Cópia não autorizada

ABNT – Associação Brasileira de Normas Técnicas

Sede:
Rio de Janeiro
Av. Treze de Maio, 13 28º andar
CEP 20003-900 – Caixa Postal 1680
Rio de Janeiro – RJ
Tel.: PABX (021) 210-3122
Fax: (021) 220-1762/220-6436
Endereço eletrônico:
www.abnt.org.br

Copyright © 2001,
ABNT–Associação Brasileira
de Normas Técnicas
Printed in Brazil/
Impresso no Brasil
Todos os direitos reservados

AGO 2001 **NBR ISO/IEC 17799**

Tecnologia da informação - Código de prática para a gestão da segurança da informação

Origem: Projeto 21:204.01-010:2001
ABNT/CB-21 - Comitê Brasileiro de Computadores e Processamento de Dados
CE-21:204.01 - Comissão de Estudo de Segurança Física em Instalações de Informática
NBR ISO/IEC 17799 - Information technology - Code of practice for information security management
Descriptors: Information technology. Security
Esta Norma é equivalente à ISO/IEC 17799:2000
Válida a partir de 30.09.2001

Palavras-chave: Tecnologia da informação. Segurança | 56 páginas

Sumário

Prefácio

A ABNT - Associação Brasileira de Normas Técnicas - é o Fórum Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB) e dos Organismos de Normalização Setorial (ABNT/ONS), 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 Projetos de Norma Brasileira, elaborados no âmbito dos ABNT/CB e ABNT/ONS, circulam para Consulta Pública entre os associados da ABNT e demais interessados.

Esta Norma é equivalente à ISO/IEC 17799:2000

Esta Norma contém o anexo A, de cárater informativo.

O anexo A foi incorporado a esta tradução da ISO/IEC 17799:2000, a fim de prestar informações na descrição de termos na língua inglesa mantidos nesta Norma por não possuírem tradução equivalente para a língua portuguesa.

Cópia não autorizada

Introdução

O que é segurança da informação?

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

A informação pode existir em muitas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

A segurança da informação é aqui caracterizada pela preservação de:

a) confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;

b) integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Segurança da informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software.* Estes controles precisam ser estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos.

Por que a segurança da informação é necessária

A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Confidencialidade, integridade e disponibilidade da informação podem ser essenciais para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado.

Cada vez mais as organizações, seus sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças à segurança da informação de uma variedade de fontes, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo ou inundação. Problemas causados por vírus, *hackers* e ataques de *denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

A dependência nos sistemas de informação e serviços significa que as organizações estão mais vulneráveis às ameaças de segurança. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída dificulta a implementação de um controle de acesso centralizado realmente eficiente.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança que pode ser alcançada por meios técnicos é limitada e convém que seja apoiada por gestão e procedimentos apropriados. A identificação de quais controles convém que sejam implantados requer planejamento cuidadoso e atenção aos detalhes. A gestão da segurança da informação necessita, pelo menos, da participação de todos os funcionários da organização. Pode ser que seja necessária também a participação de fornecedores, clientes e acionistas. Consultoria externa especializada pode ser também necessária.

Os controles de segurança da informação são consideravelmente mais baratos e mais eficientes se forem incorporados nos estágios do projeto e da especificação dos requisitos.

Como estabelecer requisitos de segurança

É essencial que uma organização identifique os seus requisitos de segurança. Existem três fontes principais.

A primeira fonte é derivada da avaliação de risco dos ativos da organização. Através da avaliação de risco são identificadas as ameaças aos ativos, as vulnerabilidades e sua probabilidade de ocorrência é avaliada, bem como o impacto potencial é estimado.

A segunda fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender.

A terceira fonte é o conjunto particular de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

Avaliando os riscos de segurança

Os requisitos de segurança são identificados através de uma avaliação sistemática dos riscos de segurança. Os gastos com os controles necessitam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança. As técnicas de avaliação de risco podem ser aplicadas em toda a organização ou apenas em parte dela, assim como em um sistema de informação individual, componentes de um sistema específico ou serviços, quando for viável, prático e útil.

A avaliação de risco é uma consideração sistemática:

a) do impacto nos negócios como resultado de uma falha de segurança, levando-se em conta as potenciais conseqüências da perda de confidencialidade, integridade ou disponibilidade da informação ou de outros ativos;

b) da probabilidade de tal falha realmente ocorrer à luz das ameaças e vulnerabilidades mais freqüentes e nos controles atualmente implementados.

Os resultados dessa avaliação ajudarão a direcionar e determinar ações gerenciais e prioridades mais adequadas para um gerenciamento dos riscos da segurança da informação e a selecionar os controles a serem implementados para a proteção contra estes riscos. Pode ser necessário que o processo de avaliação de riscos e seleção de controles seja executado um determinado número de vezes para proteger as diferentes partes da organização ou sistemas de informação isolados.

Cópia não autorizada

É necessário realizar análises críticas periódicas dos riscos de segurança e dos controles implementados para:

a) considerar as mudanças nos requisitos de negócio e suas prioridades;

b) considerar novas ameaças e vulnerabilidades;

c) confirmar que os controles permanecem eficientes e adequados.

Convém que as análises críticas sejam executadas em diferentes níveis de profundidade, dependendo dos resultados das avaliações de risco feitas anteriormente e das mudanças nos níveis de riscos que a direção considera aceitável para os negócios. As avaliações de risco são sempre realizadas primeiro em nível mais geral, como uma forma de priorizar recursos em áreas de alto risco, e então em um nível mais detalhado, para solucionar riscos específicos.

Seleção de controles

Uma vez tendo sido identificados os requisitos de segurança, convém que os controles sejam selecionados e implementados para assegurar que os riscos são reduzidos a um nível aceitável. Os controles podem ser selecionados a partir desta Norma ou de outro conjunto de controles, ou novos controles podem ser desenvolvidos para atender às necessidades específicas, quando apropriado. Existem diversas maneiras de gerenciar os riscos e esta Norma fornece exemplos para as situações mais comuns. De qualquer forma, é necessário reconhecer que alguns controles não são aplicáveis em todos os sistemas de informação ou ambientes e que podem não ser praticáveis para todas as organizações. Como um exemplo, 8.1.4 descreve como as funções podem ser segregadas para prevenir fraudes e erros. Pode não ser possível para pequenas organizações segregar todas as funções e uma outra maneira de se alcançar o mesmo objetivo de controle pode ser necessária. Como outro exemplo, 9.7 e 12.1 descrevem como o uso de um sistema pode ser monitorado e como as evidências podem ser coletadas. Os controles descritos, por exemplo o registro de eventos, podem ser conflitantes com a legislação vigente, como a proteção da privacidade de clientes ou no local de trabalho.

Convém que os controles sejam selecionados baseados nos custos de implementação em relação aos riscos que serão reduzidos e as perdas potenciais se as falhas na segurança ocorrerem. Convém que fatores não financeiros, como, por exemplo, prejuízos na reputação da organização, sejam também levados em consideração.

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. Eles são explicados em mais detalhes no item “Ponto de partida para a segurança da informação”.

Ponto de partida para a segurança da informação

Um número de controles pode ser considerado como princípios básicos, fornecendo um bom ponto de partida para a implementação da segurança da informação. São baseados tanto em requisitos legais como nas melhores práticas de segurança da informação normalmente usadas.

Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem:

a) proteção de dados e privacidade de informações pessoais (ver 12.1.4);

b) salvaguarda de registros organizacionais (ver 12.1.3);

c) direitos de propriedade intelectual (ver 12.1.2).

Os controles considerados como melhores práticas para a segurança da informação incluem:

a) documento da política de segurança da informação (ver 3.1);

b) definição das responsabilidades na segurança da informação (ver 4.1.3);

c) educação e treinamento em segurança da informação (ver 6.2.1);

d) relatório dos incidentes de segurança (ver 6.3.1);

e) gestão da continuidade do negócio (ver 11.1).

Estes controles se aplicam para a maioria das organizações e na maioria dos ambientes. Convém que seja notado que, embora todos os controles nesta Norma sejam importantes, a relevância de qualquer controle seja determinada à luz de riscos específicos que uma organização está exposta. Por isto, embora o enfoque acima seja considerado um bom ponto de partida, ele não substitui a seleção de controles, baseada na avaliação de risco.

Fatores críticos de sucesso

A experiência tem mostrado que os seguintes fatores são geralmente críticos para o sucesso da implementação da segurança da informação dentro de uma organização:

a) política de segurança, objetivos e atividades, que reflitam os objetivos do negócio;

b) um enfoque para a implementação da segurança que seja consistente com a cultura organizacional;

c) comprometimento e apoio visível da direção;

d) um bom entendimento dos requisitos de segurança, avaliação de risco e gerenciamento de risco;

e) divulgação eficiente da segurança para todos os gestores e funcionários;

Cópia não autorizada

f) distribuição das diretrizes sobre as normas e política de segurança da informação para todos os funcionários e fornecedores;

g) proporcionar educação e treinamento adequados;

h) um abrangente e balanceado sistema de medição, que é usado para avaliar o desempenho da gestão de segurança da informação e obtenção de sugestões para a melhoria.

Desenvolvendo suas próprias recomendações

Esta Norma pode ser considerada como o ponto de partida para o desenvolvimento de recomendações específicas para a organização. Nem todas as recomendações e os controles nesta Norma podem ser aplicados. Além disto, controles adicionais não incluídos nesta Norma podem ser necessários. Quando isto acontecer pode ser útil manter uma referência cruzada para facilitar a verificação da conformidade por auditores e parceiros de negócio.

1 Objetivo

Esta Norma fornece recomendações para gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações. Tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre as organizações. Convém que as recomendações descritas nesta Norma sejam selecionadas e usadas de acordo com a legislação e as regulamentações vigentes.

2 Termos e definições

Para os efeitos desta Norma, aplicam-se as seguintes definições:

2.1 segurança da informação: Preservação da confidencialidade, integridade e disponibilidade da informação.

- **confidencialidade:** Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

- **integridade:** Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

- **disponibilidade:** Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2.2 avaliação de risco: Avaliação das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência.

2.3 gerenciamento de risco: Processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

3 Política de segurança

3.1 Política de segurança da informação

Objetivo: Prover à direção uma orientação e apoio para a segurança da informação.
Convém que a direção estabeleça uma política clara e demonstre apoio e comprometimento com a segurança da informação através da emissão e manutenção de uma política de segurança da informação para toda a organização.

3.1.1 Documento da política de segurança da informação

Convém que um documento da política seja aprovado pela direção, publicado e comunicado, de forma adequada, para todos os funcionários. Convém que este expresse as preocupações da direção e estabeleça as linhas-mestras para a gestão da segurança da informação. No mínimo, convém que as seguintes orientações sejam incluídas:

a) definição de segurança da informação, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação (ver introdução);

b) declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação;

c) breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização, por exemplo:

1) conformidade com a legislação e cláusulas contratuais;

2) requisitos na educação de segurança;

3) prevenção e detecção de vírus e *software* maliciosos;

4) gestão da continuidade do negócio;

5) conseqüências das violações na política de segurança da informação;

d) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança;

e) referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que convém que os usuários sigam.

Convém que esta política seja comunicada através de toda a organização para os usuários na forma que seja relevante, acessível e compreensível para o leitor em foco.

Cópia não autorizada

3.1.2 Análise crítica e avaliação

Convém que a política tenha um gestor que seja responsável por sua manutenção e análise crítica, de acordo com um processo de análise crítica definido. Convém que este processo garanta que a análise crítica ocorra como decorrência de qualquer mudança que venha a afetar a avaliação de risco original, tais como um incidente de segurança significativo, novas vulnerabilidades ou mudanças organizacionais ou na infra-estrutura técnica. Convém que também sejam agendadas as seguintes análises críticas periódicas:

a) efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados;

b) custo e impacto dos controles na eficiência do negócio;

c) efeitos das mudanças na tecnologia.

4 Segurança organizacional

4.1 Infra-estrutura da segurança da informação

Objetivo: Gerenciar a segurança da informação na organização.

Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização.

Convém que fóruns apropriados de gerenciamento com liderança da direção sejam estabelecidos para aprovar a política de segurança da informação, atribuir as funções da segurança e coordenar a implementação da segurança através da organização. Se necessário, convém que uma fonte especializada em segurança da informação seja estabelecida e disponibilizada dentro da organização. Convém que contatos com especialistas de segurança externos sejam feitos para se manter atualizado com as tendências do mercado, monitorar normas e métodos de avaliação, além de fornecer o principal apoio durante os incidentes de segurança. Convém que um enfoque multidisciplinar na segurança da informação seja incentivado, tais como o envolvimento, cooperação e colaboração de gestores, usuários, administradores, projetistas de aplicações, auditores, equipes de segurança e especialistas em áreas como seguro e gerenciamento de risco.

4.1.1 Gestão do fórum de segurança da informação

A segurança da informação é uma responsabilidade de negócios compartilhada por todos os membros da equipe da direção. Convém que seja considerada a criação de um fórum de gestão para garantir um direcionamento claro e um suporte de gestão visível dos envolvidos para as iniciativas de segurança. Convém que este fórum promova a segurança dentro da organização através do comprometimento apropriado e dos recursos adequados. O fórum pode ser parte de um corpo administrativo existente. Tipicamente, tal fórum é responsável pelo seguinte:

a) análise crítica e aprovação da política da segurança da informação e das responsabilidades envolvidas;

b) monitoração das principais mudanças na exposição dos ativos das informações às principais ameaças;

c) análise crítica e monitoração de incidentes de segurança da informação;

d) aprovação das principais iniciativas para aumentar o nível da segurança da informação.

Convém que um gestor seja responsável por todas as atividades relacionadas com a segurança.

4.1.2 Coordenação da segurança da informação

Em grandes organizações um fórum multifuncional com representantes da direção de áreas relevantes da organização pode ser necessário para coordenar a implementação de controles da segurança da informação. Tipicamente, tal fórum:

a) busca as regras e as responsabilidades específicas para a segurança da informação através da organização;

b) busca as metodologias e processos específicos para a segurança da informação, tais como avaliação de risco e sistema de classificação de segurança;

c) busca e apóia iniciativas de segurança da informação aplicáveis por toda a organização, por exemplo programa da conscientização em segurança;

d) garante que a segurança seja parte do processo de planejamento da informação;

e) avalia a adequação e coordena a implementação de controles específicos de segurança da informação para novos sistemas ou serviços;

f) analisa criticamente incidentes de segurança da informação;

g) promove a visibilidade do suporte aos negócios para segurança da informação através da organização.

4.1.3 Atribuição das responsabilidades em segurança da informação

Convém que as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança específicos sejam claramente definidas.

Convém que a política de segurança da informação (ver seção 3) forneça um guia geral sobre a atribuição de regras e responsabilidades de segurança na organização. Convém que seja complementada, onde for necessário, com orientações mais detalhadas para locais, sistemas ou serviços específicos. Convém que sejam claramente definidas as responsabilidades em cada local para os ativos físicos e de informação, bem como dos processos de segurança, como, por exemplo, o plano de continuidade de negócios.

Em muitas organizações um gestor de segurança da informação será indicado para arcar com toda a responsabilidade pelo desenvolvimento e implementação da segurança e pelo suporte à identificação dos controles.

Cópia não autorizada

Contudo, a responsabilidade pela alocação de recursos e pela implementação dos controles geralmente permanece com os gestores. Uma prática comum é indicar um proprietário para cada ativo de informação, tornando responsável pela sua segurança do dia-a-dia.

Os proprietários dos ativos de informação podem delegar suas responsabilidades de segurança a outros gestores ou prestadores de serviço. Todavia o proprietário continua como responsável final pela segurança do ativo e convém que seja capaz de determinar se estão sendo corretamente delegadas as responsabilidades.

É essencial que as áreas pelas quais cada gestor é responsável estejam claramente estabelecidas; em particular recomenda-se que os itens seguintes sejam cumpridos.

a) Convém que os vários ativos e processos de segurança associados com cada sistema sejam identificados e claramente definidos.

b) Convém que o gestor responsável por cada ativo ou processo de segurança esteja de acordo e os detalhes dessa responsabilidade sejam documentados.

c) Convém que os níveis de autorização sejam claramente definidos e documentados.

4.1.4 Processo de autorização para as instalações de processamento da informação

Convém que seja estabelecido um processo de gestão de autorização para novos recursos de processamento da informação.

Recomenda-se que os seguintes controles sejam considerados.

a) Convém que novos recursos tenham aprovação adequada por parte da administração de usuários, autorizando seus propósitos e uso. Convém que a aprovação também seja obtida junto ao gestor responsável pela manutenção do sistema de segurança da informação para garantir que todas as políticas e requisitos de segurança relevantes são atendidos.

b) Convém que o *hardware* e o *software* sejam verificados para garantir que são compatíveis com outros componentes do sistema, onde necessários.

NOTA - Este tipo de aprovação pode ser requerido para certas conexões.

c) Convém que o uso de recursos pessoais de processamento de informação para o processamento de informação de negócio e para quaisquer controles necessários seja autorizado.

d) O uso de recursos pessoais de processamento de informação no ambiente de trabalho pode causar novas vulnerabilidades e, por esta razão, convém que seja avaliado e autorizado.

Estes controles são especialmente importantes em um ambiente de rede de computadores.

4.1.5 Consultoria especializada em segurança da informação

Consultoria especializada em segurança é normalmente necessária em diversas organizações. Em condições ideais, convém que um consultor de segurança da informação interno e com boa experiência forneça isso. Nem todas as organizações desejam empregar um consultor especialista. Nestes casos, é recomendável que seja identificado um colaborador específico para coordenar o conhecimento e as experiências internos para garantir consistência e fornecer auxílio nas tomadas de decisão sobre segurança. Convém que essas organizações também tenham acesso a consultores externos para prover consultoria especializada além da sua própria experiência.

Convém que consultores em segurança da informação ou contatos equivalentes sejam incumbidos de fornecer apoio em todos os aspectos da segurança da informação, utilizando suas próprias experiências ou consultoria externa. A qualidade de suas avaliações das ameaças à segurança e a consultoria nos controles determinarão a eficiência da segurança da informação da organização. Para efetividade e impactos máximos convém que eles tenham permissão de acesso direto à administração em toda a organização.

Convém que o consultor em segurança da informação ou contato equivalente seja consultado o mais cedo possível após suspeitas de incidente ou violação de segurança para fornecer orientações especializadas ou recursos para o processo investigativo. Embora a maioria das investigações de segurança internas normalmente seja executada sob controle da administração, o consultor de segurança da informação pode ser chamado para recomendar, liderar ou conduzir a investigação.

4.1.6 Cooperação entre organizações

Convém que sejam mantidos contatos apropriados com autoridades legais, organismos reguladores, provedores de serviço de informação e operadores de telecomunicações, de forma a garantir que ações adequadas e apoio especializado possam ser rapidamente acionados na ocorrência de incidentes de segurança. De forma similar, convém que a filiação a grupos de segurança e a fóruns setoriais seja considerada.

Convém que trocas de informações de segurança sejam restritas para garantir que informações confidenciais da organização não sejam passadas para pessoas não autorizadas.

4.1.7 Análise crítica independente de segurança da informação

O documento da política de segurança da informação (ver 3.1) estabelece a política e as responsabilidades pela segurança da informação. Convém que a sua implementação seja analisada criticamente, de forma independente, para fornecer garantia de que as práticas da organização refletem apropriadamente a política, e que esta é adequada e eficiente (ver 12.2).

Cópia não autorizada

Tal análise crítica pode ser executada pela auditoria interna, por um gestor independente ou por uma organização prestadora de serviços especializada em tais análises críticas, onde estes possuírem habilidade e experiência apropriadas.

4.2 Segurança no acesso de prestadores de serviços

Objetivo: Manter a segurança dos recursos de processamento de informação e ativos de informação organizacionais acessados por prestadores de serviços.

Convém que seja controlado o acesso de prestadores de serviços aos recursos de processamento da informação da organização.

Onde existir uma necessidade de negócio para este acesso de prestadores de serviços, convém que seja feita uma avaliação dos riscos envolvidos para determinar as possíveis implicações na segurança e os controles necessários. Convém que os controles sejam acordados e definidos através de contrato assinado com os prestadores de serviços.

O acesso de prestadores de serviços pode também envolver outros participantes. Convém que os contratos liberando o acesso de prestadores de serviços incluam a permissão para designação de outros participantes qualificados, assim como as condições de seus acessos.

Esta Norma pode ser utilizada como base para tais contratos e levada em consideração na terceirização do processamento da informação.

4.2.1 Identificação dos riscos no acesso de prestadores de serviços

4.2.1.1 Tipos de acesso

O tipo de acesso dado a prestadores de serviços é de especial importância. Por exemplo, os riscos no acesso através de uma conexão de rede são diferentes dos riscos resultantes do acesso físico. Convém que os seguintes tipos de acesso sejam considerados:

a) acesso físico, por exemplo a escritórios, sala de computadores, gabinetes de cabeamento;

b) acesso lógico, por exemplo aos bancos de dados da organização, sistemas de informação.

4.2.1.2 Razões para o acesso

Acessos a prestadores de serviços podem ser concedidos por diversas razões. Por exemplo, existem prestadores de serviços que fornecem serviços para uma organização e não estão localizados no mesmo ambiente, mas necessitam de acessos físicos e lógicos, tais como:

a) equipes de suporte de *hardware* e *software*, que necessitam ter acesso em nível de sistema ou acesso às funcionalidades de baixo nível nas aplicações;

b) parceiros comerciais ou *joint ventures*, que podem trocar informações, acessar sistemas de informação ou compartilhar bases de dados.

As informações podem ser colocadas em risco pelo acesso de prestadores de serviços com uma administração inadequada da segurança. Existindo a necessidade de negócios de conexão com prestadores de serviços, convém que uma avaliação de risco seja feita para se identificar quaisquer necessidades de implementação de controles de segurança. Convém que sejam levados em conta o tipo de acesso requerido, o valor da informação, os controles empregados por prestadores de serviços e as implicações deste acesso à segurança da informação da organização.

4.2.1.3 Contratados para serviços internos

Prestadores de serviços que, por contrato, devem permanecer dentro da organização por um período de tempo determinado também podem aumentar a fragilidade na segurança. Exemplos de prestadores de serviço dentro da organização incluem:

a) equipes de suporte e manutenção de *hardware* e *software;*

b) pessoal da limpeza, serviços de *buffets*, guardas da segurança e outros serviços de apoio terceirizados;

c) alocação de estagiários e outras contratações de curta duração;

d) consultores.

É essencial entender quais controles são necessários para administrar o acesso de prestadores de serviços aos recursos de processamento da informação. Geralmente, convém que todos os requisitos de segurança resultantes do acesso de prestadores de serviços ou dos controles internos sejam refletidos nos contratos firmados com estes (ver também 4.2.2).

Cópia não autorizada

Por exemplo, caso exista uma necessidade especial por confidencialidade da informação, um acordo de sigilo pode ser utilizado (ver 6.1.3).

Convém que o acesso de prestadores de serviços à informação e aos recursos de processamento da informação não seja permitido até que os controles apropriados sejam implementados e um contrato definindo os termos para a conexão ou acesso seja assinado.

4.2.2 Requisitos de segurança nos contratos com prestadores de serviços

Convém que acordos envolvendo o acesso de prestadores de serviços aos recursos de processamento da informação da organização sejam baseados em contratos formais que contenham, ou façam referência a, todos os requisitos de segurança, de forma a garantir a conformidade com as normas e políticas de segurança da organização. Convém que o contrato garanta que não existam mal-entendidos entre a organização e prestadores de serviços. Convém que as organizações considerem a indenização a ser paga por seus fornecedores em situações de violações de contrato. Convém que os seguintes termos sejam considerados e incluídos nos contratos:

a) a política geral sobre segurança da informação;

b) proteção de ativos, incluindo:

1) procedimentos para proteção dos ativos da organização, incluindo informação e *software*;

2) procedimentos para determinar se houve algum comprometimento destes ativos, por exemplo se houve perda ou modificação de dados;

3) controles para garantir a devolução ou destruição das informações e ativos em um determinado momento durante ou no final do contrato;

4) integridade e disponibilidade;

5) restrições relacionadas com a cópia e divulgação da informação;

c) descrição de cada serviço que deve estar disponível;

d) níveis de serviço desejados e não aceitáveis;

e) condições para transferência da equipe de trabalho, onde for apropriado;

f) as respectivas obrigações dos envolvidos no acordo;

g) responsabilidades com aspectos legais, por exemplo leis de proteção de dados, especialmente levando em consideração diferenças nas legislações vigentes se o contrato envolver a cooperação com organizações de outros países (ver também 12.1);

h) direitos de propriedade intelectual e direitos autorais (ver 12.1.2) e proteção de qualquer trabalho colaborativo (ver também 6.1.3);

i) acordos de controle de acesso, abrangendo:

1) métodos de acesso permitidos e controle e uso de identificadores únicos como ID e senhas de acesso;

2) processo de autorização para acesso e privilégios para os usuários;

3) requisitos para manter uma lista de usuários autorizados a usar os serviços disponibilizados e quais são seus direitos e privilégios;

j) definição de critérios de verificação do desempenho, sua monitoração e registro;

k) direito de monitorar e revogar as atividades de usuários;

l) direito de auditar as responsabilidades contratuais ou ter a auditoria executada por prestadores de serviço;

m) estabelecimento de um processo escalonável para a resolução de problemas; convém que também sejam considerados procedimentos de contingência, onde apropriados;

n) responsabilidades envolvendo a instalação e manutenção de *hardware* e *software*;

o) registros com estrutura clara e formato preestabelecido;

p) procedimentos claros e específicos para gerenciamento de mudanças;

q) quaisquer controles de proteção física e mecanismos necessários para garantir que tais controles estão sendo seguidos;

r) treinamento de administradores e usuários em métodos, procedimentos e segurança;

s) controles que garantam proteção contra *software* malicioso (ver 8.3);

t) requisitos para registro, notificação e investigação de incidentes e violações da segurança;

u) envolvimento de prestadores de serviços com subcontratados.

Cópia não autorizada

4.3 Terceirização

Objetivo: Manter a segurança da informação quando a responsabilidade pelo processamento da informação é terceirizada para uma outra organização.

Convém que o acordo de terceirização considere riscos, controles de segurança e procedimentos para os sistemas de informação, rede de computadores e/ou estações de trabalho no contrato entre as partes.

4.3.1 Requisitos de segurança dos contratos de terceirização

Convém que os requisitos de segurança com prestadores de serviços para gerenciamento e controle de todos ou alguns dos sistemas de informação, redes de computadores e/ou estações de trabalho constem no contrato entre as partes.

Por exemplo, convém que o contrato considere:

a) como os requisitos legais devem ser atendidos, por exemplo a legislação de proteção de dados;

b) quais acordos devem ser estabelecidos para garantir que todas as partes envolvidas na terceirização, incluindo subcontratados, estejam cientes das suas responsabilidades de segurança;

c) como a integridade e a confidencialidade dos ativos organizacionais devem ser mantidas e testadas;

d) quais controles físicos e lógicos serão utilizados para restringir e limitar o acesso de usuários autorizados às informações sensíveis da organização;

e) como a disponibilidade dos serviços será mantida em caso de desastre;

f) quais níveis de segurança física estão sendo fornecidos para equipamentos terceirizados;

g) o direito de auditar.

Convém que os termos descritos em 4.2.2 também façam parte deste contrato. Convém que o contrato permita que os requisitos e procedimentos de segurança possam ser expandidos em um plano de gestão da segurança em comum acordo entre as duas partes.

Embora os contratos de terceirização possam levantar algumas questões complexas de segurança, os controles incluídos nesta Norma podem servir como um ponto de partida para contratos que envolvam a estrutura e o conteúdo do plano de gestão da segurança.

5 Classificação e controle dos ativos de informação

5.1 Contabilização dos ativos

Objetivo: Manter a proteção adequada dos ativos da organização.

Convém que todos os principais ativos de informação sejam inventariados e tenham um proprietário responsável.

O inventário dos ativos ajuda a assegurar que a proteção está sendo mantida de forma adequada. Convém que os proprietários dos principais ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles. A responsabilidade pela implementação dos controles pode ser delegada. Convém que a responsabilidade pela prestação de contas fique com o proprietário nomeado do ativo.

5.1.1 Inventário dos ativos de informação

O inventário dos ativos ajuda a assegurar que as proteções estão sendo feitas de forma efetiva e também pode ser requerido para outras finalidades de negócio, como saúde e segurança, seguro ou financeira (gerenciamento patrimonial). O processo de compilação de um inventário de ativos é um aspecto importante no gerenciamento de risco. Uma organização precisa ser capaz de identificar seus ativos e seus respectivos valores e importância. Baseada nesta informação, uma organização pode então fornecer níveis de proteção proporcionais ao valor e importância desses ativos. Convém que um inventário dos principais ativos associados com cada sistema de informação seja estruturado e mantido. Convém que cada ativo e seu respectivo proprietário sejam claramente identificados e a classificação de segurança (ver 5.2) seja acordada e documentada, juntamente com a sua localização atual (importante quando se tenta recuperar perdas ou danos). Exemplos de ativos associados com sistemas de informação são:

a) ativos de informação: base de dados e arquivos, documentação de sistema, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas;

b) ativos de *software*: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

c) ativos físicos: equipamentos computacionais (processadores, monitores, *laptops*, *modems*), equipamentos de comunicação (roteadores, PABXs, fax, secretárias eletrônicas), mídia magnética (fitas e discos), outros equipamentos técnicos (*no-breaks*, ar-condicionado), mobília, acomodações;

d) serviços: computação e serviços de comunicação, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade, refrigeração.

Cópia não autorizada

5.2 Classificação da informação

Objetivo: Assegurar que os ativos de informação recebam um nível adequado de proteção.

Convém que a informação seja classificada para indicar a importância, a prioridade e o nível de proteção.

A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.

5.2.1 Recomendações para classificação

Convém que a classificação da informação e seus respectivos controles de proteção levem em consideração as necessidades de negócios para compartilhamento ou restrição de informações e os respectivos impactos nos negócios como, por exemplo, o acesso não autorizado ou danos à informação. Em geral, a classificação dada a uma informação é o caminho mais curto para determinar como ela é tratada e protegida.

Convém que informações e resultados de sistemas que processam dados classificados sejam rotulados de acordo com seu valor e sua sensibilidade para a organização. Também pode ser apropriado rotular a informação em termos de quão crítica ela é para a organização como, por exemplo, em termos de integridade e disponibilidade. A informação freqüentemente deixa de ser sensível ou crítica após um 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 a custos adicionais desnecessários. Convém que as regras de classificação previnam e alertem para o fato de que um determinado item de informação não tem necessariamente uma classificação fixa, podendo sofrer modificação de acordo com alguma política predeterminada (ver 9.1).

Convém que cuidados sejam tomados com a quantidade de categorias de classificação e com os benefícios obtidos pelo seu uso. Esquemas excessivamente complexos podem tornar o uso incômodo, inviável economicamente ou impraticável. Convém que atenção especial seja dada na interpretação dos rótulos de classificação sobre documentos de outras organizações, que podem ter definições diferentes para rótulos iguais ou semelhantes aos usados.

Convém que a responsabilidade pela definição da classificação de um item de informação, tais como um documento, registro de dado, arquivo de dados ou disquete, e a análise crítica periódica desta classificação fiquem com o autor ou com o proprietário responsável pela informação.

5.2.2 Rótulos e tratamento da informação

É importante que um conjunto apropriado de procedimentos seja definido para rotular e tratar a informação de acordo com o esquema de classificação adotado pela organização. Estes procedimentos precisam abranger tanto os ativos de informação no formato físico quanto no eletrônico. Para cada classificação, convém que procedimentos de tratamento sejam definidos para abranger os seguintes tipos de atividade de processamento da informação:

a) cópia;

b) armazenamento;

c) transmissão pelo correio, fax ou correio eletrônico;

d) transmissão pela fala, incluindo telefonia móvel, correio de voz ou secretárias eletrônicas;

e) destruição.

Convém que as saídas de sistemas que contêm informações classificadas como sensíveis ou críticas tenham o rótulo apropriado da classificação da informação (na saída). Convém que o rótulo reflita a classificação de acordo com as regras estabelecidas em 5.2.1. Itens que devem ser considerados incluem relatórios impressos, telas, mídias magnéticas (fitas, discos, CDs, cassetes), mensagens eletrônicas e transferências de arquivos.

Rótulos físicos são geralmente a forma mais apropriada de rotular a informação. Entretanto, alguns ativos de informação, como documentos em forma eletrônica, não podem ser fisicamente rotulados, sendo necessário usar um rótulo eletrônico.

6 Segurança em pessoas

6.1 Segurança na definição e nos recursos de trabalho

Objetivo: Reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações.

Convém que responsabilidades de segurança sejam atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a vigência de cada contrato de trabalho.

Convém que candidatos potenciais sejam devidamente analisados (ver 6.1.2), especialmente para trabalhos sensíveis. Convém que todos os funcionários e prestadores de serviço, usuários das instalações de processamento da informação, assinem um acordo de sigilo.

6.1.1 Incluindo segurança nas responsabilidades do trabalho

Convém que regras e responsabilidades de segurança sejam documentadas onde for apropriado, de acordo com a política de segurança da informação da organização (ver 3.1). Convém que elas incluam quaisquer responsabilidades gerais pela implementação ou manutenção da política de segurança, assim como quaisquer responsabilidades específicas para a proteção de determinados ativos ou pela execução de determinados processos ou atividades de segurança.

Cópia não autorizada

6.1.2 Seleção e política de pessoal

Convém que verificações de controle sobre a equipe permanente sejam conduzidas no momento da seleção de candidatos. Recomenda-se que isso inclua o seguinte:

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

b) verificação da exatidão e inteireza das informações do *curriculum vitae* do candidato;

c) confirmação das qualificações acadêmicas e profissionais;

d) verificação da identidade (passaporte ou documento similar).

Onde um trabalho envolver pessoas, tanto por contratação como por promoção, que tenham acesso às instalações de processamento da informação, em particular aquelas que tratam de informações sensíveis, tais como informações financeiras ou informações altamente confidenciais, convém que a organização também faça uma verificação da idoneidade de crédito. Para funcionários que estão em posições com níveis consideráveis de autoridade, convém que este procedimento seja refeito periodicamente.

Convém que um processo similar de seleção seja feito para temporários e fornecedores. Onde esses recursos humanos são fornecidos por uma agência, convém que o contrato especifique claramente as responsabilidades da agência pela seleção e os procedimentos de notificação que devem ser seguidos se a seleção não for devidamente concluída ou quando os resultados obtidos forem motivos de dúvidas ou preocupações.

Convém que a direção avalie a supervisão de funcionários novos e inexperientes com autorização para acesso a sistemas sensíveis. Convém que o trabalho de toda a equipe seja periodicamente revisto e aprovado pelo membro mais experiente da equipe.

Convém que os gestores estejam atentos ao fato de que motivos pessoais de seus funcionários podem afetar o trabalho deles. Problemas pessoais e financeiros, mudanças de comportamento ou estilo de vida, ausências freqüentes e sinais de estresse ou depressão podem levar a fraudes, roubos, erros ou outras implicações de segurança. Convém que esta informação seja tratada de acordo com qualquer legislação apropriada existente na jurisdição pertinente.

6.1.3 Acordos de confidencialidade

Acordos de confidencialidade ou de não divulgação são usados para alertar que a informação é confidencial ou secreta. Normalmente convém que os funcionários assinem tais acordos como parte dos termos e condições iniciais de contratação.

Para colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente (que contenha o acordo de confidencialidade), convém que seja exigida a assinatura do acordo de confidencialidade, antes de ter acesso às instalações de processamento da informação.

Convém que acordos de confidencialidade sejam revisados quando existirem modificações nos termos de contratação, particularmente devido à saída de funcionários da organização ou ao término de contratos.

6.1.4 Termos e condições de trabalho

Convém que os termos e condições de trabalho determinem as responsabilidades dos funcionários pela segurança da informação. Quando apropriado, convém que estas responsabilidades continuem por um período de tempo definido, após o término do contrato de trabalho. Convém que as ações que podem ser tomadas nos casos de desrespeito ao acordo também sejam incluídas no contrato.

Convém que as responsabilidades e direitos legais dos funcionários, tais como leis de direitos autorais ou de proteção de dados, sejam esclarecidos e incluídos dentro dos termos e condições de trabalho. Convém que responsabilidade pela classificação e gestão dos dados do empregador também sejam incluídas. Sempre que apropriado, convém que os termos e condições de trabalho determinem se estas responsabilidades são estendidas fora das dependências da organização e fora do horário normal de trabalho como, por exemplo, nos casos de execução de atividades de trabalho em casa (ver também 7.2.5 e 9.8.1).

6.2 Treinamento dos usuários

Objetivo: Assegurar que os usuários estão cientes das ameaças e das preocupações de segurança da informação e estão equipados para apoiar a política de segurança da organização durante a execução normal do seu trabalho. Convém que usuários sejam treinados nos procedimentos de segurança e no uso correto das instalações de processamento da informação, de forma a minimizar possíveis riscos de segurança.

Cópia não autorizada

6.2.1 Educação e treinamento em segurança da informação

Convém que todos os funcionários da organização e, onde for relevante, prestadores de serviços recebam treinamento apropriado e atualizações regulares sobre as políticas e procedimentos organizacionais. Isto inclui requisitos de segurança, responsabilidades legais e controles do negócio, assim como treinamento sobre o uso correto das instalações de processamento da informação como, por exemplo, procedimentos de acesso ou uso de pacotes de *software*, antes que seja fornecido qualquer acesso aos serviços ou informações.

6.3 Respondendo aos incidentes de segurança e ao mau funcionamento

Objetivo: Minimizar danos originados pelos incidentes de segurança e mau funcionamento, e monitorar e aprender com tais incidentes.

Convém que os incidentes que afetam a segurança sejam reportados através dos canais apropriados o mais rapidamente possível.

Convém que todos os funcionários e prestadores de serviço estejam conscientes dos procedimentos para notificação dos diversos tipos de incidentes (violação da segurança, ameaças, fragilidades ou mau funcionamento) que possam ter impactos na segurança dos ativos organizacionais. Convém que eles sejam solicitados a notificar quaisquer incidentes ocorridos ou suspeitos, tão logo quanto possível, ao ponto de contato designado. Convém que a organização estabeleça um processo disciplinar formal para tratar com os funcionários que cometam violações na segurança. Para ser capaz de lidar com os incidentes de forma apropriada, pode ser necessário coletar evidências o mais rapidamente possível após a sua ocorrência (ver 12.1.7).

6.3.1 Notificação dos incidentes de segurança

Convém que os incidentes de segurança sejam reportados através dos canais apropriados da direção, o mais rapidamente possível.

Convém que um procedimento de notificação formal seja estabelecido, junto com um procedimento de resposta ao incidente, estabelecendo a ação a ser tomada ao se receber uma notificação de incidente. Convém que todos os funcionários e prestadores de serviço estejam conscientes dos procedimentos para notificação de incidentes de segurança e instruídos para relatar tais incidentes, o mais rapidamente possível. Convém que processos de retorno (*feedback*) adequados sejam implementados para assegurar que os incidentes estão notificados com os resultados obtidos após o incidente ser tratado e encerrado. Estes incidentes podem ser usados nos treinamentos de conscientização de usuários (ver 6.2) como exemplos do que pode acontecer, como reagir a tais incidentes e como evitá-los no futuro (ver 12.1.7).

6.3.2 Notificando falhas na segurança

Convém que os usuários dos serviços de informação sejam instruídos a registrar e notificar quaisquer fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou serviços. Convém que eles também notifiquem esses assuntos o mais rapidamente possível para seus superiores ou diretamente para seus provedores de serviços. Convém que os usuários sejam informados de que eles não podem, sob nenhuma circunstância, tentar averiguar uma fragilidade suspeita. Isto é para sua própria proteção, pois a investigação de uma fragilidade pode ser interpretada como potencial uso impróprio do sistema.

6.3.3 Notificando mau funcionamento de *software*

Convém que sejam estabelecidos procedimentos para notificar mau funcionamento de *software*. Recomenda-se que as seguintes ações sejam consideradas.

a) Convém que os sintomas do problema e quaisquer mensagens apresentadas na tela sejam anotados.

b) Convém que o computador seja isolado e, se possível, seu uso deve ser paralisado. Convém que o contato apropriado seja alertado imediatamente. Se o equipamento for examinado, convém que seja desconectado de qualquer rede de computadores antes de ser ligado novamente. Convém que os disquetes não sejam transferidos para outros computadores.

c) Convém que o assunto seja notificado imediatamente ao gestor da segurança da informação.

Convém que os usuários não tentem remover o *software* suspeito, a menos que sejam autorizados. Convém que uma equipe adequadamente treinada e experiente trate da recuperação.

6.3.4 Aprendendo com os incidentes

Convém que existam mecanismos para permitir que tipos, quantidades e custos dos incidentes e dos maus funcionamentos sejam quantificados e monitorados. Convém que esta informação seja usada para identificar incidentes ou maus funcionamentos recorrentes ou de alto impacto. Isto pode indicar a necessidade de melhorias ou controles adicionais para limitar a freqüência, danos e custos de ocorrências futuras ou para ser levado em consideração quando for realizado o processo de análise crítica da política de segurança.

Cópia não autorizada

6.3.5 Processo disciplinar

Convém que exista processo disciplinar formal para os funcionários que tenham violado as políticas e procedimentos de segurança organizacional (ver 6.1.4 e, para retenção de evidências, ver 12.1.7). Tal processo pode dissuadir funcionários que, de outra forma, seriam inclinados a desrespeitar os procedimentos de segurança. Adicionalmente, convém que se assegure um tratamento justo e correto aos funcionários que são suspeitos de cometer violações de segurança, sérias ou persistentes.

7 Segurança física e do ambiente

7.1 Áreas de segurança

Objetivo: Prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização.

Convém que os recursos e instalações de processamento de informações críticas ou sensíveis do negócio sejam mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso. Convém que estas áreas sejam fisicamente protegidas de acesso não autorizado, dano ou interferência.

Convém que a proteção fornecida seja proporcional aos riscos identificados. Políticas de mesa limpa e tela limpa são recomendadas para reduzir o risco de acesso não autorizado ou danos a papéis, mídias, recursos e instalações de processamento de informações.

7.1.1 Perímetro da segurança física

A proteção física pode ser alcançada através da criação de diversas barreiras físicas em torno da propriedade física do negócio e de suas instalações de processamento da informação. Cada barreira estabelece um perímetro de segurança, contribuindo para o aumento da proteção total fornecida. Convém que as organizações usem os perímetros de segurança para proteger as áreas que contêm os recursos e instalações de processamento de dados (ver 7.1.3). Um perímetro de segurança é qualquer coisa que estabeleça uma barreira, por exemplo, uma parede, uma porta com controle de entrada baseado em cartão ou mesmo um balcão de controle de acesso com registro manual. A localização e a resistência de cada barreira dependem dos resultados da avaliação de risco.

Recomenda-se que as seguintes diretrizes e controles sejam considerados e implementados nos locais apropriados.

a) Convém que o perímetro de segurança esteja claramente definido.

b) Convém que o perímetro de um prédio ou local que contenha recursos de processamento de dados seja fisicamente consistente (isto é, não podem existir brechas onde uma invasão possa ocorrer facilmente). Convém que as paredes externas do local possuam construção sólida e todas as portas externas sejam protegidas de forma apropriada contra acessos não autorizados, como, por exemplo, mecanismos de controle, travas, alarmes, grades etc.

c) Convém que uma área de recepção ou outro meio de controle de acesso físico ao local ou prédio seja usado. Convém que o acesso aos locais ou prédios seja restrito apenas ao pessoal autorizado.

d) Convém que barreiras físicas sejam, se necessário, estendidas da laje do piso até a laje superior, para prevenir acessos não autorizados ou contaminação ambiental, como as causadas por fogo e inundações.

e) Convém que todas as portas de incêndio no perímetro de segurança possuam sensores de alarme e mola para fechamento automático.

7.1.2 Controles de entrada física

Convém que as áreas de segurança sejam protegidas por controles de entrada apropriados para assegurar que apenas pessoas autorizadas tenham acesso liberado. Recomenda-se que os seguintes controles sejam considerados.

a) Convém que visitantes das áreas de segurança sejam checados quanto à permissão para ter acesso e tenham registradas data e hora de sua entrada e saída. Convém que essas pessoas obtenham acesso apenas às áreas específicas, com propósitos autorizados e que esses acessos sigam instruções baseadas nos requisitos de segurança e procedimentos de emergência próprios da área considerada.

b) Convém que o acesso às informações sensíveis, instalações e recursos de processamento de informações seja controlado e restrito apenas ao pessoal autorizado. Convém que os controles de autenticação, como, por exemplo, cartões com PIN (número de identificação individual ou *personal identification number*), sejam usados para autorizar e validar qualquer acesso. Convém que, ainda, seja mantida em segurança uma trilha de auditoria contendo todos os acessos ocorridos.

c) Convém que todos os funcionários utilizem alguma forma visível de identificação e sejam incentivados a informar à segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado.

d) Convém que os direitos de acesso às áreas de segurança sejam regularmente revistos e atualizados.

Cópia não autorizada

7.1.3 Segurança em escritórios, salas e instalações de processamento

Uma área de segurança pode ser um escritório fechado ou diversas salas dentro de um perímetro de segurança física, que podem estar fechadas ou podem conter armários fechados ou cofres. Convém que a seleção e o projeto de uma área de segurança levem em consideração as possibilidades de dano causado por fogo, inundações, explosões, manifestações civis e outras formas de desastres naturais ou causados pelo homem. Convém que também sejam levados em consideração as regulamentações e padrões de segurança e saúde. Também devem tratar qualquer ameaça originada em propriedades vizinhas, como por exemplo, vazamento de água de outras áreas.

Recomenda-se que os seguintes controles sejam considerados.

a) Convém que as instalações críticas sejam localizadas de forma a evitar o acesso público.

b) Convém que os prédios sejam sem obstruções em seu acesso, com indicações mínimas do seu propósito, sem sinais óbvios, tanto fora quanto dentro do prédio, da presença de atividades de processamento de informação.

c) Convém que os serviços de suporte e equipamentos, como por exemplo, fotocopiadoras e máquinas de fax, sejam instalados de forma apropriada dentro de áreas de segurança para evitar acesso que possa comprometer a informação.

d) Convém que as portas e janelas sejam mantidas fechadas quando não utilizadas e que sejam instaladas proteções externas, principalmente quando essas portas e janelas se localizarem em andar térreo.

e) Convém que os sistemas de detecção de intrusos sejam instalados por profissionais especializados e testados regularmente, de forma a cobrir todas as portas externas e janelas acessíveis. Convém que as áreas não ocupadas possuam um sistema de alarme que permaneça sempre ativado. Convém que esses cuidados também cubram outras áreas, como, por exemplo, a sala de computadores ou salas de comunicação.

f) Convém que as instalações de processamento da informação gerenciadas pela organização fiquem fisicamente separadas daquelas gerenciadas por prestadores de serviço.

g) Convém que os arquivos e as listas de telefones internos que identificam os locais de processamento das informações sensíveis não sejam de acesso público.

h) Convém que os materiais combustíveis ou perigosos sejam guardados de forma segura a uma distância apropriada de uma área de segurança. Convém que os suprimentos volumosos, como material de escritório, não sejam guardados em uma área de segurança, a menos que requeridos.

i) Convém que os equipamentos de contingência e meios magnéticos de reserva (*back up*) sejam guardados a uma distância segura da instalação principal, para evitar que desastres neste local os afetem.

7.1.4 Trabalhando em áreas de segurança

Manuais e controles adicionais podem ser necessários para melhorar as condições de uma área de segurança. Isto inclui controles tanto para o pessoal da organização como para prestadores de serviços que trabalham em áreas de segurança, assim como para atividades terceirizadas que possam ocorrer nessa área. Recomenda-se que os seguintes itens sejam considerados.

a) Convém que os funcionários só tenham conhecimento da existência de área de segurança ou de atividades dentro dela quando necessário.

b) Convém que se evite trabalho sem supervisão nas áreas de segurança, tanto por razões de segurança como para prevenir oportunidades para atividades maliciosas.

c) Convém que as áreas de segurança desocupadas sejam mantidas fisicamente fechadas e verificadas periodicamente.

d) Convém que pessoal de serviço de suporte terceirizado tenha acesso restrito às áreas de segurança ou às instalações de processamento de informações sensíveis somente quando suas atividades o exigirem. Convém que este acesso seja autorizado e monitorado. Barreiras e perímetros adicionais para controlar o acesso físico podem ser necessários em áreas com diferentes requisitos de segurança dentro de um mesmo perímetro de segurança.

e) Convém que não se permitam o uso de equipamentos fotográficos, de vídeo, de áudio ou de outro equipamento de gravação, a menos que seja autorizado.

7.1.5 Isolamento das áreas de expedição e carga

Convém que as áreas de expedição e de carregamento sejam controladas e, se possível, isoladas das instalações de processamento da informação, com o objetivo de evitar acessos não autorizados. Convém que os requisitos de segurança sejam determinados a partir de uma avaliação de risco. Recomenda-se que os seguintes itens sejam considerados.

a) Convém que o acesso à área de movimentação e suporte (carga e descarga) externa ao prédio seja restrito somente ao pessoal identificado e autorizado.

b) Convém que esta área seja projetada de forma que os suprimentos possam ser descarregados sem que o pessoal responsável pela entrega tenha acesso às outras partes do prédio.

Cópia não autorizada

c) Convém que a(s) porta(s) externa(s) destas áreas seja(m) mantida(s) protegida(s) quando as portas internas estiverem abertas.

d) Convém que o material de entrada seja inspecionado contra potenciais perigos [ver 7.2.1 d)], antes de ser transportado dessa área para a área na qual será utilizado.

e) Convém que o material recebido seja registrado, se apropriado (ver 5.1), quando da sua recepção.

7.2 Segurança dos equipamentos

Objetivo: Prevenir perda, dano ou comprometimento dos ativos, e a interrupção das atividades do negócio.

Convém que os equipamentos sejam fisicamente protegidos contra ameaças à sua segurança e perigos ambientais. A proteção dos equipamentos (incluindo aqueles utilizados fora das instalações físicas da organização) é necessária para reduzir o risco de acessos não autorizados a dados e para proteção contra perda ou dano. Convém que esta proteção considere os equipamentos instalados e os em alienação. Controles especiais podem ser exigidos para proteção contra perigos ou acessos não autorizados e para salvaguardar as instalações de suporte, como o fornecimento de energia elétrica e cabeamento.

7.2.1 Instalação e proteção de equipamentos

Convém que os equipamentos sejam instalados ou protegidos para reduzir o risco de ameaças ambientais, perigos e oportunidades de acesso não autorizado. Recomenda-se que os seguintes itens sejam considerados.

a) Convém que os equipamentos sejam instalados de forma a reduzir acessos desnecessários à área de trabalho.

b) Convém que as instalações de processamento e armazenamento de informação que tratam de informações sensíveis sejam posicionadas de maneira a reduzir riscos de espionagem de informações durante o seu uso.

c) Convém que os itens que necessitem de proteção especial sejam isolados para reduzir o nível geral de proteção exigida.

d) Convém que sejam adotados controles, de forma a minimizar ameaças potenciais, incluindo:

1) roubo;
2) fogo;
3) explosivos;
4) fumaça;
5) água (ou falha de abastecimento);
6) poeira;
7) vibração;
8) efeitos químicos;
9) interferência no fornecimento elétrico;
10) radiação eletromagnética.

e) Convém que uma organização considere políticas específicas para alimentação, bebida e fumo nas proximidades das instalações de processamento da informação.

f) Convém que aspectos ambientais sejam monitorados para evitar condições que possam afetar de maneira adversa a operação das instalações de processamento da informação.

g) Convém que uso de métodos de proteção especial, como capas para teclados, seja considerado para equipamentos em ambiente industrial.

h) Convém que o impacto de um desastre que possa ocorrer nas proximidades da instalação, como, por exemplo, um incêndio em um prédio vizinho, vazamentos de água no telhado ou em andares abaixo do nível do chão ou explosões na rua, também seja considerado.

7.2.2 Fornecimento de energia

Convém que os equipamentos sejam protegidos contra falhas de energia e outras anomalias na alimentação elétrica. Convém que um fornecimento de energia apropriado ocorra em conformidade com as especificações do fabricante do equipamento.

Algumas opções para alcançar a continuidade do fornecimento elétrico incluem:

a) alimentação múltipla para evitar um único ponto de falha no fornecimento elétrico;

b) *no-break* (*Uninterruptable Power Supply - UPS*);

c) gerador de reserva.

Cópia não autorizada

É recomendado o uso de *no-break* em equipamentos que suportem atividades críticas para permitir o encerramento ordenado ou a continuidade do processamento. Convém que os planos de contingência contenham ações a serem tomadas em casos de falha no *no-break*. Convém que esse tipo de equipamento seja periodicamente verificado, de forma a garantir que ele esteja com a capacidade adequada, e testado de acordo com as recomendações do fabricante.

Convém que um gerador de reserva seja considerado se o processamento requer continuidade, em caso de uma falha elétrica prolongada. Se instalados, convém que os geradores sejam testados regularmente de acordo com as instruções do fabricante. Convém que um fornecimento adequado de óleo esteja disponível para assegurar que o gerador possa ser utilizado por um período prolongado.

Adicionalmente, convém que se tenham interruptores elétricos de emergência localizados próximo às saídas de emergência das salas de equipamentos para facilitar o desligamento em caso de emergência. Convém que iluminação de emergência esteja disponível em casos de falha da fonte elétrica primária. Convém que proteção contra relâmpagos seja usada em todos os prédios e que filtros de proteção contra raios sejam instalados para todas as linhas de comunicação externas.

7.2.3 Segurança do cabeamento

Convém que o cabeamento elétrico e de telecomunicação que transmite dados ou suporta os serviços de informação seja protegido contra interceptação ou dano. Recomenda-se que os seguintes controles sejam considerados.

a) Convém que as linhas elétricas e de telecomunicações das instalações de processamento da informação sejam subterrâneas, onde possível, ou sejam submetidas à proteção alternativa adequada.

b) Convém que o cabeamento da rede seja protegido contra interceptações não autorizadas ou danos, por exemplo pelo uso de conduítes ou evitando a sua instalação através de áreas públicas.

c) Convém que os cabos elétricos fiquem separados dos cabos de comunicação para prevenir interferências.

d) Convém que para sistemas críticos ou sensíveis sejam utilizados alguns controles adicionais, tais como:

1) instalação de conduítes blindados e salas ou gabinetes trancados nos pontos de inspeção e terminais;

2) uso de rotas e meios de transmissão alternativos;

3) uso de cabeamento de fibra óptica;

4) varredura inicial para identificar dispositivos não autorizados conectados aos cabos.

7.2.4 Manutenção de equipamentos

Convém que a manutenção correta dos equipamentos garanta a continuidade da disponibilidade e integridade dos mesmos. Recomenda-se que os seguintes itens sejam considerados.

a) Convém que os equipamentos tenham manutenção de acordo com intervalos e especificações do fabricante.

b) Convém que apenas pessoal autorizado execute reparos e serviços nos equipamentos.

c) Convém que se mantenham registros de todas as falhas suspeitas ou ocorridas e de toda manutenção corretiva e preventiva.

d) Convém que controles apropriados sejam utilizados quando do envio de equipamentos para manutenção fora da instalação física (ver também 7.2.6, considerando dados excluídos, apagados e sobrepostos). Convém que todos os requisitos impostos pelas apólices de seguro sejam atendidos.

7.2.5 Segurança de equipamentos fora das instalações

Independentemente de quem seja o proprietário, convém que o uso de qualquer equipamento para o processamento da informação fora das instalações da organização seja autorizado pela direção. Convém que a segurança fornecida seja equivalente àquela oferecida aos equipamentos utilizados dentro da organização para o mesmo propósito, levando-se em conta os riscos de se trabalhar fora das instalações da organização. Os equipamentos de processamento de informação incluem todas as formas de computadores pessoais, agendas eletrônicas, telefones móveis, papéis ou outros, que são levados para se trabalhar em casa ou para fora do ambiente normal de trabalho. Recomenda-se que os seguintes itens sejam considerados.

a) Convém que equipamento e mídias levados para fora das instalações não sejam deixados desprotegidos em áreas públicas. Convém que computadores portáteis sejam carregados como bagagem de mão e disfarçados sempre que possível nas viagens.

b) Convém que as instruções dos fabricantes para proteção dos equipamentos sejam sempre observadas, como, por exemplo, proteção contra exposição a campos magnéticos intensos.

c) Convém que os controles para trabalho em casa sejam determinados através da avaliação de risco e os controles apropriados aplicados conforme a necessidade, como, por exemplo, gabinetes de arquivo fechados, política de mesa limpa e controles de acesso aos computadores.

d) Convém que se use uma cobertura adequada de seguro para proteger os equipamentos existentes fora das instalações da organização.

Os riscos de segurança, como, por exemplo, de dano, roubo e espionagem, podem variar consideravelmente conforme a localização e convém que sejam levados em conta na determinação dos controles mais apropriados. Maiores informações sobre a proteção de equipamentos móveis podem ser encontradas em 9.8.1.

Cópia não autorizada

7.2.6 Reutilização e alienação segura de equipamentos

A informação pode ser exposta pelo descuido na alienação ou reutilização de equipamentos (ver também 8.6.4). Convém que dispositivos de armazenamento que contenham informação sensível sejam destruídos fisicamente ou sobrescritos de forma segura ao invés da utilização de funções-padrão para a exclusão.

Convém que todos os itens de equipamentos que possuem meios de armazenamento, como, por exemplo, discos rígidos, sejam checados para assegurar que toda informação sensível e *software* licenciado foi removido ou sobreposto antes da alienação do equipamento. Dispositivos de armazenamento danificados contendo informações sensíveis, podem necessitar de uma avaliação de riscos para se determinar se tais itens deveriam ser destruídos, reparados ou descartados.

7.3 Controles gerais

Objetivo: Evitar exposição ou roubo de informação e de recursos de processamento da informação.

Convém que informações e recursos de processamento da informação sejam protegidos de divulgação, modificação ou roubo por pessoas não autorizadas, e que sejam adotados controles de forma a minimizar sua perda ou dano. Os procedimentos para manuseio e armazenamento estão considerados em 8.6.3.

7.3.1 Política de mesa limpa e tela limpa

A organização deve considerar a adoção de uma política de mesa limpa para papéis e mídias removíveis e uma política de tela limpa para os recursos de processamento da informação, de forma a reduzir riscos de acesso não autorizado, perda e danos à informação durante e fora do horário normal de trabalho. A política deve levar em consideração as classificações da segurança das informações (ver 5.2), os riscos correspondentes e os aspectos culturais da organização.

As informações deixadas em mesas de trabalho também são alvos prováveis de danos ou destruição em um desastre como incêndio, inundações ou explosões. Recomenda-se que os seguintes controles sejam considerados.

a) Onde for apropriado, convém que papéis e mídias de computador sejam guardados, quando não estiverem sendo utilizados, em gavetas adequadas, com fechaduras e/ou outras formas seguras de mobiliário, especialmente fora do horário normal de trabalho.

b) Informações sensíveis ou críticas ao negócio, quando não forem requeridas, devem ser guardadas, em local distante, de forma segura e fechada (de preferência em um cofre ou arquivo resistente a fogo), especialmente quando o escritório estiver vazio.

c) Computadores pessoais, terminais de computador e impressoras não devem ser deixados ligados quando não assistidos e devem ser protegidos por senhas, chaves ou outros controles quando não estiverem em uso.

d) Pontos de recepção e envio de correspondências e máquinas de fax e telex não assistidas devem ser protegidos.

e) Copiadoras devem ser travadas (ou de alguma forma protegidas contra o uso não autorizado) fora do horário normal de trabalho.

f) Informações sensíveis e classificadas, quando impressas, devem ser imediatamente retiradas da impressora.

7.3.2 Remoção de propriedade

Equipamentos, informações ou *software* não devem ser retirados da organização sem autorização. Quando necessário e apropriado, os equipamentos devem ser desconectados e conectados novamente no seu retorno. Inspeções pontuais devem ser realizadas de forma a detectar a remoção não autorizada de propriedade. As pessoas devem estar cientes de que inspeções pontuais serão realizadas.

8 Gerenciamento das operações e comunicações

8.1 Procedimentos e responsabilidades operacionais

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

Convém que os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações sejam definidos. Isto abrange o desenvolvimento de procedimentos operacionais apropriados e de resposta a incidentes.

Recomenda-se que se utilize a segregação de funções (ver 8.1.4), quando apropriado, para reduzir o risco de uso negligente ou doloso dos sistemas.

8.1.1 Documentação dos procedimentos de operação

Convém que os procedimentos de operação identificados pela política de segurança sejam documentados e mantidos atualizados. Convém que os procedimentos operacionais sejam tratados como documentos formais e que as mudanças sejam autorizadas pela direção.

Convém que os procedimentos especifiquem as instruções para a execução detalhada de cada tarefa, incluindo:

a) processamento e tratamento da informação;

b) requisitos de sincronismo, incluindo interdependências com outros sistemas, a hora mais cedo de início e a hora mais tarde de término das tarefas;

Cópia não autorizada

c) instruções para tratamento de erros ou outras condições excepcionais, que possam ocorrer durante a execução de uma determinada tarefa, incluindo restrições de uso dos recursos do sistema (ver 9.5.5);

d) contato com os técnicos do suporte para o caso de eventos operacionais não esperados ou dificuldades técnicas;

e) instruções para movimentação de saídas de produtos especiais, tais como o uso de formulários especiais ou o tratamento de produtos confidenciais, incluindo procedimentos para a alienação segura de resultados provenientes de rotinas com falhas;

f) procedimento para o reinício e recuperação para o caso de falha do sistema.

Convém que procedimentos documentados sejam também preparados para as atividades de *housekeeping* associadas com os recursos de comunicação e de processamento das informações, tais como procedimentos de inicialização e encerramento de atividades de computadores, geração de cópias de segurança (*back-up*), manutenção de equipamentos, segurança e gestão do tratamento das correspondências e sala de computadores.

8.1.2 Controle de mudanças operacionais

Convém que modificações nos sistemas e recursos de processamento da informação sejam controladas. O controle inadequado de modificações nos sistemas e nos recursos de processamento da informação é uma causa comum de falha de segurança ou de sistema. Convém que exista uma formalização dos procedimentos e das responsabilidades para garantir que haja um controle satisfatório de todas as mudanças de equipamentos, *software* ou procedimentos. Convém que programas que estejam em produção sejam submetidos a um controle específico de modificações. Quando da mudança de programas, convém que seja realizada e mantida uma trilha de auditoria (registro) com todas as informações relevantes. Modificações no ambiente operacional podem causar impacto em aplicações. Sempre que possível, convém que os procedimentos de controle operacional e de aplicações sejam integrados (ver também 10.5.1). Em particular, recomenda-se que os seguintes controles sejam considerados:

a) identificação e registro das modificações significativas;

b) avaliação de impacto potencial de tais mudanças;

c) procedimento formal de aprovação das mudanças propostas;

d) comunicação dos detalhes das modificações para todas as pessoas com envolvimento relevante;

e) procedimentos que identifiquem os responsáveis para a suspensão e recuperação de mudanças no caso de insucesso.

8.1.3 Procedimentos para o gerenciamento de incidentes

Convém que as responsabilidades e procedimentos de gerenciamento de incidentes sejam definidos para garantir uma resposta rápida, efetiva e ordenada aos incidentes de segurança (ver também 6.3.1). Recomenda-se que os seguintes controles sejam considerados:

a) Convém que sejam estabelecidos procedimentos que cubram todos os tipos potenciais de incidentes de segurança, incluindo:

1) falhas dos sistemas de informação e inoperância de serviços;

2) não obtenção de serviço;

3) erros resultantes de dados incompletos ou inconsistentes;

4) violação de confidencialidade.

b) Além dos planos de contingência (projetados para recuperação de sistemas ou serviços com a maior rapidez possível), convém que os procedimentos também contemplem (ver também 6.3.4):

1) análise e identificação das causas do incidente;

2) planejamento e implementação de medidas para prevenir a recorrência, se necessário;

3) coleta de trilhas de auditoria e evidências similares;

4) comunicação com aqueles afetados ou envolvidos na recuperação de incidentes;

5) relato da ação à autoridade apropriada.

c) Convém que trilhas de auditoria e evidências similares sejam coletadas (ver 12.1.7) e mantidas com a devida segurança, para:

1) análise de problemas internos;

2) uso como evidência para o caso de uma potencial violação de contrato ou de normas reguladoras ou em caso de delitos civis ou criminais, por exemplo relacionados ao uso doloso de computadores ou legislação de proteção dos dados;

3) negociação para compensação ou ressarcimento por parte de fornecedores de *software* e serviços.

Cópia não autorizada

d) Recomenda-se que as ações para recuperação de violações de segurança e correção de falhas do sistema sejam cuidadosa e formalmente controladas. Recomenda-se que os procedimentos garantam que:

1) apenas pessoal explicitamente identificado e autorizado esteja liberado para acessar sistemas e dados em produção (ver também 4.2.2 para acesso de prestadores de serviços);

2) todas as ações de emergência adotadas sejam documentadas em detalhe;

3) as ações de emergência sejam relatadas para a direção e analisadas criticamente de maneira ordenada;

4) a integridade dos sistemas do negócio e seus controles sejam validados na maior brevidade.

8.1.4 Segregação de funções

A segregação de funções é um método para redução do risco de mau uso acidental ou deliberado dos sistemas. Convém que a separação da administração ou execução de certas funções, ou áreas de responsabilidade, a fim de reduzir oportunidades para modificação não autorizada ou mau uso das informações ou dos serviços, seja considerada.

As pequenas organizações podem considerar esse método de controle difícil de ser implantado, mas o seu princípio deve ser aplicado tão logo quanto possível e praticável. Onde for difícil a segregação, convém que outros controles, como a monitoração das atividades, trilhas de auditoria e o acompanhamento gerencial, sejam considerados. É importante que a auditoria da segurança permaneça como uma atividade independente.

Convém que sejam tomados certos cuidados para que as áreas nas quais a responsabilidade seja apenas de uma pessoa não venham a ser alvo de fraudes que não possam ser detectadas. Recomenda-se que o início de um evento seja separado de sua autorização. Recomenda-se que os seguintes controles sejam considerados.

a) É importante segregar atividades que requeiram cumplicidade para a concretização de uma fraude, por exemplo a emissão de um pedido de compra e a confirmação do recebimento da compra.

b) Se existir o perigo de conluios, então é necessário o planejamento de controles de modo que duas ou mais pessoas necessitem estar envolvidas, diminuindo dessa forma a possibilidade de conspirações.

8.1.5 Separação dos ambientes de desenvolvimento e de produção

A separação dos ambientes de desenvolvimento, teste e produção é importante para se alcançar a segregação de funções envolvidas. Convém que as regras para a transferência de *software* em desenvolvimento para produção sejam bem definidas e documentadas.

As atividades de desenvolvimento e teste podem causar sérios problemas, como, por exemplo, modificações não autorizadas total ou parcialmente de arquivos ou do sistema. Convém que seja avaliado o nível de separação necessário entre o ambiente de produção e os ambientes de teste e de desenvolvimento, para prevenir problemas operacionais. Convém que uma separação semelhante também seja implementada entre as funções de desenvolvimento e de teste. Nesse caso, é necessária a existência de um ambiente confiável e estável, no qual possam ser executados os testes e que seja capaz de prevenir o acesso indevido do pessoal de desenvolvimento.

Quando o pessoal de desenvolvimento e teste possui acesso ao ambiente de produção, eles podem introduzir códigos não testados ou autorizados, ou mesmo alterar os dados reais do sistema. Em alguns sistemas essa capacidade pode ser mal utilizada para a execução de fraudes, ou introdução de códigos maliciosos ou não testados. Esse tipo de código pode causar sérios problemas operacionais. O pessoal de desenvolvimento e os encarregados dos testes também representam uma ameaça à confidencialidade das informações de produção.

As atividades de desenvolvimento e teste podem causar modificações não intencionais no *software* e a informação se eles compartilham o mesmo ambiente computacional. A separação dos recursos de desenvolvimento, de teste e operacionais é dessa forma bastante desejável para a redução do risco de modificação acidental ou acesso não autorizado ao *software* operacional e dados dos negócios. Recomenda-se que os seguintes controles sejam considerados.

a) Convém que o *software* em desenvolvimento e o *software* em produção sejam, sempre que possível, executados em diferentes processadores, ou diferentes domínios ou diretórios.

b) Convém que as atividades de desenvolvimento e teste ocorram de forma separada, tanto quanto possível.

c) Convém que compiladores, editores e outros programas utilitários não sejam acessíveis a partir do ambiente de produção, quando isso não for uma necessidade.

d) Convém que o processo de acesso ao ambiente de produção seja diferente do acesso de desenvolvimento para reduzir a possibilidade de erro. Convém que os usuários sejam incentivados a usar diferentes senhas para esses ambientes e as telas de abertura exibam mensagens de identificação apropriadas.

e) Convém que o pessoal de desenvolvimento receba senhas para acesso ao ambiente de produção, de forma controlada e apenas para suporte a sistemas no ambiente de produção. Convém que sejam utilizados controles que garantam que tais senhas sejam alteradas após o uso.

Cópia não autorizada

8.1.6 Gestão de recursos terceirizados

O uso de um terceiro para gerenciar processamento da informação pode gerar um aumento do grau de exposição da segurança, tais como a possibilidade de comprometimento, dano ou perda de dados no ambiente do prestador do serviço. Convém que esses riscos sejam previamente identificados e que os controles apropriados sejam acordados com os prestadores de serviços e incluídos no acordo de serviço (ver também 4.2.2 e 4.3 para referências sobre os contratos com prestadores de serviços envolvendo acesso às instalações e ambientes da organização e contratos de terceirização de serviços).

Convém que os tópicos específicos considerados incluam:

a) identificação das aplicações críticas e sensíveis que devem ser processadas internamente;

b) obtenção da aprovação dos gestores ou responsáveis pelos processos e sistemas;

c) implicações nos planos de continuidade do negócio;

d) estabelecimento de normas de segurança e um processo de aferição de conformidade a esses padrões;

e) definição de procedimentos de monitoração e das respectivas responsabilidades, de forma a garantir o acompanhamento das atividades relativas à segurança;

f) procedimentos e responsabilidades para reportar e tratar incidentes de segurança (ver 8.1.3).

8.2 Planejamento e aceitação dos sistemas

Objetivo: Minimizar o risco de falhas nos sistemas.

O planejamento e a preparação prévios são requeridos para garantir a disponibilidade adequada de capacidade e recursos.

Convém que projeções da demanda de recursos e da carga de máquina futura sejam feitas para reduzir o risco de sobrecarga dos sistemas.

Convém que os requisitos operacionais dos novos sistemas sejam estabelecidos, documentados e testados antes da sua aceitação e uso.

8.2.1 Planejamento de capacidade

Convém que as demandas de capacidade sejam monitoradas e que as projeções de cargas de produção futuras sejam feitas de forma a garantir a disponibilidade da capacidade adequada de processamento e armazenamento. Convém que essas projeções levem em consideração os requisitos de novos negócios e sistemas e as tendências atuais e projetadas do processamento de informação da organização.

Os computadores de grande porte necessitam de uma atenção particular, devido ao seu maior custo e o tempo necessário para ampliação de capacidade. Convém que os gestores dos serviços desses computadores monitorem a utilização dos principais recursos destes equipamentos, tais como processadores, memória principal, área de armazenamento de arquivo, impressoras e outros dispositivos de saída, além dos sistemas de comunicação. Convém que eles identifiquem as tendências de utilização, particularmente em relação às aplicações do negócio ou das aplicações de gestão empresarial.

Convém que os gestores utilizem essas informações para identificar e evitar os potenciais gargalos que possam representar ameaças à segurança do sistema ou aos serviços dos usuários, e planejar uma ação apropriada.

8.2.2 Aceitação de sistemas

Convém que sejam estabelecidos critérios de aceitação de novos sistemas, atualizações e novas versões e que sejam efetuados testes apropriados dos sistemas antes da sua aceitação. Convém que os gestores garantam que os requisitos e critérios para aceitação de novos sistemas estejam claramente definidos, acordados, documentados e testados. Recomenda-se que os seguintes controles sejam considerados:

a) requisitos de desempenho e de demanda de capacidade computacional;

b) recuperação de erros, procedimentos de reinicialização e planos de contingência;

c) elaboração e teste de procedimentos operacionais para o estabelecimento de padrões;

d) concordância sobre o conjunto de controles de segurança utilizados;

e) procedimentos manuais eficazes;

f) plano de continuidade de negócios, como requerido em 11.1;

g) evidência de que a instalação do novo sistema não afetará de forma adversa os sistemas já existentes, particularmente nos períodos de pico de demanda de processamento, como, por exemplo, em final de mês;

h) evidência de que tenha sido considerado o impacto do novo sistema na segurança da organização como um todo;

i) treinamento na operação ou uso de novos sistemas.

Para os novos desenvolvimentos principais, convém que os usuários e as funções de operação sejam consultados em todos os estágios do processo de desenvolvimento, de forma a garantir a eficiência operacional do projeto proposto e sua adequação às necessidades organizacionais. Convém que os devidos testes sejam executados para garantir que todos os critérios de aceitação sejam plenamente satisfeitos.

Cópia não autorizada

8.3 Proteção contra *software* malicioso

Objetivo: Proteger a integridade do *software* e da informação.

É necessário que se adotem precauções para prevenir e detectar a introdução de *software* malicioso.

Os ambientes de processamento da informação e os *softwares* são vulneráveis à introdução de *software* malicioso, tais como vírus de computador, cavalos de Tróia (ver também 10.5.4) e outros. Convém que os usuários estejam conscientes sobre os perigos do uso de *software* sem licença ou malicioso, e os gestores devem, onde cabível, implantar controles especiais para detectar ou prevenir contra sua introdução. Em particular, é essencial que sejam tomadas precauções para detecção e prevenção de vírus em computadores pessoais.

8.3.1 Controles contra *software* malicioso

Convém que sejam implantados controles para a detecção e prevenção de *software* malicioso, assim como procedimentos para a devida conscientização dos usuários. Convém que a proteção contra *software* malicioso seja baseada na conscientização da segurança, no controle de acesso adequado e nos mecanismos de gerenciamento de mudanças. Recomenda-se que os seguintes controles sejam considerados:

a) uma política formal exigindo conformidade com as licenças de uso do *software* e proibindo o uso de *software* não autorizado (ver 12.1.2.2);

b) uma política formal para proteção contra os riscos associados com a importação de arquivos e *software*, seja de redes externas ou por qualquer outro meio, indicando quais as medidas preventivas que devem ser adotadas (ver também 10.5, especialmente 10.5.4 e 10.5.5);

c) instalação e atualização regular de *software* de detecção e remoção de vírus para o exame de computadores e meios magnéticos, tanto de forma preventiva como de forma rotineira;

d) análises críticas regulares de *software* e dos dados dos sistemas que suportam processos críticos do negócio. Convém que a presença de qualquer arquivo ou atualização não autorizada seja formalmente investigada;

e) verificação, antes do uso, da existência de vírus em qualquer arquivo em meio magnético de origem desconhecida ou não autorizada, e em qualquer arquivo recebido a partir de redes não confiáveis;

f) 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;

g) procedimentos de gerenciamento e respectivas responsabilidades para tratar da prevenção de vírus no sistema, treinamento nesses procedimentos, relato e recuperação de ataques de vírus (ver 6.3 e 8.1.3);

h) planos de contingência adequados para a recuperação em caso de ataques por vírus, incluindo os procedimentos necessários para salva e recuperação dos dados e *software* (ver seção 11);

i) procedimentos para a verificação de toda informação relacionada a *software* malicioso e garantia de que os 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* antivírus, sejam utilizadas para diferenciar boatos de notícias reais de vírus. Convém que os funcionários estejam capacitados a lidar com boatos e cientes dos problemas decorrentes desses.

Esses controles são especialmente importantes para servidores de arquivo de rede que suportem um grande número de estações de trabalho.

8.4 *Housekeeping*

Objetivo: Manter a integridade e disponibilidade dos serviços de comunicação e processamento da informação.

Convém que sejam estabelecidos procedimentos de rotina para a execução das cópias de segurança e para a disponibilização dos recursos de reserva, conforme definido na estratégia de contingência (ver 11.1), de forma a viabilizar a restauração em tempo hábil, controlando e registrando eventos e falhas e, quando necessário, monitorando o ambiente operacional.

8.4.1 Cópias de segurança

Convém que cópias de segurança dos dados e de *software* essenciais ao negócio sejam feitas regularmente. Convém que recursos e instalações alternativos sejam disponibilizados de forma a garantir que todos os dados e sistemas aplicativos essenciais ao negócio possam ser recuperados após um desastre ou problemas em mídias. Convém que sejam testados regularmente os *backups* de sistemas individuais, de maneira a garantir que satisfaçam os requisitos dos planos de continuidade de negócios (ver seção 11). Recomenda-se que os seguintes controles sejam considerados.

a) Convém que um nível mínimo de cópias de segurança, juntamente com o controle consistente e atualizado dessas cópias e com a documentação dos procedimentos de recuperação, sejam mantidos em local remoto a uma distância suficiente para livrá-los de qualquer dano que possa ocorrer na instalação principal. Convém que no mínimo três gerações ou ciclos de cópias de segurança das aplicações críticas sejam mantidos.

Cópia não autorizada

b) Convém que seja dado às cópias de segurança um nível adequado de proteção física e ambiental (ver seção 7), compatível com os padrões utilizados no ambiente principal. Convém que os controles adotados para as mídias no ambiente principal sejam estendidos para o ambiente de *backup*.

c) Convém que as mídias utilizadas para cópias sejam periodicamente testadas, quando possível, de modo a garantir sua confiabilidade, quando necessário.

d) Convém que os procedimentos de recuperação sejam verificados e testados periodicamente para assegurar que sejam efetivos e que possam ser aplicados integralmente dentro dos prazos alocados para estes procedimentos operacionais de recuperação.

Convém que sejam especificados o período de retenção para informações essenciais ao negócio e também qualquer requerimento para o arquivamento de cópias de segurança com retenção permanente (ver 12.1.3).

8.4.2 Registros de operação

Convém que seja mantido registro das atividades do pessoal de operação. Convém que esses registros incluam, conforme apropriado:

a) horário de início e fim dos processamentos;

b) erros e ações corretivas adotadas nos processamentos;

c) confirmação do correto tratamento dos arquivos de dados e dos resultados gerados nos processamentos;

d) identificação de quem está efetuando a operação.

Convém que os registros de atividades dos operadores sejam submetidos a checagem regular e independente, em conformidade com os procedimentos operacionais.

8.4.3 Registro de falhas

Convém que qualquer tipo de falha seja relatada e que sejam tomadas ações corretivas. Convém que falhas informadas por usuários relativas a problemas com processamento de informação ou sistemas de comunicação sejam registradas. Convém que existam regras claras para o tratamento das falhas informadas, incluindo:

a) análise crítica sobre os registros de falha para assegurar que as falhas foram satisfatoriamente resolvidas;

b) análise crítica sobre as medidas corretivas aplicadas para se assegurar de que elas não tenham comprometido os controles e que as ações adotadas tenham sido devidamente autorizadas.

8.5 Gerenciamento da rede

Objetivo: Garantir a salvaguarda das informações na rede e a proteção da infra-estrutura de suporte.

O gerenciamento da segurança de redes que se estendam além dos limites físicos da organização requer particular atenção.

Também pode ser necessária a utilização de controles adicionais para proteção de dados sensíveis que transitam por redes públicas.

8.5.1 Controles da rede

É necessária a utilização de um conjunto de controles, de forma a obter e preservar a segurança nas redes de computadores. Convém que os gestores implementem controles para garantir a segurança de dados nas redes, assim como a proteção dos serviços disponibilizados contra acessos não autorizados. Particularmente, recomenda-se que os seguintes itens sejam considerados.

a) Convém que a responsabilidade operacional sobre a rede seja segregada da operação dos computadores, onde for apropriado (ver 8.1.4).

b) Convém que sejam estabelecidos procedimentos e responsabilidades para o gerenciamento de equipamentos remotos, incluindo equipamentos nas instalações dos usuários.

c) Quando necessário, convém que sejam estabelecidos controles especiais para salvaguardar a confidencialidade e a integridade dos dados que trafegam por redes públicas, e para proteger os respectivos sistemas (ver 9.4 e 10.3). Controles especiais também podem ser necessários para manter a disponibilidade dos serviços de rede e dos computadores conectados.

d) Convém que as atividades de gerenciamento sejam cuidadosamente coordenadas, de forma a otimizarem o serviço prestado e garantirem que os controles utilizados sejam aplicados de forma consistente por toda a infra-estrutura de processamento da informação.

Cópia não autorizada

8.6 Segurança e tratamento de mídias

Objetivo: Prevenir danos aos ativos e interrupções das atividades do negócio.

Convém que as mídias sejam controladas e fisicamente protegidas.

Convém que procedimentos operacionais apropriados sejam estabelecidos para proteger documentos, mídias magnéticas de computadores (fitas, discos, cartuchos), dados de entrada e saída e documentação dos sistemas contra roubo, acesso não autorizado e danos em geral.

8.6.1 Gerenciamento de mídias removíveis

Convém que existam procedimentos para o gerenciamento de mídias removíveis, como fitas, discos, cartuchos e formulários impressos. Recomenda-se que os controles abaixo sejam considerados.

a) Quando não for mais necessário, convém que se apague o conteúdo de qualquer meio magnético reutilizável que venha a ser retirado da organização.

b) Convém que seja requerida a autorização para remoção de qualquer mídia da organização, assim como mantido o registro dessa remoção como trilha de auditoria (ver 8.7.2).

c) Convém que toda mídia seja guardada em ambiente seguro, de acordo com as especificações do fabricante.

Convém que todos os procedimentos e os níveis de autorização sejam explicitamente documentados.

8.6.2 Descarte de mídias

Convém que as mídias sejam descartadas de forma segura e protegida quando não forem mais necessárias. Informações sensíveis podem ser divulgadas para pessoas de fora da organização através da eliminação de mídias feita sem o devido cuidado. Convém que procedimentos formais para o descarte seguro das mídias sejam definidos para minimizar este risco. Recomenda-se que os controles abaixo sejam considerados.

a) Convém que mídias contendo informações sensíveis sejam guardadas e descartadas de forma segura e protegida, como, por exemplo, através de incineração ou trituração, ou da eliminação dos dados para uso por uma outra aplicação dentro da organização.

b) A lista seguinte identifica itens que podem requerer descarte seguro:

1) documentos em papel;

2) gravação de voz ou de outros tipos;

3) papel-carbono;

4) relatórios impressos;

5) fitas de impressão descartáveis;

6) fitas magnéticas;

7) discos removíveis e cartuchos;

8) meio de armazenamento ótico (todas as formas e incluindo todas as mídias utilizadas pelos fabricantes para distribuição de *software*);

9) listagem de programas;

10) dados de teste;

11) documentação de sistemas.

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 papel, de equipamentos e de mídias magnéticas. Convém que se tenha o cuidado na seleção de um prestador de serviço com experiência e controles adequados.

e) Convém que o descarte de itens sensíveis seja registrado, sempre que possível, para se manter uma trilha de auditoria.

Quando do acúmulo de mídias para descarte, convém que se leve em consideração o efeito proveniente da agregação, tornando mais crítica uma grande quantidade de informação não classificada do que uma pequena quantidade de informação confidencial.

Cópia não autorizada

8.6.3 Procedimentos para tratamento de informação

Convém que sejam estabelecidos procedimentos para o tratamento e o armazenamento de informações, com o objetivo de proteger tais informações contra a divulgação ou uso indevidos. Convém que se estabeleçam procedimentos para o tratamento da informação, consistente com a sua classificação (ver 5.2), em documentos, sistemas de computadores, redes de computadores, computação móvel, comunicação móvel, correio eletrônico, correio de voz, comunicação de voz em geral, multimídia, serviços postais, uso de máquinas de fax e qualquer outro item sensível, como, por exemplo, cheques em branco e faturas. Recomenda-se que os seguintes controles sejam considerados (ver também 5.2 e 8.7.2):

a) tratamento e identificação de todos os meios magnéticos [ver também 8.7.2 a)];

b) restrições de acesso para a identificação de pessoal não autorizado;

c) manutenção de um registro formal dos destinatários autorizados aos dados;

d) garantia de que a entrada de dados seja completa, de que o processamento esteja devidamente concluído e de que a validação das saídas seja aplicada;

e) proteção dos dados preparados para expedição ou impressão de forma consistente com a sua criticidade;

f) armazenamento das mídias em ambientes compatíveis com as especificações dos fabricantes;

g) manutenção da distribuição de dados no menor nível possível;

h) identificação eficaz de todas as cópias de segurança, para chamar a atenção dos destinatários autorizados;

i) análise crítica das listas de distribuição e das listas de destinatários autorizados em intervalos regulares.

8.6.4 Segurança da documentação dos sistemas

A documentação dos sistemas pode conter uma série de informações sensíveis, como, por exemplo, descrições de processos da aplicação, procedimentos, estruturas de dados e processos de autorização (ver também 9.1). Recomenda-se que os seguintes controles sejam considerados para proteger a documentação dos sistemas contra acessos não autorizados.

a) Convém que a documentação dos sistemas seja guardada de forma segura.

b) Convém que a relação de pessoas com acesso autorizado à documentação de sistemas seja a menor possível e autorizada pelo gestor da aplicação.

c) Convém que a documentação de sistema mantida em uma rede pública, ou fornecida através de uma rede pública, seja protegida de forma apropriada.

8.7 Troca de informações e *software*

Objetivo: Prevenir a perda, modificação ou mau uso de informações trocadas entre organizações.

Convém que as trocas de informações e *software* entre organizações sejam controladas e estejam em conformidade com toda a legislação pertinente (ver seção 12).

Convém que as trocas sejam efetuadas baseadas em contratos.

Convém que os procedimentos e padrões para proteger informação e mídias em trânsito também sejam acordados. Convém que sejam consideradas as possíveis implicações nos negócios e na segurança, relacionadas com a troca eletrônica de dados, com o comércio eletrônico, com o correio eletrônico e com a necessidade de controles.

8.7.1 Acordos para a troca de informações e *software*

Convém que os acordos, alguns dos quais podem ser formais, incluindo acordos de distribuição de *software*, quando apropriado, sejam estabelecidos para a troca (eletrônica ou manual) de informação e de *software* entre organizações. Convém que a parte relativa à segurança em tais acordos reflita o nível de sensibilidade das informações envolvidas no negócio. Recomenda-se que os acordos sobre condições de segurança considerem:

a) responsabilidades pelo controle e comunicação de transmissões, expedições e recepções;

b) procedimentos para notificação do emissor, da transmissão, expedição e recepção;

c) padrões técnicos mínimos para embalagem e transmissão;

d) padrões para identificação de portadores;

e) responsabilidades e ônus no caso de perda de dados;

f) utilização de um sistema de identificação para informações críticas e sensíveis, garantindo que o significado dos rótulos seja imediatamente entendido e que a informação esteja devidamente protegida;

g) responsabilidades e propriedade das informações e *software* pela proteção dos dados, em conformidade com os direitos de propriedade de *software* e considerações afins (ver 12.1.2 e 12.1.4);

h) normas técnicas para a gravação e leitura de informações e *software*;

i) quaisquer controles especiais que possam ser necessários para proteção de itens sensíveis, tais como chaves criptográficas (ver 10.3.5).

Cópia não autorizada

8.7.2 Segurança de mídias em trânsito

A informação pode ficar vulnerável a acessos não autorizados, mau uso ou alteração durante o seu transporte físico, como, por exemplo, quando se enviam meios magnéticos através de serviço postal ou de mensageiro. Recomenda-se que os seguintes controles sejam aplicados para salvaguardar as mídias de computador que estão sendo transportadas entre localidades.

a) Convém que utilização de transporte ou de serviço de mensageiro seja confiável. Convém que seja definida uma relação de portadores autorizados em concordância com os gestores e que seja estabelecido um procedimento para a identificação dos portadores.

b) Convém que 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 especificações dos fabricantes.

c) Convém que sejam adotados controles especiais, quando necessário, para proteger informações críticas contra divulgação não autorizada ou modificação. Como exemplo, pode-se incluir:

1) utilização de recipientes lacrados;

2) entrega em mãos;

3) lacre explícito de pacotes (que revele qualquer tentativa de acesso);

4) em casos excepcionais, divisão do conteúdo para mais de uma entrega e expedição por rotas distintas;

5) uso de assinatura digital e de criptografia (ver 10.3).

8.7.3 Segurança do comércio eletrônico

O comércio eletrônico pode envolver o uso de troca eletrônica de dados (EDI), de correio eletrônico e de transações *on-line* através de redes públicas tal como a Internet. O comércio eletrônico é vulnerável a inúmeras ameaças da rede que podem resultar em atividades fraudulentas, violações de contratos e divulgação ou modificação de informação. Convém que controles sejam aplicados para proteger o comércio eletrônico de tais ameaças. Recomenda-se que as considerações de segurança para o comércio eletrônico incluam o seguinte.

a) Autenticação. Qual nível de confiança deve ser requerido pelo cliente e pelo comerciante para se garantir a identidade de cada um deles?

b) Autorização. Quem está autorizado a estabelecer preços, emitir ou assinar documentos comerciais chave? Como os parceiros do negócio tomam conhecimento disto?

c) Contratação e processos de apresentação de propostas. Quais são os requisitos de confidencialidade, integridade e prova de envio e recebimento de documentos-chave e de não repúdio de contratos?

d) Informação de preço. Qual nível de confiança pode-se ter da integridade da lista de preços e na confidencialidade dos acordos de descontos?

e) Transações. Qual a confidencialidade e a integridade dos detalhes do endereço fornecido para o pedido de compra, pagamento e entrega? E da confirmação de recebimento?

f) Investigação. Qual nível de investigação é o mais apropriado para checagem das informações de pagamento fornecidas pelo cliente?

g) Liquidação. Qual é a forma mais apropriada de pagamento para se evitarem fraudes?

h) Pedido de compra. Que tipos de proteção são necessários para se manter a confidencialidade e a integridade da informação do pedido de compra e para se evitar a perda ou duplicação das transações?

i) Responsabilização. Quem responde pelo risco de qualquer transação fraudulenta?

Muitas das considerações feitas acima podem ser solucionadas através da aplicação de técnicas de criptografia apresentadas em 10.3, levando-se em conta a conformidade com os requisitos legais (ver 12.1, especialmente 12.1.6, que trata da legislação sobre criptografia).

Convém que os acordos de comércio eletrônico entre parceiros comerciais sejam baseados em um contrato formal que comprometa as partes com os termos do acordo comercial, incluindo os detalhes de autorização [ver item b) acima]. Outros acordos com fornecedores de serviços de tecnologia de informação e de provedores de rede também podem ser necessários.

Convém que os sistemas comerciais públicos divulguem seus termos comerciais para seus clientes.

Convém que seja considerada a capacidade de resiliência a ataques dos computadores centrais utilizados no comércio eletrônico e a implicações na segurança de qualquer conexão que seja necessária na rede de telecomunicações para sua implementação (ver 9.4.7).

Cópia não autorizada

8.7.4 Segurança do correio eletrônico

8.7.4.1 Riscos de segurança

O correio eletrônico está sendo utilizado para as comunicações comerciais, substituindo meios tradicionais, tais como telex e cartas. O correio eletrônico difere das formas convencionais de comunicação comercial em, por exemplo, velocidade, estrutura da mensagem, grau de informalidade e vulnerabilidade a ações não autorizadas. Convém que se leve em conta a necessidade de controles para se reduzirem os riscos gerados pelo uso do correio eletrônico. Os riscos de segurança incluem:

a) vulnerabilidade das mensagens ao acesso não autorizado, à modificação ou à negação do serviço;

b) vulnerabilidade a erro, como, por exemplo, endereçamento e direcionamento incorretos, e em geral a falta de confiabilidade e disponibilidade do serviço;

c) impacto da mudança do meio de comunicação nos processos do negócio, como, por exemplo, o efeito do aumento da velocidade dos encaminhamentos ou o efeito do envio de mensagens formais no âmbito de pessoa para pessoa ao invés de companhia para companhia;

d) considerações legais relacionadas com a necessidade potencial de prova de origem, envio, entrega e aceitação;

e) implicações da divulgação externa de listas de funcionários;

f) controle sobre o acesso dos usuários remotos às contas de correio eletrônico.

8.7.4.2 Política de uso do correio eletrônico

Convém que as organizações definam uma política clara para a utilização do correio eletrônico, incluindo:

a) ataques ao correio eletrônico, como, por exemplo, por vírus e interceptação;

b) proteção de anexos de correio eletrônico;

c) orientações de quando não se deve utilizar o correio eletrônico;

d) responsabilidades dos funcionários de forma a não comprometer a organização, como, por exemplo, o envio de mensagens difamatórias, uso do correio eletrônico para atormentar pessoas ou fazer compras não autorizadas;

e) uso de técnicas de criptografia para proteger a confidencialidade e integridade das mensagens eletrônicas (ver 10.3);

f) retenção de mensagens que, se guardadas, podem ser descobertas e utilizadas em casos de litígio;

g) controles adicionais para a investigação de mensagens que não puderem ser autenticadas.

8.7.5 Segurança dos sistemas eletrônicos de escritório

Convém que políticas e diretrizes sejam preparadas e implementadas para controlar o negócio e os riscos de segurança associados com os sistemas eletrônicos de escritório. Isso traz oportunidades para a rápida disseminação e compartilhamento de informações, utilizando-se uma combinação de: documentos, computadores, computação móvel, comunicação móvel, correio eletrônico, correio de voz, comunicação de voz em geral, multimídia, serviços postais e máquinas de fax. Convém que as considerações relacionadas com a segurança e com o negócio envolvidas com tal conjunto de recursos incluam:

a) vulnerabilidades da informação nos sistemas de escritório, como, por exemplo, gravação de chamadas telefônicas, confidencialidade das chamadas, armazenamento de faxes, abertura de correio, distribuição de correspondência;

b) política e controles apropriados para gerenciar o compartilhamento de informações, como, por exemplo, o uso de BBS (*Bulletin Board System*) corporativo (ver 9.1);

c) exclusão das categorias de informação sensível ao negócio caso o sistema não forneça o nível de proteção apropriado (ver 5.2);

d) restrição do acesso a informações de trabalho relacionadas com indivíduos específicos, como, por exemplo, grupo de trabalho de projetos sensíveis;

e) adequação, ou outras medidas, dos sistemas que suportam aplicações do negócio, como os de comunicações ou autorizações;

f) categorias de funcionários, fornecedores ou parceiros nos negócios autorizados a usar o sistema e as localidades a partir das quais obtém-se acesso aos mesmos (ver 4.2);

g) restrição do acesso a categorias específicas de usuários;

h) identificação da categoria dos usuários, como, por exemplo, listas dos funcionários da organização ou prestadores de serviço, em benefício de outros usuários;

i) retenção e cópia de segurança das informações mantidas no sistema (ver 12.1.3 e 8.4.1);

j) requisitos e acordos de recuperação e contingência (ver 11.1).

Cópia não autorizada

8.7.6 Sistemas disponíveis publicamente

Convém que se tome cuidado para proteger a integridade da informação divulgada eletronicamente, de forma a prevenir modificações não autorizadas que possam prejudicar a reputação pública da organização. A informação em sistemas disponíveis para o público, como, por exemplo, informações em um servidor acessível através da Internet, pode necessitar estar em conformidade com as leis, normas e regulamentações na jurisdição na qual o sistema esteja localizado ou onde a transação estiver sendo realizada. Convém que exista um processo de autorização formal antes da publicação de uma informação.

Convém que *software*, dados e outras informações que requeiram um alto nível de integridade, expostos em um sistema público, sejam protegidos por mecanismos apropriados, como, por exemplo, assinaturas digitais (ver 10.3.3). Convém que sistemas de publicação eletrônica, especialmente aqueles que permitam retorno (*feedback*) e entrada direta de informações, sejam cuidadosamente controlados, de forma que:

a) a informação seja obtida em conformidade com a legislação relacionada à proteção de dados (ver 12.1.4);

b) a entrada e o processamento de dados sejam feitos de forma completa e no devido tempo;

c) as informações sensíveis sejam protegidas durante o processo de coleta e quando armazenadas;

d) a forma de acesso a sistemas que divulguem informações não permita o acesso casual às redes nas quais esses sistemas estejam conectados.

8.7.7 Outras formas de troca de informação

Convém que sejam definidos procedimentos e controles para proteção da troca de informação através da comunicação verbal, de fax e de vídeo. A informação pode ser comprometida devido à falta de atenção e de políticas e procedimentos adequados à utilização destes recursos, como, por exemplo, através da escuta de conversa quando do uso de um telefone móvel em local público, através da escuta não autorizada de mensagens em secretárias eletrônicas, através do acesso não autorizado a sistemas de correios de voz ou através do envio acidental de fax para pessoas erradas.

As operações de negócio podem ser prejudicadas e a informação pode ser comprometida se os recursos de comunicação falharem, forem sobrecarregados ou interrompidos (ver 7.2 e seção 11). A informação também pode ser comprometida se o acesso a esta for obtido por usuários não autorizados (ver seção 9).

Convém que seja estabelecida uma política clara, dispondo sobre os procedimentos a serem seguidos pelos funcionários, na utilização de comunicação por voz, fax e vídeo. Recomenda-se que isso inclua:

a) relembrar aos funcionários que convém que eles tomem as precauções apropriadas, como, por exemplo, não revelar informações sensíveis ou evitar deixar que suas ligações a partir de locais públicos sejam captadas ou interceptadas por pessoas que se encontram próximas ao telefone utilizado, levando-se em conta:

1) pessoas nas proximidades, principalmente quando se está falando em telefones móveis;

2) interceptação de cabo telefônico e outras formas de escuta através de acesso físico ao aparelho ou à linha telefônica, ou através do uso de receptores que façam o rastreamento da freqüência quando se utilizam telefones móveis analógicos;

3) outras pessoas próximas ao receptor final;

b) relembrar aos funcionários que convém que eles não efetuem conversações sobre assuntos confidenciais em locais públicos ou em escritórios abertos ou em reuniões em salas com paredes finas;

c) não deixar mensagens em secretárias eletrônicas, pois essas podem ser resgatadas por pessoas não autorizadas, armazenadas em sistemas de uso comum ou armazenadas de forma incorreta como resultado de erro de discagem;

d) relembrar aos funcionários sobre os problemas relativos à utilização de equipamentos de fax, a saber:

1) acesso não autorizado às mensagens enviadas ou a serem enviadas;

2) falha intencional ou acidental na programação do envio de faxes;

3) envio de documentos e mensagens para números errados através de discagem incorreta ou da utilização de números errados guardados em memória.

9 Controle de acesso

9.1 Requisitos do negócio para controle de acesso

Objetivo: Controlar o acesso à informação. Convém que o acesso à informação e processos do negócio seja controlado na base dos requisitos de segurança e do negócio. Convém que isto leve em consideração as políticas de autorização e disseminação da informação.

Cópia não autorizada

9.1.1 Política de controle de acesso

9.1.1.1 Requisitos do negócio e política

Convém que os requisitos do negócio para controle de acesso sejam definidos e documentados. Convém que as regras de controle de acesso e direitos para cada usuário ou grupo de usuários estejam claramente estabelecidas no documento da política de controle de acesso. Convém que seja dado aos usuários e provedores de serviço um documento contendo claramente os controles de acesso que satisfaçam os requisitos do negócio.

Recomenda-se que a política leve em conta o seguinte:

a) requisitos de segurança de aplicações específicas do negócio;

b) identificação de toda informação referente às aplicações do negócio;

c) políticas para autorização e distribuição de informação, por exemplo a necessidade de conhecer os princípios e níveis de segurança, bem como a classificação da informação;

d) compatibilidade entre o controle de acesso e as políticas de classificação da informação dos diferentes sistemas e redes;

e) legislação vigente e qualquer obrigação contratual considerando a proteção do acesso a dados ou serviços (ver seção 12);

f) perfil de acesso de usuário-padrão para categorias de trabalho comuns;

g) gerenciamento dos direitos de acesso em todos os tipos de conexões disponíveis em um ambiente distribuído e conectado em rede.

9.1.1.2 Regras de controle de acesso

Na especificação de regras para controle de acesso, convém que alguns cuidados sejam considerados:

a) diferenciação entre as regras que sempre devem ser cumpridas das regras opcionais ou condicionais;

b) estabelecimento de regras baseadas na premissa “Tudo deve ser proibido a menos que expressamente permitido“, ao invés da regra “Tudo é permitido a menos que expressamente proibido”;

c) modificações nos rótulos de informação (ver 5.2) que são atribuídos automaticamente pelos recursos de processamento de dados e dos atribuídos a critério de um usuário;

d) modificações nas permissões de usuários que são atribuídas automaticamente por um sistema de informação daquelas atribuídas por um administrador;

e) diferenciação entre regras que requerem aprovação do administrador ou outro funcionário antes da liberação e aquelas que não necessitam de tal aprovação.

9.2 Gerenciamento de acessos do usuário

Objetivo: Prevenir acessos não autorizados aos sistemas de informação.

Convém que procedimentos formais sejam estabelecidos para controlar a concessão de direitos de acesso aos sistemas de informação e serviços.

Convém que os procedimentos cubram todos os estágios do ciclo de vida de acesso de um usuário, do registro inicial de novos usuários até o registro final de exclusão dos usuários que não mais necessitam ter acesso aos sistemas de informação e serviços. Convém que seja dada atenção especial, onde apropriado, à necessidade de controlar a concessão de direitos de acesso privilegiados, os quais permitem aos usuários sobrepor os controles do sistema.

9.2.1 Registro de usuário

Convém que exista um procedimento formal de registro e cancelamento de usuário para obtenção de acesso a todos os sistemas de informação e serviços multiusuários.

Convém que o acesso aos serviços de informação multiusuário seja controlado através de um processo formal de registro de usuário, que recomenda-se que inclua:

a) utilização de identificador de usuário (ID) único, de forma que cada usuário possa ser identificado e feito responsável por suas ações. Convém que o uso de identificador (ID) de grupo somente seja permitido onde for necessário para a execução do trabalho;

b) verificação de que o usuário tem autorização do proprietário do sistema para a utilização do sistema de informação ou serviço. Aprovação do direito de acesso pelo gestor pode também ser necessária;

c) verificação de que o nível de acesso concedido está adequado aos propósitos do negócio (ver 9.1) e está consistente com a política de segurança da organização, por exemplo não compromete a segregação de funções (ver 8.1.4);

d) entrega de um documento escrito aos usuários sobre seus direitos de acesso;

e) solicitação da assinatura dos usuários indicando que eles entenderam as condições de seus direitos de acesso;

Cópia não autorizada

f) garantia de que o provedor de serviço não fornecerá direitos de acesso até que os procedimentos de autorização sejam concluídos;

g) manutenção de um registro formal de todas as pessoas cadastradas para usar o serviço;

h) remoção imediata dos direitos de acesso de usuários que tenham mudado de função ou saído da organização;

i) verificação periódica para remoção de usuários (ID) e contas redundantes;

j) garantia de que identificadores de usuários (ID) redundantes não sejam atribuídos para outros usuários.

Convém que seja considerada a inclusão de cláusulas nos contratos de funcionários e de serviços que especifiquem as sanções em caso de tentativa de acesso não autorizado por funcionário ou prestador de serviço (ver também 6.1.4 e 6.3.5).

9.2.2 Gerenciamento de privilégios

Convém que a concessão e o uso de privilégios (qualquer característica ou facilidade de um sistema de informação multiusuário que permita ao usuário sobrepor controles do sistema ou aplicação) sejam restritos e controlados. O uso inadequado de privilégios em sistemas é freqüentemente apontado como o maior fator de vulnerabilidade de sistemas.

Convém que sistemas multiusuário que necessitam de proteção contra acesso não autorizado tenham a concessão de privilégios controlada através de um processo de autorização formal. Recomenda-se que os seguintes passos sejam considerados.

a) Convém que os privilégios associados a cada produto do sistema, por exemplo sistema operacional, sistema de gerenciamento de banco de dados e cada aplicação, e as categorias dos funcionários para os quais estes necessitam ser concedidos sejam identificados.

b) Convém que os privilégios sejam concedidos a indivíduos conforme a necessidade de uso ou determinação por eventos, por exemplo os requisitos mínimos para sua função somente quando necessário.

c) Convém que um processo de autorização e um registro de todos os privilégios concedidos sejam mantidos. Convém que os privilégios não sejam fornecidos até que todo o processo de autorização esteja finalizado.

d) Convém que o desenvolvimento e o uso de rotinas do sistema sejam incentivados de forma a evitar a necessidade de fornecer privilégios aos usuários.

e) Convém que privilégios sejam estabelecidos para uma identidade de usuário diferente daquelas usadas normalmente para os negócios.

9.2.3 Gerenciamento de senha dos usuários

Senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a um sistema de informação ou serviço. Convém que a concessão de senhas seja controlada através de um processo de gerenciamento formal, que recomenda-se que considere o seguinte:

a) solicitar aos usuários a assinatura de uma declaração, a fim de manter a confidencialidade de sua senha pessoal e das senhas de grupos de trabalho (isto pode estar incluso nos termos e condições do contrato de trabalho, ver 6.1.4);

b) garantir, onde os usuários necessitam manter suas próprias senhas, que estão sendo fornecidas senhas iniciais seguras e temporárias, o que obriga o usuário a alterá-la imediatamente. Convém que o fornecimento de senhas temporárias para o caso de os usuários esquecerem sua senha seja efetuado somente após a sua identificação positiva;

c) requerer que senhas temporárias sejam dadas aos usuários de forma segura. Convém que o uso de prestadores de serviço ou de mensagens de correio eletrônico desprotegidas (texto claro) seja evitado. Convém que os usuários acusem o recebimento das senhas.

Não convém que senhas sejam armazenadas em sistemas de computador de forma desprotegida (ver 9.5.4). Outras tecnologias para a identificação e autenticação de usuários, tais como reconhecimento biométrico, por exemplo verificação de impressão digital, verificação de assinatura e utilização de *tokens*, como *smart cards*, já estão disponíveis e convém que sejam consideradas, se apropriado.

9.2.4 Análise crítica dos direitos de acesso do usuário

Para manter controle efetivo sobre o acesso aos dados e serviços de informação, convém que o gestor conduza em intervalos regulares de tempo um processo formal de análise crítica dos direitos de acesso dos usuários, de forma que:

a) os direitos de acesso dos usuários sejam analisados criticamente a intervalos regulares (um período de seis meses é recomendado) e após quaisquer mudanças (ver 9.2.1);

b) as autorizações para direitos de acesso privilegiados (ver 9.2.2) sejam analisadas criticamente em intervalos mais freqüentes, sendo recomendado um período de três meses;

c) as concessões de privilégios sejam verificadas em intervalos regulares para garantir que privilégios não autorizados não sejam obtidos.

Cópia não autorizada

9.3 Responsabilidades do usuário

Objetivo: Prevenir acesso não autorizado dos usuários.

A cooperação dos usuários autorizados é essencial para a eficácia da segurança.

Convém que os usuários estejam cientes de suas responsabilidades para a manutenção efetiva dos controles de acesso, considerando particularmente o uso de senhas e a segurança de seus equipamentos.

9.3.1 Uso de senhas

Convém que os usuários sigam as boas práticas de segurança na seleção e uso de senhas.

As senhas fornecem um meio de validação da identidade do usuário e conseqüentemente o estabelecimento dos direitos de acesso para os recursos ou serviços de processamento da informação. Convém que todos os usuários sejam informados para:

a) manter a confidencialidade das senhas;

b) evitar o registro das senhas em papel, a menos que o papel possa ser guardado de forma segura;

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

d) selecionar senhas de qualidade, com um tamanho mínimo de seis caracteres, que sejam:

1) fáceis de lembrar;

2) não baseadas em coisas que outras pessoas possam facilmente adivinhar ou obter a partir de informações pessoais, por exemplo nomes, números telefônicos, datas de nascimento, etc.;

3) isentas de caracteres idênticos consecutivos ou de grupos de caracteres somente numéricos ou alfabéticos.

e) alterar a senha em intervalos regulares ou baseando-se no número de acessos (senhas para contas privilegiadas devem ser alteradas com maior freqüência do que senhas normais) e evitar a reutilização de senhas antigas;

f) alterar senhas temporárias no primeiro acesso ao sistema;

g) não incluir senhas em processos automáticos de acesso ao sistema, por exemplo armazenadas em macros ou teclas de função;

h) não compartilhar senhas individuais.

Se usuários precisarem ter acesso a múltiplas plataformas ou serviços e tiverem que manter várias senhas, convém orientá-los a utilizar uma única senha de qualidade [ver 9.3.1d)] para todos os serviços que proverem um nível razoável de proteção de armazenamento de senhas.

9.3.2 Equipamento de usuário sem monitoração

Convém que os usuários garantam que equipamentos não monitorados tenham proteção apropriada. Equipamentos instalados em áreas de usuário, por exemplo estações de trabalho ou servidores de arquivo, podem necessitar de proteção específica contra acesso não autorizado, quando deixados sem monitoração por um período longo de tempo. Convém que todos os usuários e prestadores de serviço estejam cientes dos requisitos de segurança e dos procedimentos para a proteção de equipamentos não monitorados, bem como suas responsabilidades para implementação de tais proteções. Convém que os usuários sejam informados para:

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

b) efetuar a desconexão com o computador de grande porte quando a sessão for finalizada (não apenas desligar o microcomputador ou terminal, mas utilizar o procedimento para desconexão);

c) proteger microcomputadores ou terminais contra o uso não autorizado através de tecla de bloqueio ou outro controle equivalente, por exemplo senha de acesso, quando não estiverem em uso.

9.4 Controle de acesso à rede

Objetivo: Proteção dos serviços de rede.

Convém que o acesso aos serviços de rede internos e externos seja controlado.

Isto é necessário para garantir que usuários com acesso às redes e aos serviços de rede não comprometam a segurança desses serviços, assegurando:

a) uso de interfaces apropriadas entre a rede da organização e as redes de outras organizações ou redes públicas;

b) uso de mecanismos de autenticação apropriados para usuários e equipamentos;

c) controle de acesso dos usuários aos serviços de informação.

9.4.1 Política de utilização dos serviços de rede

Conexões não seguras a serviços de rede podem afetar toda a organização. Convém que os usuários possuam acesso direto somente aos serviços que eles estão especificamente autorizados para uso. Este controle é particularmente importante para as conexões de rede com aplicações sensíveis ou críticas do negócio ou para usuários que estão em locais de alto risco, como, por exemplo, em áreas públicas ou externas que se encontram fora do controle e da gerência de segurança da organização.

Convém que uma política seja formulada considerando-se o uso de redes e seus serviços. Convém incluir:

a) redes e serviços de rede aos quais o acesso é permitido;

b) procedimentos de autorização para a determinação de quem tem acesso a que redes e a quais serviços de rede;

c) procedimentos e controles de gerenciamento para proteger o acesso às conexões e serviços de rede.

Convém que esta política seja consistente com a política de controle de acesso do negócio (ver 9.1).

9.4.2 Rota de rede obrigatória

O caminho entre o terminal do usuário e o serviço do computador pode necessitar ser controlado. Redes são projetadas para permitir a máxima extensão no compartilhamento de recursos e flexibilidade de roteamento. Estas características podem oferecer também oportunidades para acessos não autorizados às aplicações do negócio ou ao uso não autorizado dos recursos de informação. A incorporação de controles que restringem a rota entre um terminal de usuário e os serviços do computador, aos quais o usuário é autorizado a obter acesso, como, por exemplo, a criação de uma rota forçada, pode reduzir tais riscos.

O objetivo de uma rota forçada é prevenir que qualquer usuário selecione rotas fora da rota entre o terminal do usuário e os serviços para os quais ele está autorizado a obter acesso.

Isto usualmente requer a implementação de um número de controles em diferentes pontos da rota. A idéia é limitar as opções de roteamento para cada ponto da rede através de alternativas predeterminadas.

Exemplos disto são os seguintes:

a) alocação de linhas ou número de telefones dedicados;

b) portas de conexão automática para sistemas de aplicação específicos ou *gateways* de segurança;

c) limitação das opções de menu e submenu para usuários individuais;

d) prevenção de transferência (*roaming*) ilimitada na rede;

e) imposição do uso de sistemas de aplicação específicos e/ou *gateways* de segurança para usuários de redes externas;

f) controle ativo das origens permitidas para comunicação com destinos através de *gateways* de segurança, por exemplo *firewalls;*

g) restrição de acesso à rede através do estabelecimento de domínios lógicos separados, por exemplo redes virtuais privadas, para grupos de usuários dentro da organização (ver também 9.4.6).

Convém que os requisitos para a especificação de rotas (imposição de caminho) sejam baseados na política de controle de acesso do negócio (ver 9.1).

9.4.3 Autenticação para conexão externa do usuário

As conexões externas proporcionam um potencial para acesso não autorizado às informações do negócio, por exemplo acessos através de métodos *dial-up*. Portanto, convém que acessos de usuários remotos estejam sujeitos à autenticação. Existem diferentes métodos de autenticação, alguns deles fornecendo maior nível de proteção que outros, por exemplo métodos baseados no uso de técnicas de criptografia podem fornecer autenticação forte. É importante determinar o nível de proteção requerido a partir de uma avaliação de risco. Isso é necessário para selecionar apropriadamente um método de autenticação.

A autenticação de usuários remotos pode ser alcançada pelo uso, por exemplo, de técnicas baseadas em criptografia, de dispositivos de *tokens* ou de protocolo de desafio/resposta. Linhas privadas dedicadas ou recursos de verificação de endereço de usuário de rede podem também ser utilizados para garantir a origem das conexões.

Controles e procedimentos de discagem reversa (*dial back*), por exemplo uso de *modems* com discagem reversa, podem fornecer proteção contra conexões indesejáveis ou não autorizadas aos recursos de processamento de informação da organização. Este tipo de controle autentica aqueles usuários que tentam estabelecer uma conexão com a rede da organização a partir de uma localização remota. Ao se utilizarem estes controles, convém que uma organização não faça uso de serviços de rede que incluam *call forwarding* ou, se fizer, convém que seja desabilitado o uso de tais facilidades para evitar exposição a fragilidades associadas ao *call forwarding.* É importante também que o processo de discagem reversa inclua a garantia de que uma desconexão efetiva ocorra pelo lado da organização. Caso contrário, o usuário remoto pode manter a linha aberta com a pretensão de que a verificação da chamada reversa tenha ocorrido. Convém que os procedimentos e controles de chamada reversa sejam exaustivamente testados para essa possibilidade.

Cópia não autorizada

9.4.4 Autenticação de nó

A facilidade de conexão automática para um computador remoto pode proporcionar uma forma de se ganhar acesso não autorizado a uma aplicação do negócio. Portanto, convém que as conexões a sistemas remotos de computadores sejam autenticadas. Isto é especialmente importante se a conexão usar uma rede que está fora do controle do gerenciamento de segurança da organização. Alguns exemplos de autenticação e como eles podem ser alcançados são fornecidos em 9.4.3 acima.

A autenticação de nó pode servir como um meio alternativo de autenticação de grupos de usuários remotos, onde eles são conectados a um recurso computacional seguro e compartilhado (ver 9.4.3).

9.4.5 Proteção de portas de diagnóstico remotas

Convém que o acesso às portas de diagnóstico seja seguramente controlado. Muitos computadores e sistemas de comunicação estão instalados com recursos que permitem o diagnóstico remoto por *dial-up* para uso dos engenheiros de manutenção. Se desprotegidas, essas portas de diagnóstico proporcionam um meio de acesso não autorizado. Convém que elas, portanto, sejam protegidas por um mecanismo de segurança apropriado, por exemplo uma chave de bloqueio e um procedimento para garantir que elas sejam acessíveis somente através de um acordo entre o gestor dos serviços computadorizados e o pessoal de suporte de *hardware*/*software* que solicitou o acesso.

9.4.6 Segregação de redes

As redes se estendem cada vez mais além dos limites tradicionais da organização, à medida que as parcerias de negócio são formadas, e podem requerer a interligação ou compartilhamento dos recursos de rede e de processamento de informações. Esta extensão pode aumentar o risco de acessos não autorizados aos sistemas de informação já existentes e que utilizam a rede, e alguns dos quais podem necessitar proteção contra os usuários de uma outra rede por conta de sua criticidade e sensitividade. Nestas circunstâncias, convém que seja considerada a introdução de controles na rede, para segregação de grupos de serviços de informação, de usuários e de sistemas de informação.

Um dos métodos de controlar a segurança de grandes redes é dividi-las em domínios lógicos de rede separados, por exemplo domínios internos e domínios externos, cada um dos quais protegidos por um perímetro de segurança definido. Tal perímetro pode ser implementado com a instalação de um *gateway* seguro entre as duas redes que serão interligadas para controlar o acesso e o fluxo de informações entre os dois domínios. Convém que este *gateway* seja configurado para filtrar o tráfego entre estes dois domínios (ver 9.4.7 e 9.4.8) e para bloquear acessos não autorizados de acordo com a política de controle de acesso da organização (ver 9.1). Um exemplo deste tipo de *gateway* é freqüentemente referenciado como *firewall*.

Convém que o critério para segregação da rede em domínios seja baseado na política de controle de acesso e nos requisitos de acesso (ver 9.1), e também leve em consideração o custo relativo e o impacto no desempenho pela incorporação de roteamento adequado para a rede ou de tecnologia baseada em *gateway* (ver 9.4.7 e 9.4.8).

9.4.7 Controle de conexões de rede

Os requisitos da política de controle de acesso para redes compartilhadas, especialmente aquelas que se estendem além dos limites da organização, podem requerer a incorporação de controles que limitem a capacidade de conexão dos usuários. Tais controles podem ser implementados através de *gateways* de rede que filtram o tráfego por meio de tabelas ou regras predefinidas. Convém que as restrições aplicadas sejam baseadas na política de controle de acesso e nos requisitos das aplicações do negócio (ver 9.1), e sejam mantidas e atualizadas adequadamente.

Exemplos de aplicações nas quais convém que estas restrições sejam aplicadas são:

a) correio eletrônico;

b) transferência unidirecional de arquivos;

c) transferência bidirecional de arquivos;

d) acesso interativo;

e) acesso à rede associado à hora do dia ou à data.

9.4.8 Controle do roteamento de rede

Redes compartilhadas, especialmente aquelas que se estendem através dos limites organizacionais, podem necessitar a incorporação de controles de roteamento que garantam que as conexões de computador e o fluxo de informações não violam a política de controle de acesso das aplicações do negócio (ver 9.1). Este controle é geralmente essencial para redes compartilhadas com prestadores de serviços (usuários que não pertencem ao quadro da organização).

Convém que controles de roteamento sejam baseados em fontes confiáveis e mecanismos de checagem de endereço de destino. A tradução dos endereços de rede também é um mecanismo muito útil para isolar redes e prevenir a utilização de rotas da rede de uma organização para redes de uma outra organização. Eles podem ser implementados em *software* ou *hardware*. Convém que os implementadores estejam cientes do poder de qualquer mecanismo usado.

9.4.9 Segurança dos serviços de rede

Uma ampla variedade de serviços públicos ou privados de rede está disponível, alguns dos quais oferecendo serviços de valor agregado. Os serviços de rede podem ter características de segurança únicas ou complexas. Convém que as organizações que usam serviços de rede se assegurem de que será fornecida uma descrição clara dos atributos de segurança de todos os serviços usados.

Cópia não autorizada

9.5 Controle de acesso ao sistema operacional

Objetivo: Prevenir acesso não autorizado ao computador.

Convém que as funcionalidades de segurança do sistema operacional sejam usadas para restringir o acesso aos recursos computacionais. Convém que estas funcionalidades permitam:

a) identificação e verificação da identidade e, se necessário, do terminal e da localização de cada usuário autorizado;

b) registro dos sucessos e das falhas de acesso ao sistema;

c) fornecimento de meios apropriados para a autenticação; se um sistema de gerenciamento de senhas for usado, convém que ele garanta senhas de qualidade [ver 9.3.1d)];

d) restrição do tempo de conexão dos usuários, quando apropriado;

Outros métodos de controle de acesso, tais como desafio/resposta, podem ser disponibilizados se forem justificados com base nos riscos do negócio.

9.5.1 Identificação automática de terminal

Convém que a identificação automática de terminal seja considerada para autenticar conexões a locais específicos e para equipamentos portáteis. A identificação automática de terminal é uma técnica que pode ser usada quando for importante que uma sessão só possa ser inicializada a partir de uma localização particular ou de um terminal de computador específico. Um identificador de terminal ou um identificador anexado ao terminal pode ser utilizado para indicar se o terminal, em particular, possui permissão para iniciar ou receber transações específicas. Pode ser necessário aplicar proteção física para o terminal, para manter a segurança do identificador. Outras técnicas também podem ser utilizadas para autenticar usuários (ver 9.4.3).

9.5.2 Procedimentos de entrada no sistema (*log-on*)

Convém que o acesso aos serviços de informação seja realizado através de um processo seguro de entrada no sistema (*log-on*). Convém que o procedimento para entrada no sistema de computador seja projetado para minimizar a oportunidade de acessos não autorizados. Convém que o procedimento de entrada no sistema (*log-on*), portanto, divulgue o mínimo de informações sobre o sistema, 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 aplicações até que o processo de entrada no sistema (*log-on*) tenha sido concluído com sucesso;

b) mostre um aviso geral informando que somente pessoas autorizadas devem obter acesso ao computador;

c) não forneça mensagens de ajuda durante o procedimento de entrada no sistema (*log-on*) que poderiam auxiliar um usuário não autorizado;

d) valide a informação de entrada no sistema (*log-on*) apenas quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não deve indicar que parte do dado de entrada está correta ou incorreta;

e) limite o número de tentativas de entradas no sistema (*log-on*) sem sucesso (é recomendado um máximo de três tentativas) e considere:

1) registro das tentativas de acesso inválidas;

2) imposição de tempo de espera antes de permitir novas tentativas de entrada no sistema (*log-on*) ou rejeição de qualquer tentativa posterior de acesso sem autorização específica;

3) encerramento das conexões por *data link*;

f) limite o tempo máximo e mínimo para o procedimento de entrada no sistema (*log-on*). Se excedido, o sistema deverá encerrar o procedimento;

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

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 procedimento efetuado com sucesso.

9.5.3 Identificação e autenticação de usuário

Convém que todos os usuários (incluindo o pessoal de suporte técnico, como operadores, administradores de rede, programadores de sistema e administradores de banco de dados) tenham um identificador único (ID de usuário) para uso pessoal e exclusivo, de modo que as atividades possam ser rastreadas subseqüentemente a um indivíduo responsável. Convém que os identificadores de usuário não forneçam qualquer indicação do nível de privilégio do usuário (ver 9.2.2), por exemplo gestor, supervisor.

Cópia não autorizada

Em circunstâncias excepcionais, onde exista um claro benefício ao negócio, pode ocorrer a utilização de um ID compartilhado por um grupo de usuários ou para um trabalho específico. Convém que a aprovação pelo gestor esteja documentada nestes casos. Controles adicionais podem ser necessários para manutenção das responsabilidades.

Existem vários procedimentos de autenticação, que podem ser usados para confirmar a identidade alegada por um usuário. Senhas (ver também 9.3.1 e itens abaixo) são uma maneira muito comum de se prover identificação e autenticação (I&A), baseadas em um segredo que apenas o usuário conhece. O mesmo pode ser obtido com meios criptográficos e protocolos de autenticação.

Objetos como *tokens* de memória ou *smart card* (cartões inteligentes) que os usuários possuem também podem ser usados para identificação e autenticação. As tecnologias de autenticação biométrica que usam características ou atributos únicos de cada indivíduo também podem ser usadas para autenticar a identidade de uma pessoa. Uma combinação de tecnologias e mecanismos seguramente relacionados resultará em uma autenticação forte.

9.5.4 Sistema de gerenciamento de senhas

A senha é um dos principais meios de validar a autoridade de um usuário para obter acesso a um serviço de computador. Convém que sistemas de gerenciamento de senhas proporcionem facilidade interativa e eficaz que assegure senhas de qualidade (ver 9.3.1 para guiar-se no uso de senhas).

Algumas aplicações requerem que senhas de usuário sejam atribuídas por uma autoridade independente. Na maioria dos casos as senhas são selecionadas e mantidas pelos usuários.

Convém que um bom sistema de gerenciamento de senhas:

a) obrigue o uso de senhas individuais para manter responsabilidades;

b) onde apropriado, 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 como descrito em 9.3.1;

d) onde os usuários mantêm suas próprias senhas, obrigue a troca como descrito em 9.3.1;

e) onde os usuários selecionam senhas, obrigue a troca da senha temporária no primeiro acesso (ver 9.2.3);

f) mantenha registro das senhas anteriores utilizadas, por exemplo para os 12 meses passados, e bloqueie a reutilização de senhas;

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

h) armazene os arquivos de senha separadamente dos dados de sistemas e de aplicação;

i) armazene as senhas na forma cifrada, usando um algoritmo de criptografia unidirecional;

j) altere senhas-padrão fornecidas pelo fabricante, após a instalação do *software*.

9.5.5 Uso de programas utilitários

A maioria das instalações possui um ou mais programas utilitários de sistema que podem ser capazes de sobrepor os controles dos sistemas e aplicações. É essencial que o uso destes programas seja restrito e estritamente controlado. Convém que os seguintes controles sejam considerados:

a) uso de procedimentos de autenticação para utilitários de sistema;

b) segregação dos utilitários de sistema do *software* de aplicação;

c) limitação do uso dos utilitários de sistema a um número mínimo de usuários confiáveis e autorizados;

d) autorização para uso particular dos utilitários de sistema;

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

f) registro de todo o uso de utilitários de sistemas;

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

h) remoção de todo *software* utilitário e de sistemas desnecessários.

9.5.6 Alarme de intimidação para a salvaguarda de usuários

Convém que a provisão de um alarme de intimidação seja considerada para usuários que podem ser alvo de coação. Convém que a decisão de implantar tal alarme seja baseada na avaliação de riscos. Convém que sejam definidos as responsabilidades e os procedimentos para responder a um alarme de intimidação.

Cópia não autorizada

9.5.7 Desconexão de terminal por inatividade

Convém que terminais inativos em locais de alto risco, por exemplo em áreas públicas ou externas fora dos limites do gerenciamento de segurança da organização, ou servindo a sistemas de alto risco, sejam desligados automaticamente após um período predeterminado de inatividade para prevenir o acesso de pessoas não autorizadas. Convém que este recurso de desconexão por tempo preveja a limpeza da tela do terminal e o encerramento das sessões do aplicativo e da rede após um período definido de inatividade. Convém que o prazo de tempo para o desligamento reflita os riscos de segurança da área e dos usuários do terminal.

Uma forma limitada para desconexão de terminal pode ser provida por alguns microcomputadores que limpam a tela e previnem acesso não autorizado, mas não fecham as sessões das aplicações ou da rede.

9.5.8 Limitação do tempo de conexão

Convém que restrições nos horários de conexão proporcionem segurança adicional para aplicações de alto risco. Limitando o período durante o qual as conexões de terminal são permitidas para os serviços computadorizados, se reduz a janela de oportunidade para acessos não autorizados. Convém que tal controle seja considerado para aplicações computacionais sensíveis, especialmente aquelas com terminais instalados em locais de alto risco, por exemplo em áreas públicas ou externas fora dos limites do gerenciamento de segurança da organização. Exemplos deste tipo de restrição incluem:

a) utilização de blocos de tempo predeterminados, por exemplo para transmissão de arquivos em lote ou sessões regulares interativas de curta duração;

b) restrição dos horários de conexão às horas normais de expediente, se não houver necessidades para horas extras ou trabalhos fora do horário normal.

9.6 Controle de acesso às aplicações

Objetivo: Prevenir acesso não autorizado à informação contida nos sistemas de informação.

Convém que os recursos de segurança sejam utilizados para restringir o acesso aos sistemas de aplicação.

Convém que o acesso lógico a *software* e informação seja restrito a usuários autorizados. Convém que os sistemas de aplicação:

a) controlem o acesso dos usuários à informação e às funções dos sistemas de aplicação, de acordo com uma política definida de controle de acesso do negócio;

b) proporcionem proteção contra acesso não autorizado para qualquer *software* utilitário e de sistema operacional que seja capaz de sobrepor os controles das aplicações ou do sistema;

c) não comprometam a segurança de outros sistemas com os quais os recursos de informação são compartilhados;

d) sejam capazes de dar acesso à informação apenas ao seu proprietário, a outros indivíduos nominalmente autorizados ou a determinados grupos de usuários.

9.6.1 Restrição de acesso à informação

Convém que os usuários dos sistemas de aplicação, incluindo o pessoal de suporte, sejam providos de acesso à informação e às funções dos sistemas de aplicação de acordo com uma política de controle de acesso definida, baseada nos requisitos das aplicações individuais do negócio e consistente com a política de acesso à informação organizacional (ver 9.1). Convém que a aplicação dos seguintes controles seja considerada de forma a suportar os requisitos de restrição de acesso:

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

b) restringindo o conhecimento do usuário sobre informações ou funções de aplicação do sistema às quais ele não tem autoridade de acesso, com a publicação apropriada de documentação para o usuário;

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

d) assegurando que as saídas dos sistemas de aplicação que tratam informações sensíveis contenham apenas informações que sejam relevantes ao uso de tal saída e são enviadas apenas para os terminais e locais autorizados, incluindo análise crítica periódica de tais saídas para garantir que as informações redundantes são removidas.

9.6.2 Isolamento de sistemas sensíveis

Os sistemas sensíveis podem requerer um ambiente computacional dedicado (isolado). Alguns sistemas de aplicação são suficientemente sensíveis a perdas potenciais, requerendo tratamento especial. A sensibilidade pode indicar que convém que o sistema de aplicação seja executado a partir de um computador dedicado e que somente compartilhe recursos com sistemas de aplicação confiáveis ou não tenha limitações. As seguintes considerações aplicam-se.

a) Convém que a sensibilidade de um sistema de aplicação seja explicitamente identificada e documentada pelo proprietário da aplicação (ver 4.1.3).

b) Quando uma aplicação sensível é executada em um ambiente compartilhado, convém que se identifiquem os sistemas de aplicação com os quais ela compartilhará recursos e se obtenha a concordância do proprietário da aplicação sensível.

Cópia não autorizada

9.7 Monitoração do uso e acesso ao sistema

Objetivo: Descobrir atividades não autorizadas.

Convém que os sistemas sejam monitorados para detectar divergências entre a política de controle de acesso e os registros de eventos monitorados, fornecendo evidências no caso de incidentes de segurança.

A monitoração do sistema permite que sejam verificadas a efetividade dos controles adotados e a conformidade com o modelo de política de acesso (ver 9.1).

9.7.1 Registro (*log*) de eventos

Convém que trilhas de auditoria registrando as exceções e outros eventos de segurança relevantes sejam produzidas e mantidas por um período de tempo acordado para auxiliar em investigações futuras e na monitoração do controle de acesso. Convém que os registros (*log*) de auditoria também incluam:

a) identificação dos usuários;

b) datas e horários de entrada (*log-on*) e saída (*log-off*) no sistema;

c) identidade do terminal ou, quando possível, a sua localização;

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

e) registros das tentativas de acesso a outros recursos e dados aceitas e rejeitadas.

Certos registros (*log*) de auditoria podem ser guardados como parte da política de retenção de registros ou devido aos requisitos para a coleta de evidência (ver também a seção 12).

9.7.2 Monitoração do uso do sistema

9.7.2.1 Procedimentos e áreas de risco

Convém que sejam estabelecidos procedimentos para a monitoração do uso dos recursos de processamento da informação. Tais procedimentos são necessários para garantir que os usuários estão executando apenas as atividades para as quais eles foram explicitamente autorizados. Convém que o nível de monitoração requerido para os recursos individuais seja determinado através de uma avaliação de risco. As áreas que devem ser consideradas incluem:

a) acessos autorizados, incluindo detalhes do tipo:
   1) a identificação (ID) do usuário;
   2) a data e o horário dos eventos-chave;
   3) tipo do evento;
   4) os arquivos cujo acesso foi obtido;
   5) os programas ou utilitários utilizados;

b) todas as operações privilegiadas, tais como:
   1) utilização de conta de supervisor;
   2) inicialização e finalização do sistema;
   3) a conexão e a desconexão de dispositivos de entrada e saída;

c) tentativas de acesso não autorizado, tais como:
   1) tentativas que falharam;
   2) violação da política de acesso e notificações para *gateways* e *firewalls* da rede;
   3) alertas dos sistemas proprietários de detecção de intrusão;

d) alertas e falhas do sistema, tais como:
   1) alertas ou mensagens do console;
   2) registro das exceções do sistema;
   3) alarmes do gerenciamento da rede.

9.7.2.2 Fatores de risco

Convém que o resultado das atividades de monitoração seja analisado criticamente em intervalos regulares. Convém que a freqüência da análise crítica dependa dos riscos envolvidos. Convém que os fatores de risco que devem ser considerados incluam:

a) criticidade dos processos de aplicação;

b) valor, sensibilidade ou criticidade da informação envolvida;

c) experiência anterior com infiltrações e uso impróprio do sistema;

d) extensão da interconexão dos sistemas (particularmente com redes públicas).

Cópia não autorizada

9.7.2.3 Registro e análise crítica dos eventos

A análise crítica dos registros (*logs*) envolve a compreensão das ameaças encontradas no sistema e a maneira pela qual isto pode acontecer. Exemplos de eventos que podem requerer uma maior investigação em casos de incidentes de segurança são comentados em 9.7.1.

Registros (*logs*) de sistema normalmente contêm um grande volume de informações, e muitas das quais não dizem respeito à monitoração da segurança. Para ajudar a identificar eventos significativos para propósito de monitoração de segurança, convém que a cópia automática dos tipos de mensagens apropriadas para um segundo registro (log) e/ou o uso de utilitários de sistema apropriados ou ferramentas de auditoria para a execução de consulta sejam considerados.

Quando forem alocadas as responsabilidades pela análise crítica dos registros (*logs*), convém que seja considerada uma separação entre as funções da(s) pessoa(s) que conduz(em) a análise crítica daquelas cujas atividades estão sendo monitoradas.

Convém que atenção especial seja dada à segurança dos recursos do registro (*log*) porque, se adulterados, podem prover uma falsa impressão de segurança. Convém que os controles objetivem a proteção contra modificações não autorizadas e problemas operacionais, incluindo:

a) desativação das facilidades de registro (*log*);

b) alterações dos tipos de mensagens que são gravadas;

c) arquivos de registros (*logs*) sendo editados ou excluídos;

d) esgotamento do meio magnético do arquivo de registros (*logs*), falhas no registro de eventos ou sobreposição do próprio arquivo.

9.7.3 Sincronização dos relógios

O estabelecimento correto dos relógios dos computadores é importante para garantir a exatidão dos registros de auditoria, que podem ser requeridos por investigações ou como evidências em casos legais ou disciplinares. Registros de auditoria incorretos podem impedir tais investigações e causar danos à credibilidade das evidências.

Onde um computador ou dispositivo de comunicação tiver a capacidade para operar um relógio (*clock*) de tempo real, convém que ele seja ajustado conforme o padrão acordado, por exemplo o tempo coordenado universal (*Universal Co-ordinated time* - UCT) ou um padrão local de tempo. Como alguns relógios são conhecidos pela sua variação durante o tempo, convém que exista um procedimento que verifique esses tipos de inconsistências e corrija qualquer variação significativa.

9.8 Computação móvel e trabalho remoto

Objetivo: Garantir a segurança da informação quando se utilizam a computação móvel e os recursos de trabalho remoto.

Convém que a proteção requerida seja proporcional com o risco desta forma específica de trabalho. Quando se utiliza a computação móvel, convém que os riscos de trabalhar em um ambiente desprotegido sejam considerados e a proteção adequada seja aplicada. No caso de trabalho remoto, convém que a organização aplique proteção ao local do trabalho remoto e garanta que os arranjos adequados foram feitos para este tipo de trabalho.

9.8.1 Computação móvel

Quando se utilizam recursos da computação móvel, por exemplo *notebooks*, *palmtops*, *laptops* e telefones celulares, convém que cuidados especiais sejam tomados para garantir que a informação do negócio não está comprometida. Convém que uma política formal seja adotada levando em conta os riscos de trabalhar com os recursos de computação móvel, particularmente em ambientes desprotegidos. Por exemplo, convém que tais políticas incluam os requisitos para proteção física, controles de acesso, técnicas criptográficas, cópias de segurança e proteção contra vírus. Convém que esta política inclua também regras e avisos sobre a conexão de recursos móveis à rede e orientação sobre o uso destes recursos em locais públicos.

Convém que sejam tomadas certas precauções ao se utilizarem os recursos de computação móvel em locais públicos, salas de reuniões e outras áreas desprotegidas fora dos limites da organização. Convém que sejam estabelecidas proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nestes recursos, por exemplo através da utilização de técnicas de criptografia (ver 10.3).

É importante que, quando tais recursos forem utilizados em locais públicos, seja tomado cuidado para evitar o risco de captação por pessoas não autorizadas. Convém que também sejam estabelecidos procedimentos contra *software* malicioso, mantendo-os sempre atualizados (ver 8.3). Convém que equipamentos estejam disponíveis para possibilitar uma recuperação rápida e fácil das informações. Para essas recuperações, convém que sejam dadas proteções adequadas contra, por exemplo, roubo ou perda de informação.

Cópia não autorizada

Convém que proteção adequada seja dada para o uso dos recursos de computação móvel conectados em rede. Convém que o acesso remoto às informações do negócio através de redes públicas, usando os recursos de computação móvel, ocorra apenas após o sucesso da identificação e da autenticação, e com os mecanismos de controle de acesso apropriados implantados (ver 9.4).

Convém que os recursos de computação móvel também estejam 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 os equipamentos que contêm informações importantes, sensíveis e/ou críticas para o negócio nunca sejam deixados sem observação e, quando possível, sejam fisicamente trancados, ou convém que travas especiais sejam utilizadas de forma a manter o equipamento seguro. Maiores informações sobre a proteção física de equipamentos móveis podem ser encontradas em 7.2.5.

Convém que seja preparado treinamento para o grupo de trabalho que utiliza a computação móvel, para aumentar o nível de conscientização a respeito dos riscos adicionais resultantes desta forma de trabalho e dos controles que devem ser implementados.

9.8.2 Trabalho remoto

O trabalho remoto utiliza tecnologia de comunicação para permitir que funcionários trabalhem remotamente a partir de uma localização física fora da sua organização. Convém que a proteção apropriada do local do trabalho remoto seja implantada para evitar, por exemplo, o roubo do equipamento e de informações, a divulgação não autorizada de informação, o acesso remoto não autorizado aos sistemas internos da organização ou o uso impróprio destes recursos. É importante que o trabalho remoto seja tanto autorizado quanto controlado pelo gestor e que as providências adequadas a esta forma de trabalho tenham sido tomadas.

Convém que as organizações considerem o desenvolvimento de políticas, procedimentos e normas para controlar as atividades do trabalho remoto. Convém que as organizações somente autorizem as atividades de trabalho remoto se existirem controles e acordos de segurança apropriados e em vigor e que estejam em conformidade com a política de segurança da organização. Recomenda-se considerar o seguinte:

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

b) o ambiente proposto de trabalho remoto;

c) os requisitos de segurança nas comunicações, levando em conta a necessidade do acesso remoto para os sistemas internos da organização, a sensibilidade das informações que serão acessadas e que serão trafegadas na linha de comunicação e a sensibilidade do sistema interno;

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

Os controles e providências que devem ser considerados incluem:

a) a provisão de equipamento e mobília apropriados às atividade de trabalho remoto;

b) uma definição do trabalho permitido, as horas de trabalho, a classificação da informação que pode ser tratada e os sistemas internos e serviços que o funcionário é autorizado a obter acesso;

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

d) segurança física;

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

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

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

h) auditoria e monitoração da segurança;

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

10 Desenvolvimento e manutenção de sistemas

10.1 Requisitos de segurança de sistemas

Objetivos: Garantir que a segurança seja parte integrante dos sistemas de informação.

Isto incluirá infra-estrutura, aplicações do negócio e aplicações desenvolvidas pelo usuário. O projeto e a implementação dos processos do negócio que dão suporte às aplicações e aos serviços podem ser cruciais para segurança. Convém que requisitos de segurança sejam identificados e acordados antes do desenvolvimento dos sistemas de informação.

Convém que todos os requisitos de segurança, incluindo a necessidade de acordos de contingência, sejam identificados na fase de levantamento de requisitos de um projeto e justificados, acordados e documentados como parte do estudo de caso de um negócio para um sistema de informação.

Cópia não autorizada

10.1.1 Análise e especificação dos requisitos de segurança

Na especificação dos requisitos do negócio para novos sistemas, ou melhoria nos sistemas já existentes, convém que também se especifiquem os requisitos de controle. Convém que tais especificações considerem os controles automatizados a serem incorporados no sistema e a necessidade de suporte a controles manuais. Convém que considerações semelhantes sejam aplicadas quando se avaliam pacotes de *software* para as aplicações do negócio. Se considerado apropriado, a direção pode desejar fazer uso de produtos com avaliação e certificação independentes.

Convém que os requisitos e controles de segurança reflitam o valor, para o negócio, dos ativos de informação envolvidos e o dano potencial ao negócio, que pode resultar da falha ou ausência de segurança. A estrutura para analisar os requisitos de segurança e identificar os controles que os satisfazem está na avaliação de riscos e no gerenciamento de riscos.

Os controles introduzidos no desenvolvimento do projeto são significativamente mais baratos para implementar e manter do que aqueles incluídos durante ou após a implementação.

10.2 Segurança nos sistemas de aplicação

Objetivo: Prevenir perda, modificação ou uso impróprio de dados do usuário nos sistemas de aplicações.

Convém que os controles apropriados e trilhas de auditoria ou registros de atividades sejam previstos para os sistemas de aplicação, incluindo aplicações escritas pelo usuário. Convém que estes incluam a validação dos dados de entrada, processamento interno e dados de saída.

Controles adicionais podem ser necessários para sistemas que processam ou têm impacto em ativos organizacionais críticos, valiosos ou sensíveis. Convém que tais controles sejam determinados na base dos requisitos de segurança e na avaliação de riscos.

10.2.1 Validação de dados de entrada

Convém que os dados de entrada dos sistemas de aplicação sejam validados para garantir que estão corretos e que são apropriados. Convém que validações sejam aplicadas na entrada das transações de negócio, nos dados permanentes (nomes e endereços, limites de crédito, números de referência de clientes) e nas tabelas de parâmetros (preços de venda, razão de conversão de moeda, taxas de impostos). Recomenda-se que os seguintes controles sejam considerados:

a) dupla entrada ou outra forma de checagem de entrada para detecção dos seguintes erros:

   1) valores fora dos limites aceitáveis;

   2) caracteres inválidos nos campos de dados;

   3) dados ausentes ou incompletos;

   4) dados excedendo os volumes máximos e mínimos;

   5) controle de dados não autorizados ou inconsistentes;

b) análise crítica periódica do conteúdo dos campos-chave ou arquivos de dados para confirmar a sua validade e integridade;

c) inspeção de cópias de documentos de entrada de dados para qualquer modificação não autorizada aos dados de entrada (qualquer modificação dos documentos de entrada de dados deve ser explicitamente autorizada);

d) procedimentos de resposta à validação de erros;

e) procedimentos de teste de plausibilidade dos dados de entrada;

f) definição de responsabilidades de todo pessoal envolvido no processo de entrada de dados.

10.2.2 Controle do processamento interno

10.2.2.1 Áreas de risco

Dados que foram introduzidos corretamente podem ser corrompidos por erros de processamento ou através de ações intencionais. Convém que checagens de validação sejam incorporadas no sistema para detectar tais corrupções. Convém que o projeto de aplicações garanta que restrições sejam implementadas para minimizar o risco de falhas de processamento que possam levar à perda da integridade. Áreas específicas que devem ser consideradas incluem:

a) uso e localização nos programas de funções de adição e exclusão para implementar modificações nos dados;

b) procedimentos para prevenir a execução de programas na ordem errada ou executar após falhas no processamento anterior (ver também 8.1.1);

c) uso de programas corretos para recuperação de falhas que assegurem o processamento correto dos dados.

Cópia não autorizada

10.2.2.2 Checagens e controles

Os controles necessários dependerão da natureza das aplicações e do impacto nos negócios de qualquer corrupção de dados. Exemplos de checagens que podem ser incorporadas incluem o seguinte:

a) controles de sessão ou processamento em lote, para reconciliar o balanço dos arquivos de dados, após transações de atualização;

b) controles de balanceamento, para checagem dos balanços de abertura contra os balanços de fechamento anteriores, tais como:

1) controles entre execução;

2) totalizadores de atualização de arquivo;

3) controle de programa a programa;

c) validação de dados gerados pelo sistema (ver 10.2.1);

d) checagem da integridade de dados ou de *software* trazidos ou enviados entre computador central e remoto (ver 10.3.3);

e) totais de registros e arquivos;

f) checagem para garantir que os programas de aplicação são executados no horário correto;

g) checagem para garantir que os programas estão executando na ordem correta e terminando em caso de uma falha, e que o processamento subseqüente ficará suspenso até que o problema seja solucionado.

10.2.3 Autenticação de mensagem

A autenticação de mensagem é uma técnica utilizada para detectar modificações não autorizadas no conteúdo das mensagens transmitidas eletronicamente, ou então corrupção deste conteúdo. Ela pode ser implementada em *hardware* ou *software* que suporte um dispositivo físico de autenticação de mensagem ou um algoritmo de *software*.

Convém que a autenticação de mensagem seja considerada para aplicações onde exista requisito de segurança para proteger a integridade do conteúdo da mensagem, por exemplo transferência eletrônica de fundos, especificações, contratos, propostas, etc., com importância significativa ou outras trocas similares de dados eletrônicos. Convém que uma avaliação dos riscos de segurança seja executada para determinar se a autenticação da mensagem é necessária e para identificar o método mais apropriado de implementação.

A autenticação de mensagem não é projetada para proteger o conteúdo da mensagem de divulgação não autorizada. Técnicas de criptografia (ver 10.3.2 e 10.3.3) podem ser utilizadas como meios apropriados de implementação de autenticação de mensagem.

10.2.4 Validação dos dados de saída

Convém que os dados de saída de um sistema de aplicação sejam validados para garantir que o processo de armazenamento da informação está correto e apropriado para as circunstâncias. Tipicamente, os sistemas são construídos com a premissa de que, passados pela apropriada validação, verificação e teste, a saída sempre estará correta. Isto nem sempre é o caso. A validação de saída pode incluir:

a) verificação de plausibilidade para testar se o dado de saída é razoável;

b) contadores de controle de reconciliação, para garantir o processamento de todos os dados;

c) fornecimento de informações suficientes para um leitor ou para um sistema de processamento subseqüente poder determinar a exata, completa e precisa classificação da informação;

d) procedimentos para responder aos testes de validação de saída;

e) definição de responsabilidades para todo o pessoal envolvido com o processo de saída de dados.

10.3 Controles de criptografia

Objetivo: Proteger a confidencialidade, autenticidade ou integridade das informações. Convém que técnicas e sistemas criptográficos sejam usados para a proteção das informações que são consideradas de risco e que para as quais outros controles não fornecem proteção adequada.

10.3.1 Política para o uso de controles de criptografia

Convém que a tomada de decisão sobre o quão adequada é uma solução criptográfica seja vista como parte de um processo mais amplo de avaliação de riscos e seleção de controles. Convém que uma avaliação de riscos seja executada para determinar o nível de proteção que deve ser dado à informação. Esta avaliação pode então ser usada para determinar se um controle criptográfico é apropriado, que tipo de controle deve ser aplicado e para que propósito e processos do negócio.

Cópia não autorizada

Convém que uma organização desenvolva uma política do uso de controles de criptografia para a proteção das suas informações. Tal política é necessária para se maximizar os benefícios e minimizar os riscos da utilização das técnicas criptográficas e para se evitar o uso impróprio ou incorreto. Quando do desenvolvimento de uma política, recomenda-se considerar o seguinte:

a) enfoque da direção frente ao uso dos controles de criptografia através da organização, incluindo os princípios gerais sob os quais as informações do negócio devem ser protegidas;

b) enfoque utilizado para o gerenciamento de chaves, incluindo métodos para tratar a recuperação de informações criptografadas em casos de chaves perdidas, expostas ou danificadas;

c) regras e responsabilidades, por exemplo quem é responsável por:

d) implementação da política;

e) gerenciamento das chaves;

f) como deve ser determinado o nível apropriado de proteção criptográfica;

g) as normas a serem adotadas para a efetiva implementação através da organização (qual solução é utilizada para qual processo do negócio).

10.3.2 Criptografia

A codificação é uma técnica criptográfica que pode ser usada para proteger a confidencialidade da informação. Convém que seja considerada para a proteção de informações críticas ou sensíveis.

Baseado na avaliação de risco, convém que o nível apropriado de proteção seja identificado levando-se em conta o tipo e a qualidade do algoritmo de codificação usado e o tamanho das chaves criptográficas a serem utilizadas.

Quando se implementa a política de criptografia na organização, convém que se tenha atenção com as regulamentações e restrições nacionais que possam ter implicações no uso das técnicas criptográficas em diferentes partes do mundo e com o fluxo de informações codificadas além das fronteiras. Em adição, convém que também se considerem os controles aplicados para a exportação e importação de tecnologias de criptografia (ver também 12.1.6).

Convém que assessoria especializada seja procurada para a identificação do nível de proteção apropriado, para seleção dos produtos mais adequados que fornecerão a proteção necessária e a implementação de um sistema seguro de gerenciamento de chaves (ver também 10.3.5). Adicionalmente, assessoria legal pode ser necessária com respeito às leis e regulamentações aplicáveis à organização que pretende usar criptografia.

10.3.3 Assinatura digital

As assinaturas digitais fornecem os meios para proteção da autenticidade e integridade de documentos eletrônicos. Por exemplo, elas podem ser utilizadas no comércio eletrônico onde existe a necessidade de verificar quem assinou o documento eletrônico e checar se o conteúdo do documento eletrônico assinado foi modificado.

Assinaturas digitais podem ser aplicadas a qualquer forma de documento que é processado eletronicamente, por exemplo elas podem ser usadas para assinar pagamentos eletrônicos, transferências de fundos, contratos e acordos. Assinaturas digitais podem ser implementadas utilizando as técnicas criptográficas baseadas em um único par de chaves relacionadas, em que uma das chaves é utilizada para criar uma assinatura (a chave privada) e a outra para verificar a assinatura (chave pública).

Convém que cuidados sejam tomados para proteger a confidencialidade da chave privada. Convém que esta chave seja mantida em segredo, uma vez que qualquer pessoa que tiver acesso a esta chave pode assinar documentos, por exemplo pagamentos e contratos, falsificando a assinatura do proprietário da chave. Adicionalmente, é importante a proteção da integridade da chave pública. Esta proteção é fornecida pelo uso de certificados de chave pública (ver 10.3.5).

Deve-se considerar o tipo e a qualidade do algoritmo de assinatura digital usado e o tamanho da chave. Convém que as chaves criptográficas usadas para assinaturas digitais sejam diferentes daquelas usadas para criptografia (ver 10.3.2).

Quando se utilizam assinaturas digitais, convém que se considere qualquer legislação relacionada que descreva as condições sob as quais uma assinatura digital possui valor legal. Por exemplo, no caso do comércio eletrônico é importante saber a sustentação legal das assinaturas digitais. Pode ser necessário, onde a estrutura legal for inadequada, ter contratos de obrigações ou outro tipo de acordo para suportar o uso de assinaturas digitais. Convém que se procure um aconselhamento legal considerando as leis e regulamentações que podem ser aplicadas à organização que pretende usar assinaturas digitais.

10.3.4 Serviços de não repúdio

Convém que os serviços de não repúdio sejam usados nos casos em que seja necessário resolver disputas sobre ocorrência ou não ocorrência de um evento ou ação, por exemplo uma disputa envolvendo o uso de uma assinatura digital em um contrato ou pagamento eletrônico. Eles podem ajudar a estabelecer evidências para substanciar se um evento ou ação em particular ocorreu, por exemplo, negação do envio de uma instrução assinada digitalmente usando-se o correio eletrônico. Estes serviços são baseados no uso de criptografia e técnicas de assinatura digital (ver também 10.3.2 e 10.3.3).

Cópia não autorizada

10.3.5 Gerenciamento de chaves

10.3.5.1 Proteção de chaves criptográficas

O gerenciamento das chaves criptográficas é essencial para o uso eficaz das técnicas de criptografia. Qualquer exposição ou perda das chaves criptográficas pode levar ao comprometimento da confidencialidade, da autenticidade e/ou da integridade da informação. Convém que um sistema de gerenciamento de chaves seja implantado para suportar o uso, pela organização dos dois tipos de técnicas criptográficas, que são:

a) técnicas de chave secreta, onde duas ou mais partes compartilham a mesma chave e esta chave é utilizada tanto para codificar como para decodificar a informação. Estas chaves necessitam ser mantidas em segredo, uma vez que qualquer pessoa que tiver acesso à chave será capaz de decodificar toda informação codificada com aquela chave, ou introduzir informações não autorizadas;

b) técnicas de chave pública, onde cada usuário possui um par de chaves, uma chave pública (que pode ser revelada a qualquer pessoa) e uma chave privada (que tem que ser mantida em segredo). As técnicas de chave pública podem ser utilizadas para codificar (ver 10.3.2) e para produzir assinaturas digitais (ver 10.3.3).

Convém que todas as chaves sejam protegidas contra modificação e destruição, e as chaves secretas e privadas necessitam de proteção contra a divulgação não autorizada. As técnicas de criptografia podem ser utilizadas para este propósito. Convém que proteção física seja utilizada para a proteção de equipamentos usados na geração, armazenamento e arquivamento de chaves.

10.3.5.2 Normas, procedimentos e métodos

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

a) geração de chaves para diferentes sistemas criptográficos e diferentes aplicações;

b) geração e obtenção de certificados de chave pública;

c) distribuição de chaves para usuários predeterminados, incluindo como as chaves devem ser ativadas quando recebidas;

d) armazenamento de chaves, incluindo como os usuários autorizados obtêm acesso às chaves;

e) modificação ou atualização de chaves, incluindo regras sobre quando as chaves devem ser modificadas e como isto pode ser feito;

f) tratamento de chaves comprometidas;

g) revogação de chaves, incluindo como as chaves devem ser recolhidas ou desativadas por exemplo, quando as chaves forem comprometidas ou quando um usuário deixar a organização (nestes casos as chaves também devem ser arquivadas);

h) recuperação de chaves que estão perdidas ou corrompidas como parte do gerenciamento da continuidade do negócio, por exemplo para a recuperação de informações codificadas;

i) arquivamento de chaves, por exemplo para informações arquivadas ou de reserva (*back-up*);

j) destruição de chaves;

k) registros (*logs*) e auditoria das atividades relacionadas com o gerenciamento de chaves.

Para poder reduzir a probabilidade de comprometimento, convém que as chaves tenham data de ativação e desativação definidas, de forma que somente possam ser usadas por um período limitado de tempo. Convém que este período de tempo dependa das circunstâncias sob as quais os controles de criptografia estão sendo utilizados e dos riscos observados.

Pode ser necessário considerar certos procedimentos para o tratamento de requisitos legais para acessar chaves criptográficas; por exemplo, as informações codificadas podem ser necessárias na sua forma não codificada como evidências em um julgamento de uma determinada causa legal.

Adicionalmente à questão do gerenciamento seguro das chaves secretas e privadas, convém que a proteção de chaves públicas também seja considerada. Existe a ameaça de alguém falsificar uma assinatura digital através da troca da chave pública do usuário pela sua própria. Este problema é solucionado com o uso de certificados de chave pública. Convém que estes certificados sejam produzidos de forma que se relacionem de um único modo as informações do proprietário do par de chave pública/privada com a chave pública considerada. Além disto é importante que o processo de gerenciamento que gerou este certificado possa ser confiável. Este processo é normalmente implementado por uma autoridade certificadora que convém que seja uma organização reconhecida e com controles e procedimentos implementados para fornecer o grau de confiabilidade necessário.

Convém que o conteúdo do acordo do nível de serviço ou contrato com fornecedores externos de serviços de criptografia, por exemplo com uma autoridade certificadora, cubra questões relacionadas com a responsabilidade cível, a confiabilidade dos serviços e o tempo de resposta para o fornecimento dos serviços contratados (ver 4.2.2).

Cópia não autorizada

10.4 Segurança de arquivos do sistema

Objetivo: Garantir que os projetos de tecnologia da informação e as atividades de suporte serão conduzidas de maneira segura.

Convém que o acesso aos arquivos do sistema seja controlado.

Convém que a manutenção da integridade do sistema seja de responsabilidade da função do usuário ou do grupo de desenvolvimento a quem pertence o sistema de aplicação ou *software*.

10.4.1 Controle de *software* em produção

Convém que seja estabelecido controle para a implementação de *software* em sistemas operacionais. Para se minimizar o risco de corrupção dos sistemas operacionais, recomenda-se que se considerem os seguintes controles.

a) Convém que a atualização das bibliotecas de programa da produção ocorra apenas por um "bibliotecário" nomeado e sob autorização gerencial apropriada (ver 10.4.3).

b) Se possível, convém que o sistema operacional mantenha somente código executável.

c) Convém que código executável não seja implantado no sistema operacional até que sejam obtidas evidências do sucesso dos testes e a aceitação do usuário, e a biblioteca com os programas-fonte correspondentes tenha sido atualizada.

d) Convém que seja mantido um registro (*log*) de auditoria para todas as atualizações de bibliotecas de programas em produção.

e) Convém que as versões anteriores do *software* sejam retidas como medida de contingência.

Convém que *software* de fornecedores usado em sistemas operacionais seja mantido em um nível suportado pelo fornecedor. Convém que qualquer decisão de atualização para uma nova versão leve em conta a segurança da versão, por exemplo a introdução de uma nova funcionalidade de segurança ou o número e a severidade dos problemas de segurança que afetam esta versão. Convém que as correções (*patches*) de *software* sejam aplicadas quando puderem ajudar na remoção ou redução de fragilidade de segurança.

Convém que o acesso físico ou lógico só seja dado a fornecedores por motivo de suporte, quando necessário, e com a aprovação da gerência. Convém que as atividades dos fornecedores sejam monitoradas.

10.4.2 Proteção de dados de teste do sistema

Convém que os dados de teste sejam protegidos e controlados. Testes de sistema e de aceitação normalmente requerem volumes substanciais de dados e devem refletir, o mais próximo possível, os dados em produção. Convém que o uso de base de dados de produção contendo informações pessoais seja evitado. Se tal informação for utilizada, convém que ela seja despersonalizada antes do uso. Recomenda-se que os seguintes controles sejam aplicados para proteção de dados de produção, quando utilizados com o propósito de teste.

a) Convém que os procedimentos de controle de acesso, os quais são aplicados aos sistemas de aplicação em produção, também sejam aplicados aos sistemas de aplicação em teste.

b) Convém que exista uma autorização separada cada vez que uma informação em produção for copiada para teste no sistema de aplicação.

c) Convém que informações de produção sejam apagadas dos sistemas de teste de aplicação imediatamente após a finalização dos testes.

d) Convém que a cópia e o uso de informações de produção sejam registrados de forma a permitir uma trilha de auditoria.

10.4.3 Controle de acesso a bibliotecas de programa-fonte

Para reduzir o potencial de corrupção de programas de computadores, recomenda-se que um controle rígido e completo seja mantido sobre o acesso às bibliotecas de programa-fonte, como o que segue (ver também 8.3).

a) Onde possível, convém que as bibliotecas de programas-fonte não sejam manipuladas em ambiente de produção.

b) Convém que seja designado um responsável pela biblioteca de programas-fonte de cada aplicação.

c) Convém que a equipe de suporte de tecnologia da informação não possua acesso ilimitado às bibliotecas de código-fonte.

d) Convém que os programas em desenvolvimento ou manutenção não sejam mantidos nas bibliotecas de programa-fonte que estiverem em produção.

e) Convém que a atualização das bibliotecas de programa-fonte e a distribuição de programas-fonte para os programadores somente sejam efetuadas pelo responsável designado em manter a biblioteca e sob autorização do gestor de suporte de tecnologia da informação da aplicação.

f) Convém que listas de programa somente sejam mantidas em um ambiente seguro (ver 8.6.4).

g) Convém que seja mantido um registro de auditoria contendo todos os acessos às bibliotecas de programa-fonte.

Cópia não autorizada

h) Convém que as versões antigas de programas-fonte sejam arquivadas, com uma indicação clara e precisa da data e período no qual estiveram em produção, junto com todo o respectivo *software* de suporte, controle de tarefa, definições de dados e procedimentos.

i) Convém que a manutenção e a cópia de bibliotecas de programa-fonte estejam sujeitas a procedimentos rígidos de controle de mudança (ver 10.4.1).

10.5 Segurança nos processos de desenvolvimento e suporte

Objetivo: Manter a segurança do *software* e da informação do sistema de aplicação. Convém que os ambientes de desenvolvimento e suporte sejam rigidamente controlados. Convém que os gestores responsáveis pelos sistemas de aplicação também sejam responsáveis pela segurança do ambiente de desenvolvimento ou suporte. Convém que eles garantam que todas as modificações de sistemas propostas sejam analisadas criticamente, a fim de verificar que elas não comprometem a segurança do sistema ou do ambiente de produção.

10.5.1 Procedimentos de controle de mudanças

Para minimizar a corrupção dos sistemas de informação, convém que exista um controle rígido sobre a implementação de mudanças. Convém que seja exigida a existência de procedimentos formais de controle de mudanças. Convém que eles garantam que os procedimentos de segurança e controle não serão comprometidos, que os programadores de suporte só terão acesso àquelas partes do sistema que serão necessárias ao seu trabalho e acordos formais e que qualquer mudança somente será implementada após aprovação. Mudanças nos sistemas aplicativos podem trazer impacto ao ambiente operacional. Sempre que for possível, convém que os procedimentos de controle de mudança na produção sejam integrados com a de aplicação (ver 8.1.2). Convém que este processo inclua:

a) manter um registro dos níveis de autorização estabelecidos;

b) garantir que as mudanças serão implementadas por usuários autorizados;

c) analisar criticamente controles e a integridade dos procedimentos, de forma a garantir que os mesmos não serão comprometidos pelas mudanças;

d) identificar todo *software* de computadores, informação, entidades de base de dados e *hardware* que necessitam de correção;

e) obter aprovação formal para proposta detalhada antes do início dos trabalhos;

f) garantir que o usuário autorizado aceite as modificações antes de qualquer implementação;

g) garantir que a implementação ocorrerá com o mínimo de transtorno para o negócio;

h) garantir que a documentação do sistema seja atualizada ao final de cada modificação e que a documentação antiga seja arquivada ou destruída;

i) manter o controle da versão para todas as atualizações de *software*;

j) manter uma trilha de auditoria para toda modificação requerida;

k) garantir que a documentação de operação (ver 8.1.1) e os procedimentos de usuário serão modificados conforme necessário, de forma a adequar as mudanças implementadas;

l) garantir que a implementação de mudanças ocorrerá no tempo certo e não atrapalhará os processos do negócio envolvidos.

Muitas organizações mantêm um ambiente no qual os usuários testam novos *softwares* segregados dos ambientes de desenvolvimento e de produção. Esta estratégia favorece o controle sobre novo *software*, permitindo ainda a proteção adicional da informação de produção que é usada para a finalidade de teste.

10.5.2 Análise crítica das mudanças técnicas do sistema operacional da produção

Periodicamente é necessário modificar o sistema operacional, por exemplo para instalar uma correção (*patch*) ou uma nova versão de *software* enviada pelo fornecedor. Quando as modificações ocorrerem, convém que os sistemas de aplicação sejam analisados criticamente e testados para garantir que não ocorrerá nenhum impacto adverso na produção ou na segurança. Recomenda-se que este processo cubra:

a) análise crítica dos procedimentos de controle e integridade da aplicação, para garantir que eles não foram comprometidos pelas mudanças efetuadas no sistema operacional;

b) garantia de que o planejamento e o orçamento anual para suporte cobrirão revisões e testes de sistemas resultantes das modificações do sistema operacional;

c) garantia de que a notificação da modificação do sistema operacional é feita de modo a permitir que as análises críticas apropriadas ocorram antes de qualquer implementação;

d) garantia de que as modificações sejam feitas no plano de continuidade dos negócios (ver seção 11).

10.5.3 Restrições nas mudanças dos pacotes de *software*

Convém que modificações dos pacotes de *software* sejam desencorajadas. Tão longe quanto possível e praticável, convém que os pacotes de *software* adquiridos de fornecedores sejam usados sem modificações. Onde for avaliado como essencial a modificação do pacote de *software*, recomenda-se que os seguintes pontos sejam considerados:

a) risco de comprometimento dos controles embutidos e da integridade dos processos;

b) se é necessária a obtenção do consentimento do fornecedor;

c) possibilidade de obter a modificação necessária diretamente do fornecedor como atualização padrão do programa;

d) impacto de a organização se tornar no futuro responsável pela manutenção do *software* como resultado da modificação.

Se as modificações forem consideradas essenciais, convém que o *software* original seja retido e as modificações efetuadas em uma cópia claramente identificada. Convém que todas as modificações sejam completamente testadas e documentadas, de forma que elas possam ser reaplicadas, se necessário, em futuras atualizações de *software*.

10.5.4 *Covert channels* e cavalo de Tróia

Um c*overt channel* pode expor a informação através de meios indiretos e obscuros. Ele pode ser ativado a partir da troca de parâmetros acessíveis tanto por elementos seguros como por elementos inseguros de um sistema de computação, ou por informações embutidas em um determinado fluxo de dados. Um cavalo de Tróia é projetado para afetar um sistema de uma forma não autorizada ou prontamente informada, e ainda não solicitada pelo receptor ou usuário do programa. Os canais secretos e os cavalos de Tróia acarretam muita preocupação e raramente ocorrem por acidente. Recomenda-se que os seguintes itens sejam considerados:

a) comprar programas apenas de fontes conhecidas e idôneas;

b) comprar programas em código-fonte, de forma que o código possa ser verificado;

c) utilizar produtos que já tenham sido avaliados;

d) inspecionar todo o código-fonte antes do uso em produção;

e) controlar o acesso ao código e a modificação do mesmo, uma vez que esteja instalado;

f) utilizar pessoal de comprovada confiança para trabalhar com os sistemas-chave.

10.5.5 Desenvolvimento terceirizado de *software*

Quando o desenvolvimento de *software* for terceirizado, recomenda-se que os seguintes pontos sejam considerados:

a) acordos sobre licenças, propriedade do código-fonte e direitos de propriedade intelectual (ver 12.1.2);

b) certificação da qualidade e da exatidão do trabalho implementado;

c) acordos na eventualidade de haver falha por parte de prestadores de serviços;

d) direitos de acesso para auditoria da qualidade e exatidão do trabalho executado;

e) requisitos contratuais de qualidade do código;

f) teste antes da instalação para detecção de cavalos de Tróia.

11 Gestão da continuidade do negócio

11.1 Aspectos da gestão da continuidade do negócio

Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos.

Convém que o processo de gestão da continuidade seja implementado para reduzir, para um nível aceitável, a interrupção causada por desastres ou falhas da segurança (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) através da combinação de ações de prevenção e recuperação.

É importante que as conseqüências de desastres, falhas de segurança e perda de serviços sejam analisadas. Recomenda-se que os planos de contingência sejam desenvolvidos e implementados para garantir que os processos do negócio possam ser recuperados dentro da requerida escala de tempo. É importante que tais planos sejam mantidos e testados de forma a se tornarem parte integrante de todos os outros processos gerenciais.

É importante que a gestão da continuidade do negócio inclua controles para a identificação e redução de riscos, a limitação das conseqüências dos danos do incidente e a garantia da recuperação tempestiva das operações vitais.

Cópia não autorizada

11.1.1 Processo de gestão da continuidade do negócio

É importante que um processo de gestão que permeie toda a organização esteja implantado para o desenvolvimento e manutenção da continuidade do negócio. Convém que este processo agregue os seguintes elementos-chave da gestão da continuidade do negócio:

a) entendimento dos riscos a que a organização está exposta, no que diz respeito à sua probabilidade e impacto, incluindo a identificação e priorização dos processos críticos do negócio;

b) entendimento do impacto que as interrupções provavelmente terão sobre os negócios (é importante que as soluções encontradas possam tratar tanto os pequenos incidentes como os mais sérios, que poderiam colocar em risco a continuidade da organização) e estabelecimento dos objetivos do negócio relacionados com as instalações e recursos de processamento da informação;

c) consideração de contratação de seguro compatível que possa ser parte integrante do processo de continuidade;

d) definição e documentação de estratégia de continuidade consistente com os objetivos e prioridades estabelecidos para o negócio;

e) detalhamento e documentação de planos de continuidade alinhados com a estratégia estabelecida;

f) testes e atualizações regulares dos planos e procedimentos implantados;

g) garantia de que a gestão da continuidade do negócio esteja incorporada aos processos e estrutura da organização. A responsabilidade pela coordenação do processo de gestão de continuidade do negócio deve ser atribuída a um nível adequado dentro da organização, por exemplo ao fórum de segurança da informação (ver 4.1.1).

11.1.2 Continuidade do negócio e análise de impacto

Convém que a continuidade do negócio tenha como ponto de partida a identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios. Em seguida, convém que seja feita uma avaliação de risco para a determinação do impacto destas interrupções (tanto em termos de escala de dano quanto em relação ao período de recuperação). Convém que estas atividades sejam executadas com o total envolvimento dos responsáveis pelos processos e recursos do negócio. A avaliação deve considerar todos os processos do negócio e não deve estar limitada aos recursos e instalações de processamento da informação.

Em função dos resultados da avaliação de risco, convém que um plano estratégico seja desenvolvido para se determinar a abordagem mais abrangente a ser adotada para a continuidade do negócio. Uma vez criado, o plano deverá ser validado pela direção.

11.1.3 Documentando e implementando planos de continuidade

Convém que os planos sejam desenvolvidos para a manutenção ou recuperação das operações do negócio, na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos. Recomenda-se que o processo de planejamento da continuidade do negócio considere os seguintes itens:

a) identificação e concordância de todas as responsabilidades e procedimentos de emergência;

b) implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial deve ser dada à avaliação de dependências externas ao negócio e de contratos existentes;

c) documentação dos processos e procedimentos acordados;

d) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;

e) teste e atualização dos planos.

Convém que o processo de planejamento foque os objetivos requeridos do negócio, por exemplo recuperação de determinados serviços específicos para os clientes, em um período de tempo aceitável. Convém que os serviços e recursos que possibilitarão isto ocorrer sejam previstos contemplando pessoal, recursos em geral, além dos de tecnologia de informação, assim como itens de reposição dos recursos e instalações de processamento da informação.

11.1.4 Estrutura do plano de continuidade do negócio

Convém que uma estrutura básica dos planos de continuidade do negócio seja mantida para se assegurar que todos os planos sejam consistentes e para identificar prioridades para testes e manutenção. É importante que cada plano de continuidade do negócio especifique claramente as condições da sua ativação, assim como as responsabilidades individuais para a execução de cada uma das atividades do plano. Quando novos requisitos são identificados, é importante que os procedimentos de emergência relacionados sejam ajustados de forma apropriada, por exemplo os planos de evacuação ou qualquer acordo de recuperação da capacidade de processamento.

Convém que uma estrutura de planejamento para continuidade do negócio considere os seguintes itens:

a) as condições para ativação dos planos, os quais descrevem os processos a serem seguidos previamente à sua ativação (como se avaliar a situação, quem deve ser acionado, etc.);

b) os procedimentos de emergência que descrevam as ações a serem tomadas após a ocorrência de um incidente que coloque em risco as operações do negócio e/ou vidas humanas. Convém que isto inclua procedimentos para a gestão das relações públicas e para o contato eficaz com as autoridades públicas apropriadas, tais como polícia, bombeiros e governo local;

Cópia não autorizada

c) procedimentos de recuperação que descrevam as ações necessárias para a transferência das atividades essenciais do negócio ou os serviços de infra-estrutura para localidades alternativas temporárias e para a reativação dos processos do negócio no prazo necessário;

d) procedimentos de recuperação que descrevam as ações a serem adotadas quando do restabelecimento das operações;

e) uma programação de manutenção que especifique quando e como o plano deverá ser testado e a forma de se proceder à manutenção deste plano;

f) desenvolvimento de atividades educativas e de conscientização com o propósito de criar o entendimento do processo de continuidade do negócio e de assegurar que os processos continuem a serem efetivos;

g) designação das responsabilidades individuais, descrevendo quem é responsável pela execução de que item do plano. Convém que suplentes sejam definidos quando necessário.

É importante que cada plano possua um responsável. Convém que os procedimentos de emergência, planos de retomada manual e os planos de recuperação fiquem sob a guarda do respectivo responsável pelos processos e recursos envolvidos. Convém que atividades de recuperação de serviços técnicos, tais como processamento da informação e instalações de comunicação, sejam usualmente de responsabilidade dos fornecedores destes serviços.

11.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio

11.1.5.1 Teste dos planos

Os planos de continuidade do negócio podem apresentar falhas quando testados, geralmente devido a pressupostos incorretos, omissões ou mudanças de equipamentos e de pessoal. Por isto convém que eles sejam testados regularmente, de forma a garantir sua permanente atualização e efetividade. É importante que tais testes também assegurem que todos os membros da equipe de recuperação e outras pessoas de relevância estão conscientes sobre os planos.

É importante que o planejamento e a programação dos testes do(s) plano(s) de continuidade do negócio indiquem como e quando cada elemento deve ser testado. É recomendável que os componentes isolados do(s) plano(s) sejam freqüentemente testados. Convém que várias técnicas sejam utilizadas, de modo a garantir a confiança de que o(s) plano(s) irá(ão) operar consistentemente em casos reais. Convém que sejam considerados:

a) testes de mesa simulando diferentes cenários (verbalizando os procedimentos de recuperação para diferentes formas de interrupção);

b) simulações (particularmente útil para o treinamento do pessoal nas suas atividades gerenciais pós-crise);

c) testes de recuperação técnica (garantindo que os sistemas de informação possam ser efetivamente recuperados);

d) testes de recuperação em um local alternativo (executando os processos de negócio em paralelo com a recuperação das operações);

e) testes dos recursos, serviços e instalações de fornecedores (garantindo que os serviços e produtos fornecidos atendam aos requisitos contratados);

f) ensaio geral (testando se a organização, o pessoal, os equipamentos, os recursos e os processos podem enfrentar interrupções).

Estas técnicas podem ser utilizadas por qualquer organização e convém que elas reflitam a natureza do plano de recuperação específico.

11.1.5.2 Manutenção e reavaliação dos planos

É importante que os planos de continuidade do negócio sejam mantidos por meio de análises críticas regulares e atualizações, de forma a assegurar a sua contínua efetividade (ver 11.1.5.1). Convém que procedimentos sejam incluídos no programa de gerenciamento de mudanças da organização, de forma a garantir que as questões relativas à continuidade de negócios estão devidamente tratadas.

Convém que a responsabilidade pelas análises críticas periódicas de cada parte do plano seja definida e estabelecida; convém que a identificação de mudanças nas atividades do negócio que ainda não tenham sido contempladas nos planos de continuidade de negócio seja seguida da apropriada atualização. Convém que um controle formal de mudanças assegure que os planos atualizados são distribuídos e reforçados por análises críticas periódicas do plano como um todo.

Exemplos de situações que podem demandar atualizações nos planos incluem a aquisição de novo equipamento, ou atualização dos sistemas operacionais e alterações:

a) de pessoal;

b) de endereços ou números telefônicos;

c) de estratégia de negócio;

d) na localização, instalações e recursos;

Cópia não autorizada

e) na legislação;

f) em prestadores de serviço, fornecedores e clientes-chave;

g) de processos (inclusões e exclusões);

h) no risco (operacional e financeiro).

12 Conformidade

12.1 Conformidade com requisitos legais

Objetivo: Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.

O projeto, a operação, o uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentares ou estatutários.

Convém que consultoria em requisitos legais específicos seja procurada em organizações de consultoria jurídica ou em profissionais liberais, adequadamente qualificados nos aspectos legais. Os requisitos legislativos variam de país para país e também para a informação criada em um país e transmitida para outro (isto é, fluxo de dados internacional).

12.1.1 Identificação da legislação vigente

Convém que estatutos, regulamentações ou cláusulas contratuais relevantes sejam explicitamente definidos e documentados para cada sistema de informação. Convém que os controles e as responsabilidades específicos para atender a estes requisitos sejam, de forma similar, definidos e documentados.

12.1.2 Direitos de propriedade intelectual

12.1.2.1 Direitos autorais

Convém que procedimentos apropriados sejam implementados para garantir a conformidade com as restrições legais no uso de material de acordo com leis de propriedade intelectual, como as de direitos autorais, patentes ou marcas registradas. A violação do direito autoral pode levar a uma ação legal envolvendo processos criminais.

Legislação, regulamentação e cláusulas contratuais podem estabelecer restrições para cópia de material que tenha direitos autorais. Em particular, pode ser requerido que somente material que seja desenvolvido pela organização ou que foi licenciado ou fornecido pelos desenvolvedores para a organização seja utilizado.

12.1.2.2 Direitos autorais de *software*

Produtos de *software* proprietários são normalmente fornecidos sob um contrato de licenciamento que restringe o uso dos produtos em máquinas especificadas e que pode limitar a cópia apenas para criação de uma cópia de segurança. Convém que os seguintes controles sejam considerados:

a) divulgar uma política de conformidade de direito autoral de *software* que defina o uso legal de produtos de *software* e de informação;

b) emitir padrões para procedimentos de aquisição de produtos de *software*;

c) manter atenção sobre a política de aquisição e de direitos autorais de *software* e notificar a intenção de tomar ações disciplinares contra colaboradores que violarem essas políticas;

d) manter adequadamente os registros de ativos;

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 não excede o número de licenças adquiridas;

g) conduzir verificações para que somente produtos de *software* autorizados e licenciados sejam instalados;

h) estabelecer política para a manutenção das condições adequadas de licenças;

i) estabelecer uma política para disposição ou transferência de *software* para outros;

j) utilizar ferramentas de auditoria apropriadas;

k) cumprir termos e condições para *software* e informação obtidos a partir de redes públicas (ver também 8.7.6).

Cópia não autorizada

12.1.3 Salvaguarda de registros organizacionais

Convém que registros importantes de uma organização sejam protegidos contra perda, destruição e falsificação. Alguns registros podem precisar ser retidos de forma segura para atender a requisitos estatutários ou regulamentações, assim como para apoiar as atividades essenciais do negócio. Exemplo disso são os registros que podem ser exigidos como evidência de que uma organização opera de acordo com as regras estatutárias e regulamentares, ou que podem assegurar a defesa adequada contra potenciais processos civis ou criminais ou confirmar a situação financeira de uma organização perante aos acionistas, parceiros e auditores. O período de tempo e o conteúdo da informação retida podem estar definidos através de leis ou regulamentações nacionais.

Convém que 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 10.3.2 e 10.3.3) sejam mantidas de forma segura e tornadas disponíveis para as pessoas autorizadas quando necessário.

Convém que cuidados sejam tomados a respeito da possibilidade de degradação das mídias usadas no armazenamento dos registros. Convém que os procedimentos de armazenamento e tratamento 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.

Convém que sistemas de armazenamento de dados sejam escolhidos de modo que o dado solicitado possa ser recuperado de forma aceitável pelo tribunal de justiça, como, por exemplo, todos os registros solicitados possam ser recuperados nos prazos e nos formatos aceitáveis.

Convém que o sistema de armazenamento e tratamento assegure a clara identificação dos registros e dos seus períodos de retenção estatutários e regulamentares. Convém que seja permitida a destruição apropriada dos registros após esse período, caso não sejam mais necessários à organização.

Para atender a estas obrigações, convém que os seguintes passos sejam tomados dentro da organização.

a) Emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações.

b) Elaborar uma programação para retenção, identificando os tipos de registro essenciais e o período que cada um deve ser mantido.

c) Manter um inventário das fontes de informações-chave.

d) Implementar controles apropriados para proteger registros e informações essenciais de perda, destruição e falsificação.

12.1.4 Proteção de dados e privacidade da informação pessoal

Alguns países têm promulgado leis que estabelecem controles no processamento e na transmissão de dados pessoais (geralmente informação sobre indivíduos vivos que podem ser identificados a partir de tais informações). Tais controles podem impor responsabilidades sobre aqueles que coletam, processam e disseminam informação pessoal, e podem restringir a capacidade de transferência desses dados para outros países.

Conformidade com leis de proteção de dados necessita de uma estrutura de gestão e de controles apropriados. Geralmente isto é melhor alcançado através da indicação de um responsável pela proteção de dados que deve fornecer orientações gerais para gestores, usuários e provedores de serviço sobre as responsabilidades de cada um e sobre quais procedimentos específicos recomenda-se seguir. Convém que seja responsabilidade do proprietário do dado notificar ao responsável pela proteção de dados sobre qualquer proposta de armazenamento de informações pessoais em um arquivo estruturado e garantir a capacitação nos princípios de proteção de dados definidos na legislação vigente.

12.1.5 Prevenção contra uso indevido de recursos de processamento da informação

Os recursos de processamento da informação de uma organização são fornecidos para propósitos do negócio. A direção deve autorizar o seu uso. Convém que qualquer uso destes recursos para propósitos não profissionais ou não autorizados, sem a aprovação da direção, seja considerado como uso impróprio. Se essa atividade for identificada por processo de monitoração ou outros meios, convém que seja levada ao conhecimento do gestor respon-sável para que sejam aplicadas as ações disciplinares cabíveis.

A legalidade do processo de monitoração do uso varia de país para país e pode requerer que os funcionários sejam avisados dessa monitoração ou estejam formalmente em concordância com este processo. Convém que se busque uma assessoria legal antes da implementação dos procedimentos de monitoração.

Cópia não autorizada

Muitos países possuem, ou têm em processo de promulgação, leis de proteção contra o uso impróprio de computadores. Pode ser crime o uso de um computador para fins não autorizados. Desta forma, é essencial que os usuários estejam conscientes do escopo exato de suas permissões de acesso. Isto pode, por exemplo, ser alcançado pelo registro das autorizações dos usuários por escrito, recomendando-se que a cópia seja assinada pelo usuário e armazenada de forma segura pela organização. Convém que os funcionários de uma organização e prestadores de serviço sejam informados de que nenhum acesso é permitido, com exceção daqueles que foram autorizados.

No momento da conexão inicial convém que seja apresentada uma mensagem de advertência na tela do computador, indicando que o sistema que está sendo acessado é privado e que não são permitidos acessos não autorizados. O usuário tem que confirmar e reagir adequadamente à mensagem na tela para continuar com o processo de conexão.

12.1.6 Regulamentação de controles de criptografia

Alguns países têm estabelecido acordos, leis, regulamentações ou outros instrumentos para controlar o acesso ou uso de controles de criptografia. Tais controles podem incluir:

a) importação e/ou exportação de *hardware* e *software* de computador para execução de funções criptográficas;

b) importação e/ou exportação de *hardware* e *software* de computador que foi projetado para ter funções criptográficas embutidas;

c) métodos mandatórios ou discricionários de acesso dos países à informação cifrada por *hardware* ou *software* para fornecer confidencialidade ao conteúdo.

Convém que assessoria jurídica seja obtida para garantir a conformidade com a legislação nacional vigente. Também convém que seja obtida assessoria jurídica antes de se transferirem informações cifradas ou controles de criptografia para outros países.

12.1.7 Coleta de evidências

12.1.7.1 Regras para evidências

É necessário ter evidências adequadas para apoiar um processo jurídico contra uma pessoa ou organização. Sempre que este processo for uma questão disciplinar interna, as evidências necessárias estarão descritas nos procedimentos internos.

Quando o processo envolver a lei, civil ou criminal, convém que as evidências apresentadas estejam de acordo com as regras para evidências estabelecidas pela lei ou pelo tribunal de justiça específico onde o caso será julgado. Em geral, estas regras abrangem:

a) admissibilidade da evidência: se a evidência pode ser ou não utilizada pela corte;

b) importância da evidência: qualidade e inteireza da evidência;

c) evidência adequada de que controles estavam operando correta e consistentemente (isto é, processo de controle de evidências) durante todo o período que a evidência recuperada foi armazenada e processada pelo sistema.

12.1.7.2 Admissibilidade da evidência

Para obter admissibilidade da evidência, recomenda-se que as organizações garantam que seus sistemas de informação estão em conformidade com qualquer norma ou código de prática publicado para produção de evidência admissível.

12.1.7.3 Qualidade e inteireza da evidência

Para obter qualidade e inteireza da evidência, uma boa trilha de evidência é necessária. Em geral, tal trilha pode ser estabelecida sob as seguintes condições.

a) Para documentos em papel: o original é mantido de forma segura e são mantidos registros sobre quem encontrou, onde foi encontrado, quando foi encontrado e quem testemunhou a descoberta. Convém que qualquer investigação garanta que os originais não foram adulterados.

b) Para informações em mídia eletrônica: convém que cópias de qualquer mídia removível, informações em disco rígido ou em memória sejam obtidas para garantir a disponibilidade. Convém que o registro de todas as ações durante o processo de cópia seja mantido e o processo seja testemunhado. Convém que uma cópia da mídia magnética e um dos registros sejam mantidos de forma segura.

Quando um incidente é detectado, pode não ser óbvio que resultará num possível processo jurídico. Entretanto, existe o perigo de que a evidência necessária seja destruída acidentalmente antes que seja percebida a seriedade do incidente. É conveniente envolver um advogado ou a polícia tão logo seja constatada a possibilidade de processos jurídicos e obter consultoria sobre as evidências necessárias.

12.2 Análise crítica da política de segurança e da conformidade técnica

Objetivo: Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança.
Convém que a segurança dos sistemas de informação seja analisada criticamente a intervalos regulares.
Convém que tais análises críticas sejam executadas com base nas políticas de segurança apropriadas e que as plataformas técnicas e sistemas de informação sejam auditados na conformidade com as normas de segurança implementadas.

Cópia não autorizada

12.2.1 Conformidade com a política de segurança

Convém que gestores garantam que todos os procedimentos de segurança dentro da sua área de responsabilidade estão sendo executados corretamente. Adicionalmente, convém que todas as áreas dentro da organização sejam consideradas na análise crítica periódica, para garantir a conformidade com as normas e políticas de segurança. Convém que isto inclua o seguinte:

a) sistemas de informação;

b) provedores de sistemas;

c) proprietários da informação e ativos de informação;

d) usuários;

e) direção.

Convém que os proprietários dos sistemas de informação (ver 5.1) apóiem as análises críticas periódicas de conformidade dos seus sistemas com as políticas de segurança, normas e qualquer outro requisito de segurança apropriado. A monitoração operacional do uso do sistema é coberta em 9.7.

12.2.2 Verificação da conformidade técnica

Convém que sistemas de informação sejam periodicamente verificados em sua conformidade com as normas de segurança implementadas. Verificação de conformidade técnica envolve a análise dos sistemas operacionais para garantir que controles de *hardware* e *software* foram corretamente implementados. Este tipo de verificação de conformidade requer a assistência de técnicos especializados. Convém que seja executado manualmente (auxiliado por funções de *software* apropriadas, se necessário) por um engenheiro de sistemas experiente ou por funções de *software* que gerem relatório técnico para interpretação subseqüente por um técnico especialista.

Verificação de conformidade também engloba, por exemplo, testes de invasão, que podem ser executados por especialistas independentes contratados especificamente para este fim. Isto pode ser útil na detecção de vulnerabilidades do sistema e na verificação do quanto os controles são eficientes na prevenção de acessos não autorizados devido a estas vulnerabilidades. Convém que cuidados sejam tomados em testes de invasão cujo sucesso pode levar ao comprometimento da segurança do sistema e inadvertidamente explorar outras vulnerabilidades.

Convém que qualquer verificação de conformidade técnica somente seja executada por, ou sob supervisão de, pessoas competentes e autorizadas.

12.3 Considerações quanto à auditoria de sistemas

Objetivo: Maximizar a eficácia e minimizar a interferência no processo de auditoria de sistema.

Convém que existam controles para a salvaguarda dos sistemas operacionais e ferramentas de auditoria durante as auditorias de sistema.

Proteção também é necessária para salvaguardar a integridade e prevenir o uso indevido das ferramentas de auditoria.

12.3.1 Controles de auditoria de sistema

Convém que requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados, para minimizar os riscos de interrupção dos processos do negócio. Recomenda-se que seja observado o seguinte.

a) Convém que os requisitos de auditoria sejam acordados com o nível apropriado da direção.

b) Convém que o escopo da verificação seja acordado e controlado.

c) Convém que a verificação esteja limitada ao acesso somente para leitura de *software* e dados.

d) Convém que outros acessos diferentes de apenas leitura sejam permitidos somente através de cópias isoladas dos arquivos do sistema, que devem ser apagados ao final da auditoria.

e) Convém que recursos de tecnologia para execução da verificação sejam identificados explicitamente e tornados disponíveis.

f) Convém que requisitos para processamento adicional ou especial sejam identificados e acordados.

g) Convém que todo acesso seja monitorado e registrado de forma a produzir uma trilha de referência.

h) Convém que todos os procedimentos, requerimentos e responsabilidades sejam documentados.

12.3.2 Proteção das ferramentas de auditoria de sistemas

Convém que acessos às ferramentas de auditoria de sistemas, isto é, *software* ou arquivos de dados, sejam protegidos para prevenir contra qualquer possibilidade de uso impróprio ou comprometimento. Convém que tais ferramentas sejam separadas de sistemas em desenvolvimento e em operação e não sejam mantidas em fitas de biblioteca ou áreas de usuários, a menos que forneçam um nível apropriado de proteção adicional.

/ANEXO A

Cópia não autorizada

Anexo A (informativo)
Descrição dos termos apresentados em inglês nesta Norma

BBS (Bulletin Board System) - sistema no qual um computador pode se comunicar com outros computadores através de linha telefônica, como na Internet

Call forwarding (Retorno de chamada) - procedimento para identificar um terminal remoto

Covert channel - canal de comunicações que permite que dois processos cooperativos transfiram a informação de uma maneira que viole a política de segurança do sistema

Denial of service (negação do serviço) - impedimento do acesso autorizado aos recursos ou retardamento de operações críticas por um certo período de tempo

Dial up - serviço por meio do qual um terminal de computador pode usar o telefone para iniciar e efetuar uma comunicação com outro computador

Firewall - sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes

Gateway - máquina que funciona como ponto de conexão entre duas redes

Hacker - pessoa que tenta obter acesso a sistemas sem autorização, usando técnicas próprias ou não, com o intuito de acesso a determinado ambiente para proveito próprio ou de terceiros. Dependendo dos objetivos da ação, podem ser chamados de *Cracker*, *Lammer* ou *BlackHat*

Housekeeping - processo que visa a manutenção da ordem, limpeza, organização e segurança nas empresas

ID – identificador de usuário para obtenção de acesso aos recursos do sistema

I&A (Integrity and Availability) – integridade e disponibilidade

Log – registro de eventos de um sistema. Trilhas de auditoria

Log-on – processo de entrada de um usuário no sistema

Log-off – processo de encerramento de uma sessão de usuário no sistema

Smartcard - cartão plástico que contém um *microchip* que inclui um microprocessador e uma memória. Do mesmo tamanho que um cartão de crédito, tem contatos que permitem que outros dispositivos se comuniquem com o cartão. Pode conter mais dados do que uma tarja magnética e pode ser programado para revelar somente a informação relevante

Trojan horse - programa de computador com função aparentemente ou realmente útil, que contém as funções (escondidas) adicionais e que explora secretamente as autorizações legítimas do processo, provocando perda da segurança

Tokens - mensagem que consiste em dados relevantes para uma comunicação específica e que contém informações que podem ser transformadas, usando uma técnica de criptografia

Cópia não autorizada

Índice alfabético

Cópia não autorizada

Cópia não autorizada

Cópia não autorizada