo que esta evidência necessária seja destruída intencionalmente ou acidentalmente antes que a gravidade do incidente seja percebida. É aconselhável envolver um advogado ou a polícia o quanto antes em qualquer ação legal e receber aconselhamento sobre a evidência requerida.

A ABNT NBR ISO/IEC 27037 fornece diretrizes para identificação, coleta, aquisição e preservação de evidências digitais.

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

17.1 Continuidade da segurança da informação

Objetivo: É recomendado que a continuidade da segurança da informação seja considerada nos sistemas de gestão da continuidade do negócio da organização.

17.1.1 Planejando a continuidade da segurança da informação

Controle

Convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

Diretrizes para implementação

Convém que uma organização avalie se a continuidade da segurança da informação está contida dentro do processo de gestão da continuidade do negócio ou no processo de gestão de recuperação de desastre. Requisitos de segurança da informação podem ser determinados quando do planejamento da continuidade do negócio e da recuperação de desastre.

Na ausência de um planejamento formal de continuidade do negócio e de recuperação de desastre, convém que a gestão da segurança da informação assuma que os requisitos de segurança da informação permanecem os mesmos, em situações adversas, comparadas com as condições de operação normal. Alternativamente, uma organização pode realizar uma análise de impacto do negócio relativa aos aspectos de segurança da informação, para determinar os requisitos de segurança da informação que são aplicáveis nas situações adversas.

Informações adicionais

Para reduzir o tempo e o esforço de uma análise de impacto do negócio adicional, da segurança da informação, é recomendado capturar os aspectos da segurança da informação no gerenciamento da continuidade normal dos negócios ou na análise do impacto ao negócio no gerenciamento da recuperação de um desastre. Isto implica que os requisitos de continuidade da segurança da informação estão explicitamente contemplados na gestão da continuidade do negócio ou nos processos de gerenciamento da recuperação de desastre.

Informações sobre gestão da continuidade do negócio podem ser encontrada na ISO/IEC 27031, ISO 22313 e ABNT NBR ISO 22301.

17.1.2 Implementando a continuidade da segurança da informação

Controle

Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.

Diretrizes para implementação

Convém que uma organização assegure-se de que:

a) uma estrutura de gerenciamento adequada está implementada para mitigar e responder a um evento de interrupção, usando pessoal com a necessária autoridade, experiência e competência;

b) o pessoal de resposta a incidente com a necessária responsabilidade, autoridade e competência para gerenciar um incidente e garantir a segurança da informação, está designado;

c) planos documentados, procedimentos de recuperação e resposta estejam desenvolvidos e aprovados, detalhando como a organização irá gerenciar um evento de interrupção e como manterá a sua segurança da informação em um nível pré-determinado, com base nos objetivos de continuidade da segurança da informação aprovado pela direção (ver 17.1.1).

Em função dos requisitos de continuidade de segurança da informação, convém que a organização estabeleça, documente, implemente e mantenha:

a) controles de segurança da informação dentro dos processos de recuperação de desastre ou de continuidade do negócio, procedimentos e ferramentas e sistemas de suporte;

b) processos, procedimentos e mudança de implementação para manter os controles de segurança da informação existentes durante uma situação adversa;

c) controles compensatórios para os controles de segurança da informação que não possam ser mantidos durante uma situação adversa.

Informações adicionais

Dentro do contexto da continuidade do negócio ou da recuperação de desastre, procedimentos e processos específicos podem ser necessários, que sejam definidos. Convém que informações que sejam tratadas nestes processos e procedimentos ou em sistemas de informação dedicados para apoia-los, sejam protegidas. Desta forma, convém que a organização envolva especialistas em segurança da informação, quando do estabelecimento, implementação e manutenção dos procedimentos e processos de recuperação de desastres ou da continuidade dos negócios.

Convém que os controles de segurança da informação a serem implementados continuem a operar durante uma condição de situação adversa. Se os controles de segurança não são capazes de manter a informação segura, convém que outros controles sejam estabelecidos, implementados e mantidos para garantir um nível aceitável da segurança da informação.

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

Controle

Convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.

Diretrizes para implementação

Mudanças organizacionais, técnicas, de procedimentos e processos, quando em um contexto operacional ou de continuidade, podem conduzir a mudanças nos requisitos de continuidade da segurança da informação. Em tais casos, convém que a continuidade dos processos, procedimentos e controles para segurança da informação sejam analisados criticamente com base nesses requisitos alterados.

Convém que a organização verifique se a sua continuidade da gestão da segurança da informação está:

a) testada e verificada a funcionalidade dos processos, procedimentos e controles da continuidade da segurança da informação para garantir que eles são consistentes com os objetivos da continuidade as segurança da informação;

b) testada e verificada quanto ao conhecimento e rotina para operar os procedimentos, processos e controles de continuidade da segurança da informação de modo a assegurar que o seu desempenho está consistente com os objetivos da continuidade da segurança da informação;

c) analisada criticamente quanto à validade e eficácia dos controles de continuidade da segurança da informação, quando os sistemas de informação, processos de segurança da informação,

procedimentos e controles ou gestão da continuidade do negócio/gestão de recuperação de desastre e soluções de mudança.

Informações adicionais

A verificação dos controles da continuidade da segurança da informação é diferente das verificações e testes da segurança da informação normal, e convém que sejam realizados fora do âmbito dos testes de mudanças. Quando possível é recomendável integrar a verificação dos controles da continuidade da segurança da informação, com os testes de recuperação de desastre ou da continuidade dos negócios da organização.

17.2 Redundâncias

Objetivo: Assegurar a disponibilidade dos recursos de processamento da informação.

17.2.1 Disponibilidade dos recursos de processamento da informação

Controle

Convém que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.

Diretrizes para implementação

Convém que a organização identifique os requisitos do negócio quanto à disponibilidade de sistemas de informação. Quando a disponibilidade não puder ser assegurada usando a arquitetura de sistemas existentes, componentes redundantes ou arquiteturas sejam considerados.

Onde aplicável, convém que sistemas de informação redundantes sejam testados para assegurar que a transferência de um componente para outro componente, quando existe falha do primeiro componente, este funciona conforme esperado.

Informações adicionais

A implementação de redundâncias pode introduzir riscos a integridade ou confidencialidade da informação e dos sistemas de informação, os quais precisam ser considerados quando do projeto dos sistemas de informação.

18 Conformidade

18.1 Conformidade com requisitos legais e contratuais

Objetivo: Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas á segurança da informação e de quaisquer requisitos de segurança.

18.1.1 Identificação da legislação aplicável e de requisitos contratuais

Controle

Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.

Diretrizes para implementação

Convém que os controles específicos e as responsabilidades individuais para atender a estes requisitos sejam definidos e documentados.

Convém que os gestores identifiquem toda a legislação aplicável à sua organização, para atender aos requisitos relativos ao seu tipo de negócio. Caso a organização realize negócios em outros países convém que os gestores considerem a conformidade em todos esses países.

18.1.2 Direitos de propriedade intelectual

Controle

Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de *software* proprietários.

Diretrizes para implementação

Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado como propriedade intelectual:

a) divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de produtos de *software* e de informação;

b) adquirir *software* somente por meio de fontes conhecidas e de reputação, para assegurar que o direito autoral não está sendo violado;

c) manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas;

d) manter de forma adequada os registros de ativos, e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;

e) manter provas e evidências da propriedade de licenças, discos-mestres, manuais etc.;

f) implementar controles para assegurar que o número máximo de usuários permitidos, dentro da licença concedida, não está excedido;

g) conduzir verificações para que somente produtos de *software* autorizados e licenciados sejam instalados;

h) estabelecer uma política para a manutenção das condições adequadas de licenças;

i) estabelecer uma política para disposição ou transferência de *software* para outros;

j) cumprir termos e condições para *software* e informação obtidos a partir de redes públicas;

k) não duplicar, converter para outro formato ou extrair de registros comerciais (filme, áudio) outros que não os permitidos pela lei de direito autoral;

l) não copiar no todo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral.

Informações adicionais

Direitos de propriedade intelectual incluem direitos autorais de *software* ou documento, direitos de projetos, marcas, patentes e licenças de código fonte.

Produtos de *software* proprietários são normalmente fornecidos sob um contrato de licenciamento que especifica os termos e condições da licença, por exemplo, limitar o uso dos produtos em máquinas especificadas ou limita a reprodução apenas para a criação de cópias de *backup*. Convém que a importância e a conscientização dos direitos de propriedade intelectual de *software* sejam comunicados aos responsáveis pelo desenvolvimento de *software* na organização.

Requisitos legais, regulamentares e contratuais podem colocar restrições sobre a cópia de material proprietário. Em particular, eles podem exigir que apenas o material que é desenvolvido pela organização ou que está licenciado ou fornecido pelo desenvolvedor para a organização, pode ser utilizado. Violação de direitos autorais pode levar a ação judicial e pode envolver multas e processos criminais.

18.1.3 Proteção de registros

Controle

Convém que registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

Diretrizes para implementação

Convém que quando a organização decida proteger os registros específicos, a classificação correspondente seja baseada no esquema classificação da organização. Convém que os registros sejam categorizados em tipos de registros, tais como registros contábeis, registros de base de dados, registros de transações, registros de auditoria e procedimentos operacionais, cada qual com detalhes do período de retenção e do tipo de mídia de armazenamento como, por exemplo, papel, microficha, meio magnético ou ótico. Convém que quaisquer chaves de criptografia relacionadas com arquivos cifrados ou assinaturas digitais (ver 10) sejam armazenadas para permitir a decifração de registros pelo período de tempo que os registros são mantidos.

Convém que cuidados sejam tomados a respeito da possibilidade de deterioração das mídias usadas no armazenamento dos registros. Convém que os procedimentos de armazenamento e manuseio sejam implementados de acordo com as recomendações dos fabricantes.

Onde mídias eletrônicas armazenadas forem escolhidas, convém que sejam incluídos procedimentos para assegurar a capacidade de acesso aos dados (leitura tanto na mídia como no formato utilizado) durante o período de retenção, para proteger contra perdas ocasionadas pelas futuras mudanças na tecnologia.

Sistemas de armazenamento de dados sejam escolhidos de modo que o dado solicitado possa ser recuperado de forma aceitável, dependendo dos requisitos a serem atendidos.

Convém que o sistema de armazenamento e manuseio assegure a clara identificação dos registros e dos seus períodos de retenção, conforme definido pela legislação nacional ou regional ou por regulamentações, se aplicável. Convém que este sistema permita a destruição apropriada dos registros após esse período, caso não sejam mais necessários à organização.

Para atender aos objetivos de proteção dos registros, convém que os seguintes passos sejam tomados pela organização:

a) emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações;

b) elaborar uma programação para retenção, identificando os registros essenciais e o período recomendado para que cada um seja mantido;

c) manter um inventário das fontes de informações-chave.

Informações adicionais

Alguns registros podem precisar ser retidos de forma segura para atender a requisitos estatutários, regulamentares ou contratuais, bem como para apoiar as atividades essenciais do negócio. Exemplos incluem os registros que podem ser exigidos como prova de que uma organização opera dentro de normas estatutárias ou regulamentares, para assegurar a defesa contra potencial ação civil ou criminal, ou para confirmar a situação financeira de uma organização perante os acionistas, partes externas e auditores. A legislação nacional ou a regulamentação pode definir conteúdo de dados e o período de tempo para a retenção de informações.

Outras informações sobre o gerenciamento de registros organizacionais podem ser encontrados na ISO 15489-1.

18.1.4 Proteção e privacidade de informações de identificação pessoal

Controle

Convém que a privacidade e proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.

Diretrizes para implementação

Convém que uma política de dados da organização para proteção e privacidade da informação de identificação pessoal, seja desenvolvida e implementada. Esta política deve ser comunicada a todas as pessoas envolvidas no processamento de informação de identificação pessoal.

A conformidade com esta política e todas as regulamentações e legislação relevantes, relativas à proteção da privacidade das pessoas e da proteção da informação de identificação pessoal requer um controle e uma estrutura de gerenciamento apropriada. Quase sempre isto é melhor conseguido indicando uma pessoa responsável, como por exemplo, um *privacy officer*, que tem a função de fornecer orientações aos gestores, usuários e provedores de serviços sobre as suas responsabilidades individuais e procedimentos específicos que devem ser seguidos.

A responsabilidade pelo manuseio da informação de identificação pessoal e a garantia da conscientização sobre os princípios da privacidade, sejam tratados de acordo com as regulamentações e legislações pertinentes. Convém que técnicas apropriadas e medidas da organização para proteger a informação de identificação pessoal, sejam implementadas.

Informações adicionais

ISO/IEC 29100 fornece uma estrutura de alto nível para a proteção da informação de identificação pessoal, no âmbito dos sistemas de tecnologia da comunicação e informação.

Alguns países têm introduzido legislação que estabelecem controles na coleta, processamento e transmissão de informação de identificação pessoal (geralmente informação sobre indivíduos vivos que podem ser identificados a partir de tais informações). Dependendo da respectiva legislação nacional, esses controles podem impor direitos sobre a coleta, tratamento e divulgação de informação de identificação pessoal, e pode também restringir a capacidade de transferir informação de identificação pessoal para outros países.

18.1.5 Regulamentação de controles de criptografia

Controle

Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

Diretrizes para implementação

Convém que os seguintes itens sejam considerados para conformidade com leis, acordos e regulamentações relevantes:

a) restrições à importação e/ou exportação de *hardware* e *software* de computador para execução de funções criptográficas;

b) restrições à importação e/ou exportação de *hardware* e *software* de computador que foi projetado para ter funções criptográficas embutidas;

c) restrições no uso de criptografia;

d) métodos mandatórios ou discricionários de acesso pelas autoridades dos países à informação cifrada por *hardware* ou *software* para fornecer confidencialidade ao conteúdo.

Convém que a assessoria jurídica garanta a conformidade com as legislações e regulamentações vigentes. Convém que seja obtida assessoria jurídica antes de se transferir informações cifradas ou controles de criptografia para outros países.

18.2 Análise crítica da segurança da informação

Objetivo: Garantir que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização.

18.2.1 Análise crítica independente da segurança da informação

Controle

Convém que 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) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.

Diretrizes para implementação

Convém que a análise crítica independente seja iniciada pela direção. Tal análise crítica independente é necessária para assegurar a contínua pertinência, adequação e eficácia do enfoque da organização para gerenciar a segurança da informação. Convém que a análise crítica inclua a avaliação de oportunidades para melhoria e a necessidade de mudanças para o enfoque da segurança da informação, incluindo a política e os objetivos de controle.

Convém que análise crítica seja executada por pessoas independentes da área avaliada, como por exemplo, uma função de auditoria interna, um gerente independente ou uma organização de externa especializada em tais análises críticas. Convém que as pessoas que realizem estas análises críticas possuam habilidade e experiência apropriadas.

Convém que os resultados da análise crítica independente sejam registrados e relatados para a direção que iniciou a análise crítica e que estes registros sejam mantidos.

Se a análise crítica independente identificar que o enfoque da organização e a implementação para gerenciar a segurança da informação são inadequados ou não conforme com as orientações estabelecidas pela segurança da informação, convém que nas políticas de segurança da informação, a direção considere a tomada de ações corretivas.

Informações adicionais

A ISO/IEC 27007, "Diretrizes para auditoria de sistemas de gestão da segurança da informação" e a ISO/IEC TR 27008 , "Diretrizes para auditores sobre controles de segurança da informação" também fornecem orientações para a realização de análise crítica independente.

18.2.2 Conformidade com as políticas e procedimentos de segurança da informação

Controle

Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.

Diretrizes para implementação

Convém que os gestores identifiquem como analisar criticamente se os requisitos da segurança da informação estabelecidos nas políticas, procedimentos, normas e outras regulamentações aplicáveis, estão sendo atendidos. Ferramentas de notificação e medições automáticas podem ser consideradas para alcançar uma análise critica regular de forma eficaz.

Se qualquer não conformidade for encontrada com um resultado da análise critica, convém que os gestores:

a) identifiquem as causas da não conformidade;

b) avaliem a necessidade de ações para atender à conformidade;

c) implementem ação corretiva apropriada;

d) analisem criticamente ação corretiva tomada, para verificar a sua eficácia e identificar quaisquer deficiências ou fragilidades.

Convém que os resultados das análises críticas e das ações corretivas realizadas pelos gestores sejam registrados e esses registros sejam mantidos. Convém que os gestores relatem os resultados para as pessoas que estão realizando a análise crítica independente, quando a análise critica independente (ver 18.2.1) for realizada na área de sua responsabilidade.

Informações adicionais

A monitorização operacional de sistemas em uso é apresentada em 12.4.

18.2.3 Análise crítica da conformidade técnica

Controle

Convém que os sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.

Diretrizes para implementação

Convém que a verificação de conformidade técnica seja analisada criticamente, preferencialmente com o apoio de uma ferramenta automática, a qual gera relatórios técnicos para a interpretação do especialistas técnicos. Alternativamente, análises criticas manuais (auxiliado por ferramentas de software apropriadas, se necessário) pode ser realizada por um engenheiro de sistemas experiente.

Se forem usados teste de invasão ou avaliações de vulnerabilidades, convém que sejam tomadas precauções uma vez que tais atividades podem conduzir a um comprometimento da segurança do sistema. Convém que tais testes sejam planejados, documentados e repetidos.

Qualquer verificação de conformidade técnica somente seja executada por pessoas autorizadas e competentes, ou sob a supervisão de tais pessoas.

Informações adicionais

A verificação da conformidade técnica envolve a análise dos sistemas operacionais para garantir que controles de *hardware* e *software* foram corretamente implementados. Este tipo análise critica de conformidade exige conhecimentos técnicos especializados.

Análise de conformidade também engloba, por exemplo, testes de invasão e avaliações de vulnerabilidades, que podem ser realizadas por peritos independentes contratados especificamente para esta finalidade. Isto pode ser útil na detecção de vulnerabilidades no sistema e na verificação do quanto os controles são eficientes na prevenção de acessos não autorizados devido a estas vulnerabilidades.

Os testes de invasão e avaliação de vulnerabilidades fornecem um *snapshot* de um sistema em um estado específico para um tempo específico. O *snapshot* está limitado para aquelas partes do sistema realmente testadas durante a etapa da invasão. O teste de invasão e as avaliações de vulnerabilidades não são um substituto da avaliação de risco.

A ISO/IEC TR 27008 fornece orientações específicas sobre as análises criticas de conformidade técnica.

Bibliografia

[1] Diretiva ABNT, Parte 2, Regras para estrutura e redação de Documentos Técnicos ABNT

[2] ISO/IEC 11770‑1, Information technology Security techniques — Key management — Part 1: Framework

[3] ISO/IEC 11770‑2, Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques

[4] ISO/IEC 11770‑3, Information technology — Security techniques — Key management — Part 3:Mechanisms using asymmetric techniques

[5] ISO 15489‑1, Information and documentation — Records management — Part 1: General

[6] ABNT NBR ISO/IEC 20000‑1:2011, Tecnologia da informação — Gestão de serviços Parte 1: Requisitos do sistema de gestão de serviços

[7] ABNT NBR ISO/IEC 20000‑2:2013, Tecnologia da informação — Gerenciamento de serviços - Parte 2: Guia de aplicação do sistema de gestão de serviços

[8] ABNT NBR ISO 22301:2013, Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos

[9] ISO 22313:2012, Societal security — Business continuity management systems — Guidance

[10] ABNT NBR ISO/IEC 27001, Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos

[11] ABNT NBR ISO/IEC 27005, Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação

[12] ABNT NBR ISO/IEC 27007, Diretrizes para auditoria de sistemas de gestão da segurança da informação

[13] ISO/IEC TR 27008, Information technology — Security techniques — Guidelines for auditors on information security controls

[14] ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[15] ISO/IEC 27033‑1, Information technology — Security techniques — Network security — Part 1: Overview and concepts

[16] ISO/IEC 27033‑2, Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security

[17] ISO/IEC 27033-3, Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

[18] ISO/IEC 27033-4, Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways

[19] ISO/IEC 27033-5, Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Network (VPNs)

[20] ISO/IEC 27035, Information technology — Security techniques — Information security incident management

[21] ISO/IEC 27036-1, Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts

[22] ISO/IEC 27036-2, Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements

[23] ISO/IEC 27036-3, Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security

[24] ISO/IEC 27037, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

[25] ISO/IEC 29100, Information technology — Security techniques — Privacy framework

[26] ISO/IEC 29101, Information technology — Security techniques — Privacy architecture framework

[27] ABNT NBR ISO 31000, Gestão de riscos - Princípios e diretrizes