Entendendo e implementando a Norma ABNT NBR ISO/IEC 17799:2005

Academia Latino-Americana de Segurança da Informação

Aspectos teóricos e práticos para implantação da Norma ABNT NBR ISO/IEC 17799:2005

Módulo 3

Entendendo e implementando a Norma ABNT NBR ISO/IEC 17799:2005

AUTOR

Arthur Roberto dos Santos Júnior

Apostila desenvolvida pelo Instituto Online em parceria com a Microsoft Informática

http://www.instonline.com.br/

Revisão 0.9 – Maio de 2006

COORDENADORES TÉCNICOS

Fernando Sérgio Santos Fonseca
Arthur Roberto dos Santos Júnior

.
.

COMO USAR ESSE MATERIAL

Este é um material de apoio para o curso “Entendendo e implementando a ABNT NBR ISO/IEC 17799:2005” ministrado pela Academia de Segurança Microsoft. Durante o curso serão apresentados vários Webcasts com o conteúdo deste material acompanhado de slides e voz para ilustrar os conceitos e práticas. A cópia desses slides está em destaque na apostila, seguida de textos com informações que serão abordadas pelo instrutor nos respectivos Webcasts.

LABORATÓRIO : TÍTULO AQUI

Os laboratórios de cada módulo do curso são identificados dessa forma e roteiro está especificado sob o título.

ÍNDICE

Capítulo
10

10 – GERÊNCIA DE OPERAÇÕES E COMUNICAÇÕES

POR ARTHUR SANTOS JR.

ESTE CAPÍTULO DA NORMA APRESENTA MEIOS DE PADRONIZAR AS FORMAS DE ARMAZENAMENTO, TROCA E DESTRUIÇÕES DE INFORMAÇÕES, GARANTINDO A OPERAÇÃO SEGURA DO PROCESSAMENTO DA INFORMAÇÃO.

OBJETIVOS

O gerenciamento das operações e comunicações visa padronizar formas de criação, armazenamento, transporte, acesso, recuperação e descarte da informação, de maneira a garantir o processamento seguro da mesma.

Como devem ser tratados os recursos de desenvolvimento, a fim de não comprometer o ambiente de produção, é um dos objetivos desta parte da norma.

Outro item importante tratado é o planejamento e aceitação dos sistemas, a fim de minimizar os riscos de falhas.

Todas essas formas de tratamento da informação devem ter procedimentos devidamente documentados, servindo como fonte de consulta para facilitar a execução de atividades corriqueiras ou emergenciais.

Ao final deste capítulo você estará apto a:

- ❒ Estabelecer os procedimentos operacionais que tornam seguro o processamento de recursos da informação;
- ❒ Saber a importância da separação de funções e áreas de responsabilidade, bem como de ambientes de desenvolvimento e produção;
- ❒ Gerenciar serviços de terceiros;
- ❒ Minimizar riscos de falhas em sistemas, através do planejamento de aceitação dos mesmos;
- ❒ Proteger softwares contra códigos maliciosos e móveis;
- ❒ Implementar estratégias de cópias de segurança;
- ❒ Proteger as informações em redes e a infra-estrutura de suporte;
- ❒ Proteger e controlar mídias de armazenamento de informações e documentação;
- ❒ Gerir a troca de informações e softwares entre organizações.

10.1 - PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS

- Preveja:
  - Todas as situações Óbvias

  - E algumas improváveis

Estabeleça e documente procedimentos e responsabilidades pela gestão operacional dos recursos de processamento da informação

Gerenciar recursos de processamento de informações é um conjunto de tarefas que demanda critério de manuseio e responsabilidades bem definidas.

Como não se pode prever tudo, devemos ao menos prever o óbvio de todas as situações e o improvável em alguns casos. Dessa forma, os riscos poderão ser minimizados a níveis até melhores do que o tolerável.

Nos subitens seguintes serão apresentadas as diretrizes a serem adotadas a fim de estabelecer e documentar procedimentos e responsabilidades pela gestão operacional dos recursos de processamento da informação, bem como a importância da separação de funções e áreas de responsabilidade. Esses temas visam assegurar o sucesso das operações dos recursos de processamento da informação, reduzindo os riscos do mau uso ou uso doloso dos sistemas.

10.1.1 – DOCUMENTAÇÃO DOS PROCEDIMENTOS DE OPERAÇÃO

- Detalhamento de procedimentos de operação, como:
  - Inicialização e desligamento de computadores
  - Geração de cópias (backup)
  - Manutenção de equipamentos
  - Tratamento de mídias e correspondências
  - Segurança de salas de computadores
  - Instruções de tratamento de erros
  - Instruções de tratamento de eventos excepcionais
  - Reinício e recuperação em caso de falhas do sistema
  - Gestão de trilhas de auditoria e informações de registros de sistema

Nada mais reconfortante para um ambiente organizacional, do que ter em mãos documentos com procedimentos operacionais detalhados de ações a serem tomadas nas mais diversas situações (como inicializar e desligar computadores, gerar cópias de segurança, manutenção de equipamentos, tratamento de mídias, segurança e gestão do tratamento das correspondências e dos ambientes de computadores). Isso demanda um trabalho rigoroso de anotação de rotinas para posterior documentação das mesmas. Também devem ser previstas situações não rotineiras, bem como emergenciais.

Relatar todas as situações possíveis pode parecer um procedimento enfadonho, e realmente o é. Porém, sua execução pode ser muito facilitada caso possa contar com o auxílio de todos os que estão diretamente ligados a cada atividade. Basta solicitar que cada um descreva suas atividades diárias ligadas ao trato com os recursos de processamento da informação. Peça também para descreverem as atividades que porventura tenham fugido da rotina, e aquelas as quais nunca ocorreram, mas que acreditam que um dia poderá ser um fato, ainda que uma única vez. Com esses dados em mãos, comece a documentar as atividades, tendo em mente que a pessoa que lerá esse documento, o fará pela primeira vez.

Comece com as atividades rotineiras e crie os procedimentos detalhados de cada tarefa, já incorporando na documentação alguma modificação ao modo como são feitas, caso ache necessário. Em seguida trate as situações menos óbvias.

Caso tenha que relatar um novo procedimento, peça ao proprietário deste que escreva as atividades de operação. Verifique se estão de acordo com requerimentos de segurança e documente-as, especificando detalhadas instruções para execução.

Ao final do levantamento, o documento certamente terá a maioria das tarefas diárias da organização, referentes ao processamento da informação. A norma ABNT NBR ISO/IEC 17799:2005, lista procedimentos de operação cujas instruções devem ser detalhadas, como:

a) processamento e manuseio de informações;

b) cópias de segurança (backup);

c) requisitos de agendamento, incluindo interdependências com outros sistemas, horários de início e término das tarefas;

d) instruções para tratamento de erros ou outras condições excepcionais, que possam ocorrer durante a execução de uma tarefa, incluindo restrições no uso de utilitários do sistema;

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

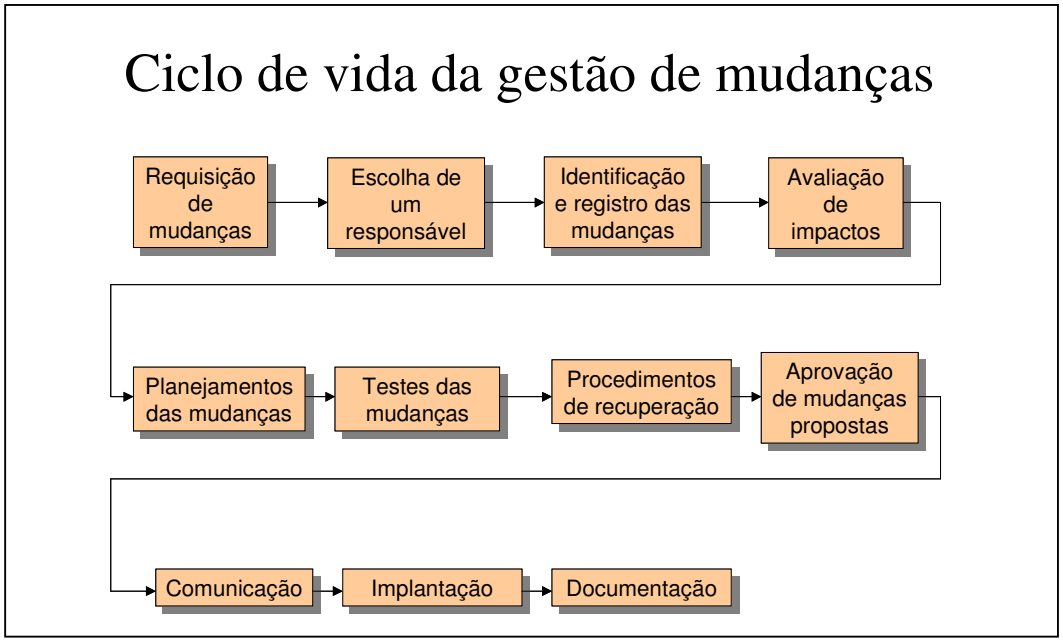
f) procedimentos para reinício e recuperação em caso de falha no sistema;

g) gerenciamento de trilhas de auditoria e informações de registros (logs) de sistemas.

Os itens acima abordam de maneira genérica as tarefas a serem documentadas, mas não as esgotam, haja vista que cada organização possui suas particularidades a serem especificadas.

A norma ainda recomenda que “os procedimentos operacionais e documentados para atividades de sistema devem ser tratados como documentos formais e as mudanças devem ser autorizadas pela direção”.

10.1.2 – GESTÃO DE MUDANÇAS



Modificações nos recursos de processamento de informação e sistemas podem ser definidas como qualquer alteração ou nova instalação de sistemas, hardware, aplicativos de software, procedimentos e infra-estrutura, que possam causar impactos nas operações.

Em todo processo de modificação sempre ocorre com algum tipo de impacto, seja positivo ou negativo. O objetivo da gestão de mudanças é minimizar os impactos negativos (como quebra de integridade do sistema ou falhas de segurança) provocados pela implantação das modificações, ou seja, gestão de mudanças é o processo de identificar novos requerimentos de segurança quando ocorrem mudanças no sistema [1].

Gerir mudanças é uma tarefa que requer planejamento, controle, comunicação e monitoramento da implantação. O planejamento irá avaliar e identificar os possíveis riscos e impactos que a mudança poderá trazer ao ambiente, e criará procedimentos para assegurar que a mudança será um sucesso. Ao mesmo tempo, como nem tudo sempre sai como planejado, devem ser criados procedimentos para a recuperação em caso de insucesso da operação ou na ocorrência de eventos inesperados.

Em todos os estágios da implementação de mudanças o gerenciamento deve monitorar e modificar os processos, caso seja necessário, como um contínuo processo de aprendizado.

A gestão de mudanças deverá documentar todos os processos de implementação, antes de serem aplicados no ambiente produtivo. Essa documentação deverá ser revisada e atualizada durante e depois do processo de mudança, a fim de mantê-la em conformidade com a realidade da implantação.

O ciclo de vida de um processo de gestão de mudanças passa pelos seguintes itens:

a. *Requisição de mudança*: Alguém irá requerer uma mudança em função de alguma necessidade do processo da informação. Deve-se documentar essa fase através da descrição da intenção da mudança e os benefícios esperados.

b. *Escolha do responsável pela mudança*: esta pessoa será responsável por coordenar o projeto e assegurar que o processo alcance seu objetivo.

c. *Identificação e registro das mudanças significativas*: Antes da implementação de qualquer mudança, é recomendável a identificação das mesmas através de registros apropriados que a denominarão. Por exemplo, se a mudança for em um aplicativo de software, deve-se identificar a mudança através de nova numeração de versão (release).

d. *Avaliação de riscos impactos potenciais das mudanças*: Toda mudança é acompanhada de um risco. É importante que esse risco seja avaliado para que se possam tomar contramedidas necessárias para sua atenuação. A avaliação do risco irá determinar inclusive a relação custo/benefício do processo de mudança, proporcionando parâmetros para decisões de prosseguimento da implantação. Níveis diferenciados de riscos devem ser atribuídos para cada requisição de mudanças:

    1. Risco alto: é o risco que provocará maior impacto em caso de falha, com pouca ou nenhuma possibilidade de recuperação. Poderá, por exemplo, provocar corrupção de dados com sérias conseqüências para o processamento da informação.

    2. Risco moderado: é o risco com conseqüências que permitem recuperação, ainda que demorada. Pode envolver vários sistemas, o que a torna preocupante quanto a seus impactos.

    3. Risco baixo: são modificações que provocarão pequeno impacto em caso de falhas. A recuperação é fácil ou até mesmo desnecessária.

e. *Planejamento da mudança*: Quanto maior o risco, maior é a necessidade de planejamento. Esta fase irá descrever como será o processo de implantação da mudança, alocando recursos humanos e financeiros, além de recursos de hardware e software. Também documentará as mudanças.

f. *Testes das mudanças*: As mudanças devem ser primeiramente implantadas em ambiente de laboratório, a fim de evitar riscos desnecessários em ambientes de produção. Testes exaustivos devem ser realizados até que se tenha certeza que as modificações terão o efeito desejado.

g. *Criação de procedimentos de recuperação*: Por melhor que se planeje todo o processo, ainda poderá ocorrer falhas ou eventos imprevistos. Por isso, crie procedimentos que possibilitarão a recuperação do sistema no menor prazo possível. Estabeleça quem será o responsável pela interrupção e recuperação de mudanças.

h. *Procedimento formal de aprovação das mudanças propostas:* Uma vez que todos os possíveis riscos foram levados em conta e após os testes das mudanças, agora é hora de submeter os resultados ao procedimento formal de aprovação na organização. A documentação deverá ser submetida ao nível hierárquico superior, que autorizará a fase de implantação em ambiente de produção.

i. *Comunicação*: Com o processo de mudança aprovado, divulgue-o às equipes afetadas. Comunique como será o processo, quais os impactos, quanto tempo de parada será necessário para a implantação e, caso a mudança envolva operações de usuários, estes devem ser previamente notificados e instruídos sobre a operação e sobre os novos procedimentos de manuseio após a implantação.

j. *Implementação das mudanças*: Com todo o processo planejado, testado, documentado e aprovado, passe agora para a implementação. Esse processo deverá seguir rigorosamente o planejado. Em ambiente de produção, situações imprevistas poderão ocorrer, e os planos de recuperação deverão entrar em ação. Alguns imprevistos provocarão pequenos ajustes no processo, o que deve ser documentado para manter atualizadas as especificações.

k. *Documentação*: o processo inteiro de mudanças deverá ser documentado, seguindo um padrão de numeração do documento que deverá ser criado. Essa documentação deverá ser atualizada durante os passos da implantação, a fim de refletir a realidade do processo.

Através desse roteiro, é possível implantar mudanças com alto nível de sucesso na operação, minimizando impactos negativos e otimizando os recursos empregados.

10.1.3 – SEGREGAÇÃO DE FUNÇÕES

- Separar funções potencialmente conflitantes,como:
  - autorização
  - aprovação
  - execução
  - controle
  - contabilização das operações.

Uma das lições aplicadas a sistemas contábeis, segundo Silvio Aparecido Crepaldi [2], é o princípio fundamental de que:

"Ninguém deveria controlar todas as etapas de uma transação sem a intervenção de outra, ou outras capazes de efetuar uma verificação cruzada... O controle total de todas as etapas de uma transação por um só indivíduo permitiria a este atuar ineficaz ou fraudulentamente, sem ser descoberto".

Segregar funções é criar um sistema de controle que consiste na separação de funções potencialmente conflitantes, como autorização, aprovação, execução, controle e contabilização das operações.

Em ambiente de TI o princípio acima se aplica com o objetivo de reduzir os riscos de uso acidental ou deliberado dos sistemas.

Caso haja possibilidade de conluios, faz-se necessário o planejamento de controles que envolvam duas ou mais pessoas, diminuído os riscos de fraudes.

Um exemplo da necessidade de segregação de funções pode ser visto em funções como: programação, criação de bancos de dados e inclusão de informações. Um administrador de banco de dados criará a base dados, que o programador usará para o desenvolvimento das rotinas de acesso, enquanto o usuário incluirá os dados na base. É interessante prevenir que tanto o programador, quanto o administrador do banco, possam alterar os dados incluídos pelo usuário.

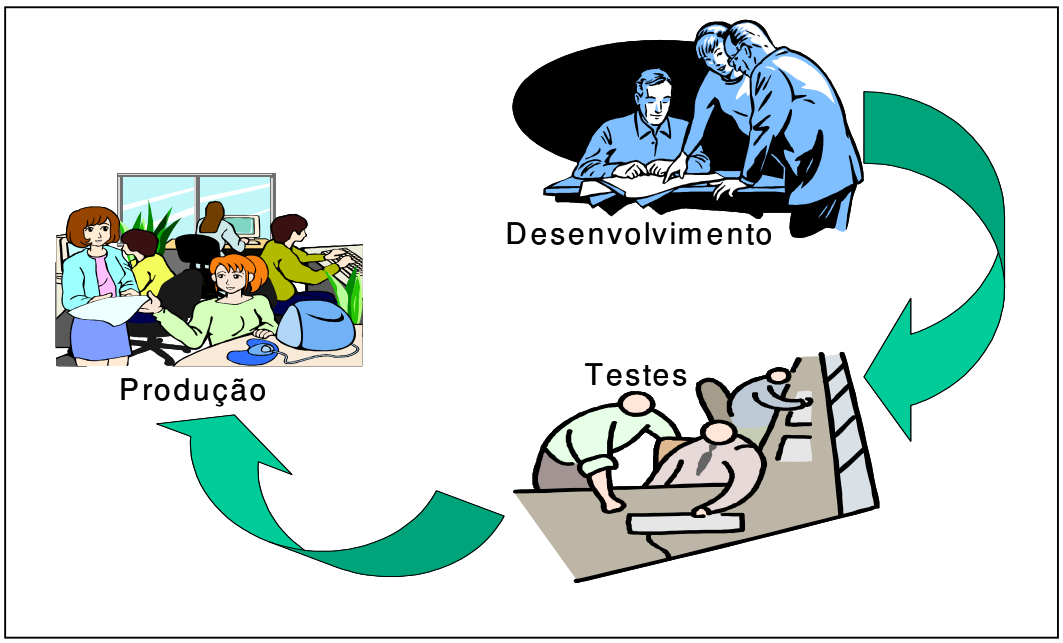
O controle das operações deve ser exercido através de métodos de aprovações, de acordo com as responsabilidades e os riscos envolvidos. Na medida do possível, a pessoa que autoriza não deve ser a que aprova para não expor a risco os interesses da organização.

As funções devem ser bem definidas, escritas e assinadas pelos responsáveis, que assim, assumem o compromisso de não apenas cumpri-las, como também não exercer a função de responsabilidade de outros.

Em empresas menores, geralmente várias funções são acumuladas por um mesmo indivíduo, como por exemplo, a de programador e administrador de banco de dados. Nesse caso, convém que controles como monitoração de atividades, trilhas de auditoria e o acompanhamento gerencial sejam considerados.

Um problema crucial na segregação de funções é alocar as funções e responsabilidade para a pessoa certa no local adequado. Márcio Araújo [3], nos coloca uma reflexão: "Algumas organizações redesenham os processos após alocar as responsabilidades e funções, mas fica uma dúvida: caso exista erro na segregação de funções definida, meus processos já não estariam comprometidos já em sua concepção? Não seria melhor desenhar os processos e depois verificar quem irá executar tais funções evitando uma segregação inadequada de funções". Essa reflexão nos sugere que devemos tomar cuidados na segregação de funções. Redesenho de processos requer conhecimento do mesmo. Atribuir responsabilidades é também ser co-responsável pelo processo e requer constante reavaliação e adequação às necessidades.

10.1.4 – SEPARAÇÃO DE RECURSOS DE DESENVOLVIMENTO, TESTE E PRODUÇÃO



Com o objetivo de reduzir os riscos de acessos ou modificações não autorizadas aos sistemas operacionais, é necessário separar os recursos de desenvolvimento, testes e produção. Esses três ambientes deverão ter recursos de hardware e software semelhantes. Porém, os dados reais, necessários para a execução dos serviços da organização, armazenados em arquivos e bancos de dados, somente existirão no ambiente de produção, enquanto dados fictícios existirão nos ambientes de desenvolvimento e teste. Esta precaução evitará que os dados reais sejam danificados ou apagados em processos de desenvolvimento e teste.

Outro cuidado importante, é que o acesso a cada ambiente seja feito apenas por pessoal destinado a trabalhar em cada área. Assim, o ambiente de produção deverá ser acessado apenas por pessoal de produção, enquanto os ambientes de desenvolvimento e teste, só poderão ser acessados por pessoal das áreas respectivas.

É importante considerar que:

a. Regras claras para transferência de softwares da situação de "desenvolvimento" para a de "produção", devem ser definidas e documentadas. Essa transferência deve ser acompanhada de processos de gestão de mudanças (item 10.1.2), onde são previstos processos de recuperação em caso de falhas.

b. A separação de ambientes deve ser feita através da utilização de um ambiente de desenvolvimento independente do ambiente de produção, porém, com a mesma configuração de hardware e software. Assim, o software em desenvolvimento terá uma simulação do ambiente de produção, ao mesmo tempo em que protege os sistemas de produção contra mau funcionamento de sistemas, inclusão de códigos maliciosos, modificação de arquivos ou sistemas.

c. Para garantir a separação dos ambientes, é imprescindível que os usuários envolvidos em desenvolvimento e testes, tenham perfis de acesso diferentes para ambientes de teste e produção, e que todas as ações sejam registradas.

d. As ferramentas de desenvolvimento, como compiladores, e editores, não devem ser acessíveis a partir do ambiente do sistema operacional de produção.

e. Os ambientes de testes devem trabalhar com dados que não sejam sensíveis à organização, a fim de garantir a confidencialidade destes.

As considerações acima devem ser acompanhadas de rígido controle, com regras claras que podem ser acompanhadas inclusive de punições em caso de violação.

10.2 – GERENCIAMENTO DE SERVIÇOS TERCEIRIZADOS

- **Objetivo**: Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.

- **Terceirização**: processo de gestão pelo qual se repassam algumas atividades para terceiros, com os quais se estabelece uma relação de parceria.

Segundo Giosa [4] "terceirizar é um processo de gestão pelo qual se repassam algumas atividades para terceiros, com os quais se estabelece uma relação de parceria, ficando a empresa concentrada apenas em tarefas essencialmente ligadas ao negócio em que atua".

Esse conceito tem sido aplicado em diversas empresas para redução dos custos de serviços diversos, inclusive de tecnologia, como operação, desenvolvimento, suporte a usuários, ou mesmo na própria área de segurança da informação.

Porém, questões de segurança envolvidas no processo de contratação de serviços de terceiros, requerem cuidados para não expor a organização, uma vez que suas informações estarão acessíveis a uma parte externa.

Contratar um serviço de terceirização, requer uma avaliação profunda da empresa a ser contratada, observando, por exemplo, seu histórico, o tempo de atuação no mercado, referências de outros clientes que a contrataram, a qualidade do serviço prestado e a qualificação dos profissionais. Além disso, mesmo com a terceirização, as organizações continuam com uma gerência do processo.

A norma trata sobre o gerenciamento de serviços terceirizados, com o objetivo de implementar e manter o nível apropriado de segurança e de entrega de serviços

em consonância com os acordos de entrega de serviços terceirizados.

É importante que os contratos tenham descrição clara de cada serviço a ser entregue, seus objetivos e níveis de qualidade de serviço, com critérios de precisão e prazos.

10.2.1 – ENTREGA DE SERVIÇOS

- Cabe ao terceiro implementar e manter:
  - os controles de segurança,
  - as definições de serviço e
  - os níveis de entrega.

  } incluídos no acordo de entrega de serviços terceirizados

- Cabe a organização garantir que o terceiro seja capaz de manter o serviço em caso de falhas ou desastres.

Terceirizar é um processo que deve ser mantido através de acordos de entrega de serviço, onde são explicitados os controles de segurança, as definições de serviço e níveis de entrega.

Nos contratos firmados com os prestadores de serviços deve ficar claro que eles são integralmente responsáveis por suas ações, estando sujeitos à monitoração interna e às leis em vigor. Além disso, os acordos devem conter as informações necessárias para gerenciar o relacionamento entre a organização e o terceiro, como por exemplo, definições de relatórios periódicos.

Muitas organizações têm terceirizado os serviços, porém mantém uma gerência sobre o terceiro. Por isso, é importante garantir que os acordos de entrega de serviços de terceiros sejam implementados, executados e mantidos pelo terceiro. O terceirizado também deve elaborar um plano de trabalho detalhado, que deve ser levado à ciência da organização.

Especial cuidado deve ser tomado na transição de informação e recursos de processamento de informações a terceiros. A organização deve garantir que a segurança seja mentida durante esse processo, uma vez que informações poderão ser expostas ou os recursos poderão ser mal utilizados. A idoneidade e qualificação do terceiro devem ser rigorosamente investigadas para assegurar a confiabilidade do processo de terceirização.

Cabe a organização garantir que o terceiro mantenha capacidade de serviço suficiente para prover a continuidade de serviço em caso de falhas severas ou desastres. Para isso, processos de continuidade de serviço devem ser previstos juntamente com o terceirizado, garantindo que haja procedimentos bem claros para gerenciar incidências problemáticas, escopo e riscos.

10.2.2 – MONITORAMENTO E ANÁLISE CRÍTICA DE SERVIÇOS TERCEIRIZADOS

a. Monitorar níveis de desempenho de serviço
b. Analisar os relatórios de serviços produzidos por terceiros
c. Agendar reuniões de análise de progresso
d. Fornecer para análise informações sobre incidentes de segurança da informação
e. Analisar trilhas de auditoria e registros de eventos
f. Resolver e gerenciar problemas identificados

Ao utilizar os serviços de uma empresa terceirizada, a organização também transfere as responsabilidades das rotinas de gerenciamento. Porém, mesmo com essa transferência a organização continua tendo a responsabilidade final pelas informações tratadas pelo terceiro. Por isso, convém que seja atribuída a um indivíduo ou equipe da organização a responsabilidade do gerenciamento de relacionamento com o terceiro.

A organização também deverá disponibilizar recursos suficientes para o monitoramento dos requisitos do acordo, em especial dos requisitos de segurança. Existem, por exemplo, softwares de gestão de serviços terceirizados que podem ser adquiridos para a execução deste trabalho.

Para que seja possível validar o serviço e garantir seu bom andamento com segurança e com entrega de serviço dentro das expectativas acordadas entre as partes, o terceirizado deve fornecer relatórios e registros periódicos para serem monitorados e analisados criticamente. Além disso, auditorias regulares devem ser executadas.

O monitoramento e análise crítica de serviços terceirizados, objetivam a avaliação do desempenho do serviço terceirizado e dos possíveis problemas e incidentes de segurança da informação. A norma sugere o envolvimento de processos e relações de gerenciamento de serviço entre as parte para:

a. Monitorar níveis de desempenho de serviço a fim de verificar a aderência aos acordos. Todos os itens acordados no contrato deverão ser verificados quanto à qualidade do serviço, cumprimento de prazos, utilização de recursos e custos associados ao serviço. Listas de verificação do andamento poderão ser elaboradas para que se tenha um roteiro de avaliação. A avaliação fornecerá os parâmetros necessários para saber se o serviço será concluído dentro das expectativas baseado na definição e no contrato do projeto. Se houver acordos ou compromissos fora do contrato, estes devem ser adicionados na lista de verificação de modo que possa ser monitorado durante todo o serviço;

b. Analisar criticamente os relatórios de serviços produzidos por terceiros e agendamento de reuniões de progresso periódicas, conforme requerido pelos acordos. Nessas reuniões o terceirizado terá a oportunidade de esclarecer o status atual do serviço e se houve desvios justificáveis. Poderão ser estabelecidos novos marcos que servirão de pontos de reavaliação de progresso e validação;

c. Fornecer informações sobre incidentes de segurança da informação, bem como os procedimentos que foram aplicados para sua gerência. A análise desses dados deverá ser feita por ambas as partes;

d. Analisar criticamente as trilhas de auditoria do terceiro e registros de eventos de segurança, problemas operacionais, falhas, investigações de falhas e interrupções relativas ao serviço entregue;

e. Resolver e gerenciar quaisquer problemas identificados.

10.2.3 – GERENCIAMENTO DE MUDANÇAS PARA SERVIÇOS TERCEIRIZADOS

Convém levar em conta:

1. Mudanças feitas pela organização
   - Melhorias dos serviços oferecidos
   - Desenvolvimento de novas aplicações ou sistemas
   - Modificações dos procedimentos da organização
   - Novos controles para resolver os incidentes de segurança da informação
2. Mudanças em serviços de terceiros
   - Mudanças e melhorias em redes
   - Uso de novas tecnologias
   - Adoção de novos produtos ou novas versões
   - Novas ferramentas e ambientes de desenvolvimento

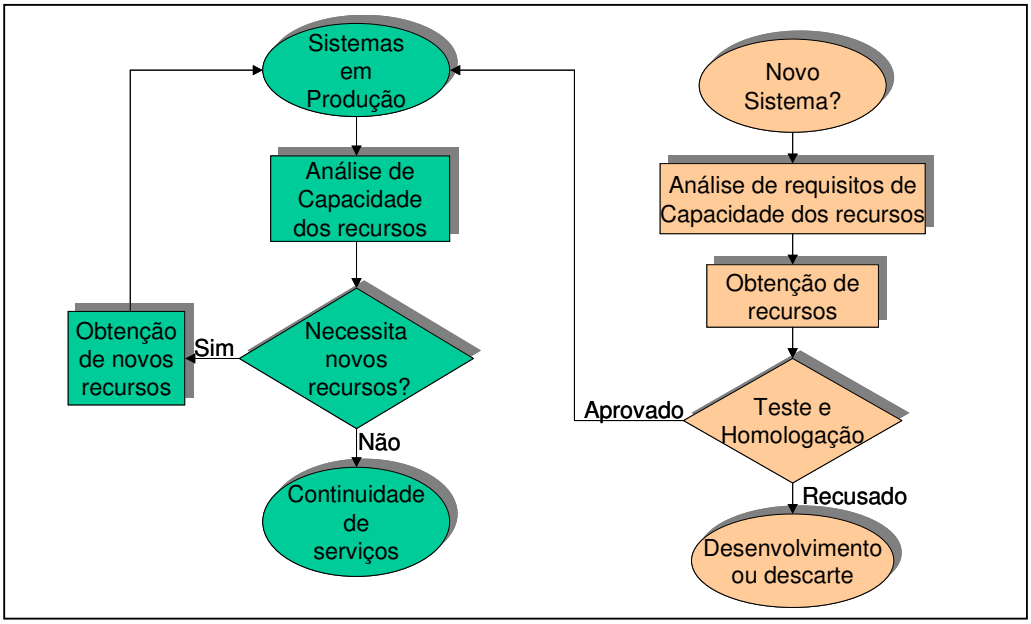
Todo processo, por melhor planejado que seja, está sujeito a mudanças seja para adaptações não previstas, seja para melhoria de procedimentos e controles, ou mesmo na manutenção ou melhoria de políticas de segurança da informação.

O processo de gestão de mudanças abordado no item 10.2.1, aplica-se à gestão de mudanças em serviços de terceiros, levando-se em conta que estes podem sofrer alterações devido a:

a. Mudanças feitas pela própria organização para implantação de:
   1. Melhorias dos serviços oferecidos;
   2. Desenvolvimento de novas aplicações ou sistemas;
   3. Modificações ou atualizações as políticas e procedimentos da organização;
   4. Novos controles para resolver os incidentes de segurança da informação e para melhoria da segurança.
b. Mudanças nos serviços de terceiros para implantação de:
   1. Mudanças e melhorias em redes;
   2. Uso de novas tecnologias;
   3. Adoção de novos produtos ou novas versões;
   4. Novas ferramentas e ambientes de desenvolvimento;

5. Mudanças da localização física dos recursos de serviços;
6. Mudanças de fornecedores.

10.3 – PLANEJAMENTO E ACEITAÇÃO DOS SISTEMAS



O desempenho desejado de um sistema é determinado pela capacidade que os recursos dispõe para desempenhar suas atividades. Por recursos, entenda-se o conjunto de equipamentos, materiais e pessoas necessárias para colocar e manter o sistema em funcionamento.

O mau planejamento da capacidade dos recursos pode trazer riscos como degradação de performance e falhas na rede e nas aplicações. Para minimizar esses riscos convém que haja um planejamento e monitoramento contínuo das capacidades dos recursos presentes. Além disso, uma análise de demanda por capacidade futura de recursos deve ser feita periodicamente para reduzir os riscos de sobrecarga dos sistemas.

É necessário ter em mente que a gestão da capacidade dos recursos afeta o desempenho da empresa, uma vez que os sistemas dependem deles para entregar o serviço demandado.

Para que novos sistemas sejam aceitos em ambiente de produção, os requisitos operacionais devem ser estabelecidos, documentados e homologados previamente.

10.3.1 – GESTÃO DE CAPACIDADE

- Gerir capacidades é buscar o equilíbrio entre o dimensionamento de recursos com o comportamento da demanda .
    1. Identifique os requisitos de capacidades
        - Requisitos tecnológicos
        - Pessoas
        - Espaço, outros
    2. Preveja a demanda por capacidade
    3. Sincronize e monitore os sistemas
    4. Implante controles detectivos

Gerir capacidades é buscar o equilíbrio entre o dimensionamento de recursos com o comportamento da demanda [5], ou seja, é a determinação dos recursos necessários para prevenir os impactos presentes e futuros no desempenho e disponibilidade dos sistemas. Atingir esse objetivo requer um trabalho contínuo de identificação dos requisitos de capacidade e avaliação da carga atual dos recursos confrontada com a capacidade efetiva dos mesmos.

1. *Identificação dos requisitos de capacidades*: vários tipos de capacidade são combinados para se realizar um trabalho. Por exemplo, equipamentos, pessoas e materiais, caminham juntas para proverem um serviço [6]. Para se colocar e manter um sistema de informação em funcionamento é necessário avaliar os vários recursos. Alguns são descritos abaixo. Outros podem ser identificados dependendo do sistema e da organização, e devem ser acrescentados:
    a. Recursos tecnológicos:
        i. CPU – deve ser garantido que o dispositivo tenha suficiente capacidade de CPU para suportar o sistema. Recursos insuficientes de CPU podem levar ao colapso total do sistema ou aumento de latência;
        ii. memória – quantidade de memória suficiente para o tratamento dos dados deve ser prevista a fim de evitar falhas do dispositivo;

iii. capacidade de armazenamento de dados – a quantidade, capacidade e velocidade dos dispositivos de armazenamento é um recurso fundamental para qualquer sistema de informação. Sua especificação deve levar em conta o número de transações por segundo demandada para assim dimensionar a velocidade da mídia, além da capacidade de armazenamento individual necessária para cada mídia, em função da quantidade de dados a ser armazenada.

iv. capacidade de tratamento de tráfego – os dispositivos de rede (switches, roteadores) devem ser dimensionados com capacidade de backplane suficiente para o tratamento de todos os dados que trafegam na rede, evitando assim os indesejáveis travamentos;

v. largura de banda e interface – refere-se aqui a quantidade de informações que pode ser transferida de um nó para outro em um determinado período. Dependendo do tipo de sistema implantado e do número de conexões necessárias, as requisições podem exigir maior ou menor largura de banda para as respostas. Em ambientes de WAN essa demanda é mais crítica, haja vista as limitações de banda inerentes. Acordos de garantia de nível de serviço devem ser previstos com provedores para suprir as necessidades de banda em WAN. A qualidade da interface e do meio de transmissão tem forte impacto na largura de banda;

b. pessoas – as pessoas utilizam os recursos físicos (equipamentos, materiais, informações) para desempenharem as tarefas que completam os trabalhos. A organização deve freqüentemente avaliar as competências e disponibilidades de pessoal para desempenharem as tarefas necessárias ao funcionamento do sistema.

c. espaço físico – este quesito muitas vezes é esquecido ao se avaliar as capacidades, porém é muito importante leva-lo em conta, uma vez que novos recursos podem demandar espaço físico para sua instalação e acomodação das pessoas que irão operá-lo, o que demandará custos a serem disponibilizados.

2. *Previsão da demanda*: as projeções de capacidade futura devem ser analisadas levando-se em conta os requisitos de novos negócios e sistemas e as tendências de capacidade de processamento de informação da organização.

3. *Sincronização e monitoramento dos sistemas*: Uma vez que as capacidades foram identificadas, as mesmas devem ser monitoradas para que possa ser determinada a necessidade de atualização do recurso.

Diferentes recursos requerem diferentes formas de medição. Por exemplo, disponibilidade de largura de banda em uma LAN é usualmente mais barata do que em uma WAN e, conseqüentemente, poderá ter um limiar mais baixo de aceitação. Tamanho de janelamento requerido para aplicações é um parâmetro para medida de desempenho da aplicação.

4. *Implantação de controles detectivos*: A fim de detectar e resolver problemas em tempo hábil, convém que controles detectivos sejam implantados. Ferramentas de diagnóstico de redes fornecem informações úteis para a determinação de taxas de utilização e verificação de pontos de ultrapassagem de limiares pré-estabelecidos que acusem necessidade de planejamento de uma atualização de capacidade antes que ocorra um problema.

As informações apuradas servirão para identificar e evitar os potencias gargalos e a dependência em pessoas-chave que possam representar ameaças à segurança dos sistemas ou aos serviços e planejar ação corretiva apropriada.

10.3.2 – ACEITAÇÃO DE SISTEMAS

Processo formal que mede:

- desempenho,
- usabilidade e
- funcionalidade

} do sistema

Inclui também testes que asseguram:

- Procedimentos de recuperação de erros e reinicilização;
- Concordância com os controles de segurança utilizados;
- Atendimento aos requisitos do negócio.

A aceitação de um sistema é o ponto no ciclo de vida do mesmo no qual cada aspecto da aplicação desenvolvida é validado antes de proceder à implantação do sistema.

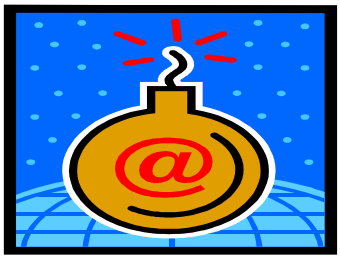
O teste de aceitação é talvez o ponto mais crítico no esforço de desenvolvimento de uma aplicação. É um processo formal onde o desempenho, aparência, usabilidade e funcionalidade do software, são medidas e comparadas com os critérios acertados anteriormente entre o desenvolvedor e o cliente. Nesse estágio, critérios de segurança também devem ser levados em conta, tais como:

- Procedimentos de recuperação de erros;
- Procedimentos de reinicialização e planos de contingência;
- Concordância sobre o conjunto de controles de segurança utilizados;
- Manuais esclarecedores;
- Medidas de continuidade do negócio;
- Treinamento de uso do novo sistema;
- Evidências que o sistema não afetará de forma negativa a base já instalada.

10.4 – PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS E CÓDIGOS MÓVEIS

Códigos maliciosos: todos os tipos de programa que executam ações maldosas em um computador.

Código móvel: é um código que tem sua fonte em um sistema remoto, porém executado em um sistema local.



A segurança de códigos executáveis é tratada normalmente pela área de sistemas operacionais.

O que se espera da execução de um código é que ele não danifique ou exponha a acessos indevidos, os dados ou os recursos acessíveis através de uma máquina.

Porém, aplicações maliciosas são concebidas para danificar, roubar ou dificultar o acesso a dados e recursos computacionais.

Um código malicioso é um termo genérico que se refere a todos os tipos de programa que executam ações maldosas em um computador. Exemplos de códigos maliciosos são vírus de computador, worms de rede, cavalos de tróia, etc.

Nem sempre é possível se prevenir da atuação de códigos ou sistemas maliciosos, mas muitas vezes é possível identificar a atuação desse tipo de sistema, permitindo atuar de forma a minimizar ou eliminar maiores danos.

O código móvel [7], por sua vez, denomina um conjunto de tecnologias de linguagem e plataforma de sistemas distribuídos que suportam a construção de programas de computador que são:

- instalados em computadores servidores;
- transferidos sob demanda para computadores clientes e;
- automaticamente executados sobre a plataforma dos computadores clientes.

Um exemplo de código móvel é o Flash que tem a sua execução iniciada por uma página HTML e roda em uma plataforma disparada pelo navegador.

Os vírus são a forma mais conhecida de códigos móveis maliciosos.

À medida que maiores quantidades de código são recebidas e executadas permissivamente, maiores são os riscos de danos ou contaminações por vírus, cavalos-de-tróia e worms (IBM, 1998).

Medidas de precaução devem ser tomadas para prevenir e detectar a introdução de códigos maliciosos e códigos móveis não autorizados.

10.4.1 – CONTROLES CONTRA CÓDIGOS MALICIOSOS

- Proibição de uso de softwares não autorizados;
- Proteção contra riscos de importação de arquivos;
- Atualização periódica de detectores de ataques;
- Verificação de códigos maliciosos em mídias, e-mail e páginas web;
- Treinamento de equipes de resposta;
- Planos de continuidade de negócio.

A norma ABNT ISO/17799:2005, recomenda que "sejam implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, bem como procedimentos de conscientização dos usuários". Para isso ela propõe uma série de diretrizes a serem consideradas.

Esses controles devem ser baseados em software de detecção de código malicioso e reparo, além da conscientização da segurança da informação, no controle de acesso adequado e nos controles de gerenciamento de mudanças.

Algumas medidas a serem tomadas são:

1. implantação de política de proibição de uso de softwares não autorizados;
2. medidas de proteção contra riscos inerentes à importação de arquivos e softwares;
3. atualização periódica de softwares de detecção e remoção de códigos maliciosos;
4. verificação, antes do uso, da existência de códigos maliciosos em arquivos armazenados em mídia, arquivos recebidos por e-mails e em páginas web;
5. treinamento dos membros responsáveis pela equipe de resposta que tratará da proteção contra ataques de códigos maliciosos, estabilizando a situação;
6. criar planos de continuidade de negócio para a recuperação em caso de ataques por código malicioso.

10.4.2 – CONTROLES CONTRA CÓDIGOS MÓVEIS

Use:

- bloqueio do uso de código móvel;
- compilação do código localmente através de compiladores confiáveis;
- verificação de códigos executáveis antes da sua execução;
- criar políticas de acesso a recurso;
- implantar controles de autenticação exclusiva do código móvel.

Ao usar códigos móveis autorizados, é desejável que o mesmo não danifique as informações da máquina que o está executando. Assim, o que se almeja é a proteção para que o código móvel não possa copiar, apagar ou alterar dados que não lhe dizem respeito em um computador. Tampouco se deseja que o sistema local altere a lógica de processamento para o qual o código móvel foi projetado.

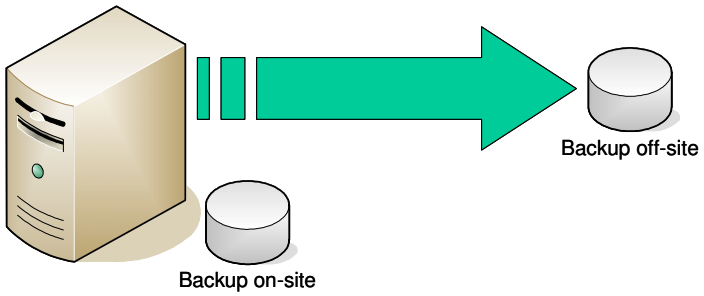
Logo, a execução de código móvel deve atender aos requisitos da política de segurança da organização, implantando algumas medidas, tais como:

1. bloqueio do uso de código móvel, exceto em casos específicos, com o conhecimento do responsável pela segurança da rede;
2. compilação do código localmente através de compiladores confiáveis;
3. verificação de códigos executáveis antes da sua execução;
4. criar políticas de acesso a recursos;
5. implantar controles de autenticação exclusiva do código móvel.

10.5 – CÓPIAS DE SEGURANÇA

Devem ser:

- De fácil recuperação com procedimentos verificados e testados regularmente;
- Armazenadas em local seguro;
- Periódicas;
- Identificadas;
- Utilizáveis.



Efetuar cópias de segurança (backup) é uma medida que visa possibilitar a recuperação de informações em caso de perda física dos dados originais devido a acidentes, garantindo assim a disponibilidade dos dados.

A política de backup deve conter os procedimentos e a infra-estrutura necessários à proteção de todo o acervo de dados da organização, possibilitando a continuidade de suas atividades [8].

Deve ser definido que dados e sistemas devem ser copiados, e com que freqüência.

Devem ser tomadas várias medidas de como fazer cópia de segurança para a eficiência do processo. Entre elas podemos destacar:

1. o acesso físico aos dados copiados deve ser protegido contra destruição física e contra acessos não autorizados;
2. configurações de sistemas devem ser guardadas separadamente;
3. execução de cópias de segurança deve ser periódica e com agendamentos a serem seguidos rigorosamente;
4. todos os backups devem ser identificados quanto ao seu conteúdo e data de atualização;
5. determinar quem tem os privilégios de execução de backup e recuperação (restore) dos dados;

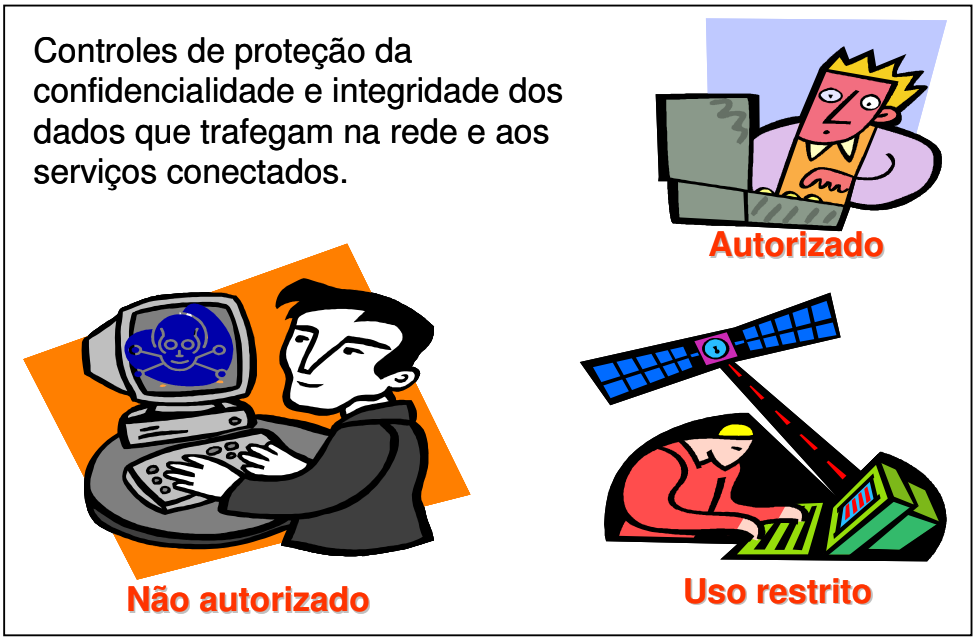
6. determinar quem pode enviar ou requisitar cópias de segurança fora do local;
7. é extremamente recomendável que haja duas cópias de segurança: uma no local próximo ao equipamento e outra local físico protegido e diferente do site original. Essa medida irá garantir que, caso haja uma catástrofe, ainda será possível conseguir recuperar os dados;
8. deve-se testar periodicamente se as cópias de segurança são utilizáveis, ou seja que não se deterioraram;
9. criar procedimentos para recuperação de cópias de segurança no menor tempo possível.

10.6 – GERENCIAMENTO DE SEGURANÇA EM REDES

Uma rede segura deve ser protegida contra códigos maliciosos e ataques inadvertidos e deve ao mesmo tempo estar em sintonia com os requerimentos do negócio.

Cabe aos gestores de segurança implementar os controles a fim de garantir a segurança dos dados em rede, bem como a proteção dos serviços disponibilizados contra acessos não autorizados.

10.6.1 – CONTROLES DE REDES



Para que uma rede possa ter um bom nível de segurança da informação, bem como seus serviços sejam protegidos, é essencial a implementação de controles que evitem acessos não autorizados. Várias medidas podem ser tomadas para a efetivação desses controles. Deve ser considerado:

1. para minimizar os riscos de uso acidental ou mau uso deliberado dos sistemas, a responsabilidade operacional pelas redes deve ser separada da operação dos recursos computacionais;
2. o estabelecimento de responsabilidades e procedimentos sobre o gerenciamento de equipamentos remotos, incluindo equipamentos em áreas de usuários;
3. implementação de controles para proteção da confidencialidade e integridade dos dados trafegando sobre redes públicas e sem fio, bem como aos sistemas e aplicações a elas conectadas. Esse quesito passa pela implantação de medidas de segurança como criptografia e VPNs;
4. Além de possuir meios para intimidar possíveis ataques, é imprescindível que a rede também disponha de meios para detectar os ataques. Portanto, mecanismos de registro e monitoração devem ser aplicados para que haja a gravação das ações relevantes de segurança. Devem ser registrados todos os eventos possíveis, permitindo analisar o que aconteceu e compreender o que estava ocorrendo em um determinado momento. Mas esses registros em si devem ser protegidos dos atacantes, para evitar que sejam alterados. Thomas Wadlow [9], sugere que os seguintes mecanismos devem ser empregados, a fim de evitar o acesso aos registros:
    i. os registros devem ser criptografados;
    ii. os registros devem ser armazenados somente para leitura;

iii. os registros devem ser armazenados em vários lugares.

5. a coordenação entre as atividades de gerenciamento, a fim de otimizar os serviços e assegurar que os controles estejam aplicados sobre toda a infra-estrutura de processamento da informação.

10.6.2 – SEGURANÇA DOS SERVIÇOS DE REDE

Refere-se a:

- determinação da capacidade de provedores de serviços
- proteção de serviços de redes privados
- soluções de segurança de rede como firewalls
- processos de detecção de intrusos

Os itens acima podem ser protegidos com:

- autenticação, encriptação e controles de conexão à rede
- restrições de acesso a serviços de rede

Existem inúmeros serviços que um site pode prover para seus usuários, alguns dos quais podem ser externos. Esses serviços têm cada um diferentes requerimentos de segurança. Estes requerimentos irão variar baseados na uso do servi;co em si. Por exemplo, um serviço que será usado apenas dentro do site, como um serviço de compartilhamento de arquivos e diretórios, irá requerer diferentes mecanismos de proteção do que um serviço provido para uso externo. Basta proteger o servidor interno contra acessos externos. Entretanto um servidor web, o qual provê páginas que devem ser vistas por qualquer usuário da Internet, irá requerer uma proteção e serviço/protocolo/servidor que evite acessos não autorizados e modificação da base de dados web.

Uma rede pode estar vulnerável por diversos meios. Um exemplo clássico é o problema da "negação de serviço", quando a rede é colocado em um estado no qual não se consegue legitimar os usuários na rede. Outro meio é o ataque a roteadores ou sobrecarga da rede por tráfico estranho (flooding).

Os serviços de rede incluem o fornecimento de conexões, serviços de rede privados, redes de valor agregado, firewalls e sistemas de detecção de intrusos.

Deve-se monitorar a capacidade do provedor de serviços de gerenciar os serviços a que se propõem.

Também é importante identificar os níveis de serviços e requisitos de gerenciamento. Uma vez identificados, os mesmos devem fazer parte de acordos de serviços de rede.

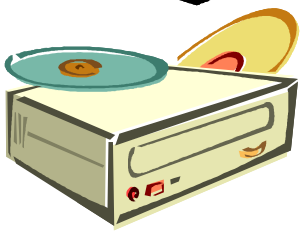
Várias técnicas devem ser observadas a fim de se obter segurança de acesso a serviços de redes, tais como:

1. ***autenticação de usuários***: através de senhas específicas os usuários autorizados ganham acesso à rede. Porém, como hoje as redes estão interconectadas e um usuário pode se logar remotamente à rede, sua senha é utilizada diversas vezes. Os riscos inerentes à captura dessa senha, que é enviada em forma de texto pleno, através de varreduras de pacotes (packet snnifers), tornam necessária a utilização de novos meios de autenticação, como PGP ou dispositivos baseados em tokens, apenas para citar alguns.
2. ***Confidencialidade***: para proteger a informação contra leituras não autorizadas, é recomendável a utilização de mecanismos como *criptografia* dos dados, permitindo ao administrador o controle de quem no sistema poderá acessar e "ver" o conteúdo dos arquivos.
3. ***Autorização***: refere-se ao processo de garantir privilégios para os processos e usuários. É diferente da autenticação, pois esta identifica o usuário.

10.7 – MANUSEIO DE MÍDIAS

Controle de ativos contra:

- divulgação não autorizada
- modificação
- remoção
- destruição



Para garantir a continuidade dos negócios sem interrupções, é imprescindível que os dados estejam sempre disponíveis a despeito de qualquer imprevisto.

Para isso é necessário que as mídias sejam controladas e protegidas fisicamente. Diversos mecanismos e procedimentos podem ser implementados para que cópias de mídias estejam disponíveis quando necessário. Também deve haver cuidados quanto ao descarte de mídias, pois os dados nela contidos poderão ser acessados se estiverem em bom estado após se desfazer da mídia.

10.7.1 – GERENCIAMENTO DE MÍDIAS REMOVÍVEIS

Mídias removíveis incluem fitas, discos, CD, DVD e mídia impressa. Medidas de gerenciamento destas mídias devem ser tomadas a fim de minimizar os impactos da perda ou deterioração das mesmas.

É muito importante que as mídias sejam identificadas, registradas e guardadas de forma segura. Isso irá garantir sua disponibilidade quando necessário.

O controle e registro de entradas e saídas de mídias da organização, devem ser documentados para que a mesma possa ser facilmente encontrada.

A destruição do conteúdo de uma mídia, quando não for mais necessário, deve ser executada quando a mídia for retirada da organização.

10.7.2 – DESCARTE DE MÍDIAS

Pessoas não autorizadas podem acessar mídias descartadas pela organização, caso os dados ainda estejam armazenados nelas. Por isso, procedimentos formais de destruição do conteúdo das mídias devem ser adotados.

O advento de softwares que conseguem recuperar mídias com dados apagados, sugere que as mídias devem não somente ser apagadas, como também fisicamente destruídas. Exemplos destes procedimentos é a trituração ou incineração da mídia.

Caso a mídia esteja em estado de reutilização, remova todos os dados.

Documente os procedimentos e autorizações de descarte seguro.

10.7.3 – PROCEDIMENTOS PARA TRATAMENTO DE INFORMAÇÃO

Para reforçar, as informações devem ser armazenadas e tratadas através de procedimentos que garantam sua fácil identificação, uso e remoção, apenas por pessoal autorizado.

Para isso, deve-se seguir alguns procedimentos:

a. tratar e identificar todas as mídias magnéticas;

b. criar procedimentos de controles de acesso às mídias;

c. dados a serem impressos devem ser protegidos de acordo com sua importância.

10.7.4 – SEGURANÇA DE DOCUMENTAÇÃO DE SISTEMAS

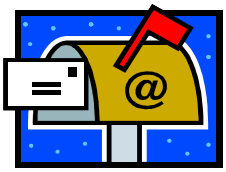
Documentação de sistemas contém informações que podem comprometer a segurança dos sistemas e dos recursos e dados a ele relacionados. Por isso, devem ser guardadas de forma segura com acesso restrito esteja em meio público ou privado.

10.8 – TROCA DE INFORMAÇÕES

Manter a segurança para troca de informação e softwares internamente à organização e entre organizações.

Crie procedimentos e controles para:

- conversas próximo a estranhos
- acessos de redes sem fio
- transporte de documentos e equipamentos



- conversas telefônicas (fixo ou celular)
- proteção de informações em trânsito
- Descarte de equipamentos, documentos e mídias

- envio, recebimento e retransmissão de mensagens

As informações que dizem respeito à organização, freqüentemente são trocadas ou compartilhadas por funcionários, clientes e/ou terceirizados. Essas trocas podem colocar em risco a confidencialidade da informação.

Criar uma política formal de troca de informação é um dos objetivos da norma ABNT ISO/IEC 17799:2005.

10.8.1 – POLÍTICAS E PROCEDIMENTOS PARA TROCA DE INFORMAÇÃO

É comum em saguão de aeroportos, ouvir executivos discutindo projetos. Se esses projetos fizerem parte de informações sensíveis para a organização, essa forma de conversa poderá comprometer o projeto caso um concorrente, por exemplo, a ouça.

Outro exemplo de risco é ligar um notebook em local público, onde as informações podem ser lidas na tela por pessoas mal intencionadas, ou capturadas através de conexões sem fio (wireless LAN) mal configuradas.

Em vista do exposto, medidas formais para troca de informações devem ser adotadas, tais como:

a. conscientização dos funcionários e terceiros quanto ao sigilo das informações passadas;
b. cuidados com envio e recebimento de e-mails contendo anexos que podem ter códigos maliciosos;
c. cuidados com segurança em redes sem fio (wireless LAN);
d. criptografia de dados transmitidos;
e. não deixar informações críticas esquecidas em copiadoras, impressoras, fax ou copiadoras, pois poderão ser vistas por pessoas não autorizadas;
f. não passar informações sensíveis por telefone quando estiver próximo a pessoas não autorizadas para ouvi-las;
g. certificar-se que não há grampos telefônicos;
h. lembrar de apagar mensagens em secretárias eletrônicas, a fim de evitar que outros tenham acesso às mesmas;
i. não armazenar dados pessoais, como endereços e senhas;

10.8.2 – ACORDOS PARA TROCA DE INFORMAÇÕES

A fim de garantir a confidencialidade na troca de informações entre organizações, devem ser criados acordos formais que destaquem de quem é a responsabilidade da operação e quais os procedimentos a serem adotados. Esses acordos devem ter um formato de contratos formais com condições de contratação.

O responsável ficará a cargo do controle de expedição e recepção das transmissões.

Para assessorá-lo devem ser criados procedimentos de notificação e acompanhamento dos eventos ocorridos, como: saber o status da informação a qualquer momento (com quem está, como está sendo usada, perda, modificações, qual o processo de transmissão usado, com que nível de segurança, tipo de embalagem , identificação dos portadores, quem procurar em caso de incidentes, normas para gravação e leitura da mesma.

10.8.3 – MÍDIAS EM TRÂNSITO

O transporte de mídias contendo informações, pode colocar os dados em riscos, por mera violação dos mesmos. Por exemplo, serviços de motoboys não qualificados podem danificar a mídia pelo mero transporte inadequado por uma pessoa não capacitada a manter os cuidados mínimos de acomodação da mídia, como a expondo ao calor ou luz ou a outro agente nocivo.

Para proteger é necessário considerar o uso de embalagens apropriadas, com identificação das mesmas e dos portadores.

A embalagem deve proteger o conteúdo contra quaisquer agentes externo nocivos à integridade física da mesma, observando as especificações do fabricante da mesma, além de conterem lacres que revelem tentativas de violação.

Também, pode ser considerada a divisão de conteúdo e envio por rotas distintas, pois caso uma parte seja violada ou danificada, a informação integral estará preservada.

10.8.4 – MENSAGENS ELETRÔNICAS

As informações trafegando por meio de mensagens eletrônicas, estão sujeitas a interceptação e acessos não autorizados. Criar mecanismos de proteção contra essas ameaças tornará mais seguro o trânsito das informações contidas na mensagem.

Considere a verificação da qualidade de segurança proporcionada por meios públicos de transmissão de mensagens, como serviços de comunicação online

por voz e mensagens eletrônicas como MSN, Skype e outros.

Conscientize os usuários de que devem ter cuidados para se assegurarem que o endereçamento da mensagem está correto.

Use meios de criptografia da mensagem a fim de dificultar sua interpretação caso seja interceptada.

10.8.5 – SISTEMAS DE INFORMAÇÕES DO NEGÓCIO

Os vários meios combinados de comunicação de escritórios, como fax, computadores, copiadoras, redes sem fio, sistemas postais, comunicação de memorandos e outros, permitem a agilidade da troca de informação com o compartilhamento das mesmas, implicando na agilidade dos negócios, mas também impondo riscos de vazamento de informações. É preciso determinar essas vulnerabilidades e criar procedimentos que protejam essas informações.

Como exemplo, temos sistemas de gravação de mensagens em secretárias eletrônicas, compartilhamento de informação através de teleconferência, armazenamento de faxes, são sistemas de difícil proteção, uma vez que podem ser facilmente acessados por quem tenha acesso aos locais desses eventos. Políticas de controle de acessos aos ambientes, proporcionam relativa proteção nesses casos.

Também deve ser considerado o uso de restrições de acesso aos recursos, classificando os funcionários, terceiros e fornecedores em grupos separadamente.

O compartilhamento de informações, requer políticas especiais para controle adequados.

Enfim, toda e qualquer informação sensível ou não à organização que passa pelos sistemas de informação, deve ser considerada para avaliação e criação de procedimentos de proteção.

10.9 – SERVIÇOS DE COMÉRCIO ELETRÔNICO

Proteção do comércio eletrônico, transações on-line e acessos web.

- Principais práticas:
  - . criptografia de dados
  - . uso de assinatura digital
  - . uso de certificado digital

O comércio eletrônico mudou a maneira das empresas de fazer negócios. Anualmente bilhões de dólares trafegam pela Internet na forma de operações de compra e venda de mercadorias e serviços. Os benefícios deste tipo de negócios são imensuráveis, porém, associados a eles existem riscos de roubo de informações, senhas, número de contas, além de ocorrerem negócios fraudulentos que comprometem a integridade e disponibilidade da informação.

Garantir a segurança dos serviços de comércio eletrônico, significa proteger o negócio em si caso esse tipo de transação faça parte do faturamento da organização.

10.9.1 – COMÉRCIO ELETRÔNICO E TRANSAÇÕES ON-LINE

A melhor maneira de proteger o comércio eletrônico e as transações on-line é fazendo uso de meios criptográficos, que embaralham a informação, não permitindo sua interpretação caso seja interceptada por acessos não autorizados.

Para garantir a autenticidade da transação, podem ser usados os certificados digitais e assinaturas digitais. Grosso modo, certificados digitais "são como carteiras de identidade digitais que servem para identificar com segurança uma pessoa (assinatura digital) ou um site/servidor (certificado de servidor SSL) no ambiente virtual. Ambas possuem também outras funções ligadas à segurança: Os certificados de servidor também possibilitam a codificação (encriptação) dos dados entre o browser do internauta e o servidor onde está hospedado o site, garantindo que dados sigilosos tais como números de cartões de crédito trafeguem com segurança pela rede. As assinaturas digitais possibilitam a autenticação de documentos ou processos - outorgando inclusive valor legal - e a codificação do conteúdo desses documentos para que só possam ser visualizadas pelo destinatário autêntico. [10]".

Ao pensar em segurança de comércio eletrônico e transações on-line, deve ser levada em conta a natureza da operação. Essa passa por meios que podem sofrer ataques nas interconexões, levando a grandes prejuízos. Por isso, medidas de proteção como implementação de firewall, uso de VPN, criptografia, certificados e assinaturas digitais, podem proporcionar o nível de segurança adequado às transações.

Também deve ser considerada a prática de implantação de acordo formal que comprometa as partes em procedimentos de comércio eletrônico entre parceiros comerciais.

10.9.2 – INFORMAÇÕES PUBLICAMENTE DISPONÍVEIS

Informações publicamente disponíveis, como páginas web armazenadas em servidores, precisam ser protegidas contra modificações não autorizadas. Para tal podem ser usados mecanismos semelhantes aos utilizados no item anterior, como assinaturas digitais e certificados. Essas informações devem ser protegidas a qualquer momento do acesso (durante a coleta, processamento e armazenamento).

10.10 – MONITORAMENTO

Meios para detectar atividades não autorizadas de processamento de informação.

Consiste em:

- Registros (logs) de atividades de usuários
- Análise dos registros
- Detecção de tentativas de ataques
- Proteção dos registros
- Registros de falhas

Além de possuir meios de evitar possíveis fraudes ou ataques à rede, é necessário dispor de meios para detectar atividades não autorizadas de processamento de informação. Sem o monitoramento nunca será possível saber como estão atuando as proteções implementadas.

Para monitorar um sistema de processamento da informação é preciso criar mecanismos de registros de acesso e falhas, a fim de identificá-los e verificar a eficácia da proteção.

Como disse Thomas Wadlow [11], uma das metas de um sistema de monitoração é reduzir tão próximo de zero quanto possível a probabilidade de um ataque ocorrer sem ser registrado, ao mesmo tempo em que se aumenta tão próximo de 10% quanto possível a probabilidade de os eventos registrados de um ataque serem reconhecidos como um ataque.

10.10.1 – REGISTROS DE AUDITORIA

Os registros de auditoria contêm as atividades dos usuários, exceções e outros eventos de segurança de informação. É mais fácil descobrir ataques e atacantes pela análise de registros do que detecta-los no momento do ataque.

Para se conseguir uma boa amostragem de dados capaz de denunciar um ataque, deve ser registrado qualquer evento que identifique padrões comuns e não tão comuns de ataques. Informações para registros incluem:

a. identificação de usuários;
b. datas e horários dos eventos;
c. identidade do terminal;
d. registros de tentativas de acesso aceitas e rejeitadas;
e. alteração de configuração de sistema;
f. uso de privilégios;
g. uso de aplicações, utilitários e recursos;
h. arquivos acessados e tipo de acesso;
i. endereço e protocolos de rede;
j. alarmes disparados pelo sistema de controle de acesso;
k. ativação e desativação dos sistemas de proteção (antivírus e sistemas de detecção de intrusos).

10.10.2 – MONITORAMENTO DO USO DO SISTEMA

De posse dos registros de auditoria, deve-se proceder à análise dos mesmos. De nada adianta coletar dados sem analisá-los e emitir conclusões. Um sistema de monitoramento serve aos propósitos de detecção de tentativas de ataques. Os registros mostrarão várias dessas tentativas.

O nível de monitoramento dos recursos deve ser determinado através da analise/avaliação dos riscos.

Para a análise dos registros, consiste na procura por padrões nos registros. Logo se chegará à conclusão que o sistema de registros oferece uma compreensão sobre a rede.

10.10.3 – PROTEÇÃO DAS INFORMAÇÕES DOS REGISTROS (LOG)

Existe a possibilidade de que os registros (logs) sejam falsificados por um atacante. Isso pode ser conseguido através do ataque às entradas de registros que já foram feitas ou a entradas que serão feitas no futuro.

Para alterar as entradas o atacante deve ter acesso aos registros. Para evitar esse acesso, pense nos seguintes registros:

a. manter os registros em uma máquina separada;
b. criptografe os registros;
c. gravar os registros somente para leitura;
d. fazer com que o sistema de registros inclua informações sobre tentativas de início de uma sessão, em vez de registrar o sucesso ou fracasso de início das sessões.

Para minimizar falhas nos sistemas de registros (logs), considere que a mídia magnética que armazena os registros deve ter sua capacidade dimensionada para o volume necessário dos registros. O uso da capacidade do meio de armazenamento requer uma administração uma vez que o arquivo continuará a crescer até esgotar o espaço disponível na máquina. Wadlow sugere-se o uso de mecanismos de rodízio de registros, no qual os arquivos de registros antigos e cheios são movidos para outro local e os arquivos de registros novos e vazios passam a ocupar o seu lugar.

10.10.4 – REGISTROS (LOG) DE ADMINISTRADOR E OPERADOR

Os administradores e operadores do sistema devem ter suas atividades registradas. Os registros devem ser os mesmos que foram listados no item 10.10.1, registrando em que conta eles estão utilizando os serviços e em que processo.

10.10.5 – REGISTROS (LOG) DE FALHAS

As falhas ocorridas também devem ser registradas. Sua análise fornecerá dados para a tomada de ações que evitem novos eventos de segurança. Nunca despreze as falhas informadas por usuários ou pelos programas. Com esses dados faça uma análise crítica dos registros e determine se as falhas foram resolvidas.

10.10.6 – SINCRONIZAÇÃO DOS RELÓGIOS

Para que os registros (logs) tenham exatidão com os eventos, é importante que todos os relógios de todos os sistemas estejam sincronizados de acordo com a hora oficial e assim facilitarão a auditoria do sistema.

Módulo
11

11 – CONTROLE DE ACESSOS

POR ARTHUR SANTOS JR.

TRATAREMOS NESTE CAPÍTULO DE CONCEITOS IMPORTANTES QUE DEVEM SER IMPLEMENTADOS EM ORGANIZAÇÕES, A FIM DE SE OBTER O CONTROLE DE ACESSO DE USUÁRIOS A SISTEMAS DE INFORMAÇÃO, PROTEGENDO OS DADOS, PROGRAMAS E ARQUIVOS CONTRA ACESSOS NÃO AUTORIZADOS.

11.1 – REQUISITOS DE NEGÓCIO PARA CONTROLE DE ACESSO

- Premissa: ***tudo é proibido exceto o que é expressamente permitido.***

- A política de controle de acesso leva em conta:
  - Os requisitos de segurança das aplicações do negócio;
  - A Identificação das informações;
  - A legislação aplicável;
  - Administração de direitos de acesso e remoção

Os controles de acesso têm o objetivo de proteger equipamentos, aplicações, arquivos e dados contra perda, modificação ou divulgação não autorizada. Diferente, porém, de outros tipos de recursos, os sistemas computacionais não podem ser facilmente controlados por dispositivos físicos (alarmes, cadeados, etc...).

Os controles de acesso são um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou outros programas.

O controle de acesso pode ser visto a partir do recurso computacional que se quer proteger e a partir do usuário a quem será concedido privilégios e acessos aos recursos.

O controle de acesso a recursos de informação é uma das principais tarefas do administrador de uma rede. Através deste controle é possível determinar quais recursos podem ser acessados por determinados usuários e que tipo de acesso pode ser realizado. Através de auditoria, também é possível determinar que tipo de acesso foi realizado a um recurso, por quem e quando.

Para executar essa função com critério, regras de controle de acesso devem ser criadas baseadas nas políticas de autorização e divulgação da informação.

11.1.1 – POLÍTICA DE CONTROLE DE ACESSO

A restrição do acesso às informações deve estar em consonância com os requisitos de negócio. Isso requer que uma política de controle de acesso seja formalizada, levando-se em conta:

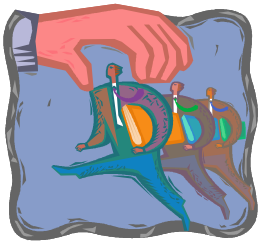
- Os requisitos de segurança das aplicações do negócio;
- A identificação de todas as informações referentes às aplicações;
- A consistência entre controle de acesso e políticas de classificação da informação;
- A legislação aplicável e obrigações contratuais;
- A administração de direitos de acesso e remoção dos mesmos.

Para a implantação de controles de acesso, devem ser criadas regras que sejam compatíveis com as políticas de autorização, lembrando da premissa de que *tudo deve ser proibido a menos que seja expressamente permitido*.

Também é importante que o responsável pela política de controle de acesso, realize periodicamente uma análise crítica dos direitos e privilégios dos usuários.

11.2 – GERENCIAMENTO DE ACESSO DO USUÁRIO

Objetivo: assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.



Obtido através de:

- Registro de usuário (ID e senha);
- Gerenciamento de privilégios a usuários e recursos;
- Gerenciamento de senhas do usuário;
- Análise dos direitos de acesso do usuário.

O gerenciamento de acesso do usuário visa garantir o acesso dos usuários onde os gestores da informação definiram ao mesmo tempo em que se previne o acesso não-autorizado a recursos onde o usuário não possui privilégios.

Procedimentos devem ser criados para o controle da distribuição de direitos de acesso a sistemas de informação, bem como a acessos de usuários. Estes procedimentos deverão abordar desde a concessão inicial de acesso a um novo usuário, passando por análises periódicas ao longo do tempo de permanência do usuário na organização, até fechar com o desligamento do usuário, quando todos os direitos de acesso e privilégios deverão ser revogados.

11.2.1 – REGISTRO DO USUÁRIO

A identificação e autenticação de um usuário (confirmação de que o usuário é quem diz ser) são feitas normalmente através de um identificador de usuário (ID ou login name) e uma senha durante o processo de logon no sistema. Com os avanços tecnológicos temos cada vez mais a presença de um segundo fator de autenticação neste processo, este fator pode ser algo que o usuário possui (token, smart card,etc.) ou algo que ele é (impressão digital, íris, voz, etc.).

A fim de padronizar e facilitar o gerenciamento de acesso do usuário deve ser criado um procedimento formal de registro e cancelamento de um usuário (registro e cancelamento de seu ID e senha) para garantir e revogar acessos a que ele tem direito em todos os sistemas e serviços.

Os procedimentos de controle devem incluir:

a. a verificação da autorização do proprietário do sistema para o uso do sistema de informação ou serviço;
b. confirmação através de documento escrito de que o usuário entende as condições de acesso;
c. remover ou modificar direitos de acesso a usuários que mudaram de funções ou se desligaram da organização;
d. cuidar para que não haja IDs redundantes.

11.2.2 – GERENCIAMENTO DE PRIVILÉGIOS

O fato de o usuário ter sido identificado e autenticado significa apenas que ele é reconhecido pelo sistema como um usuário previamente cadastrado, isso não significa que ele poderá ter acesso a qualquer informação ou recurso sem restrições.

Deve ser implementado controle específico através de concessão de privilégios que limitem o acesso do usuário, apenas ao que realmente lhe é necessário para a condução de seu trabalho, a fim de que possa desempenhar suas funções.

A concessão de privilégios de acesso pode ser feita com foco no usuário ou no recurso, dependendo da forma de funcionamento do sistema.

Os privilégios de usuário são atributos associados a um usuário, que definem quais recursos ele poderá acessar e o que ele pode ou não fazer com esses recursos (ler, alterar, etc.).

Os privilégios, ou direitos, de acesso a um recurso, são armazenados com o próprio recurso formando uma lista de controle de acesso. Neste método o recurso guarda o ID do usuário que pode acessá-lo e também a informação sobre quais tipos de acesso este usuário pode realizar.

A concessão de privilégios é prerrogativa do responsável pela rede e do responsável pela segurança da informação na organização. Ao conceder

privilégios é recomendável que se utilize um processo formal de autorização, onde deve ser levado em conta que:

a. os privilégios devem ser concedidos apenas se houver necessidade, e desde que não estejam ferindo a política de segurança;
b. as listas de controles de acesso devem ser feitas pelo proprietário (gestor) do recurso, o qual determinará o tipo de proteção adequada a cada recurso e quem terá acesso a eles;
c. deve ser criado um processo de autorização e um registro de todos os privilégios concedidos.

11.2.3 – GERENCIAMENTO SENHAS DO USUÁRIO

Após a identificação do usuário através de seu ID, o mesmo deve ser autenticado a fim de que o sistema possa conferir se o usuário é quem realmente diz ser. Conforme dito anteriormente, isso é feito através de algo que só ele saiba, seja ou possua. A solicitação de uma senha é o meio mais comum de autenticação de um usuário, porém existem outros métodos baseados nas características biométricas da pessoa (íris, retina, reconhecimento de voz ou impressão digital), ou em algo que este possua (cartões, crachás e tokens).

Qualquer que seja o método empregado, esse requer um gerenciamento formal que controle a concessão das ID's, considerando os seguintes requisitos:

a. assinatura do usuário em um documento comprometendo-se a manter confidencialidade de sua senha;
b. fornecer ID's temporários e únicos que obriguem o usuário a alterá-las quando do primeiro acesso;
c. utilizar meios seguros para informar a senha ao usuário;
d. prover uma forma segura de armazenar senhas no sistema de um computador;
e. alterar senhas padrões de instalação de sistemas ou softwares.

11.2.4 – ANÁLISE CRÍTICA DOS DIREITOS DO USUÁRIO

A análise dos direitos de acesso deve ser executada periodicamente a fim de se determinar se os direitos concedidos ainda são válidos para aquele usuário. Esse cuidado visa garantir o controle efetivo dos acessos às informações e recursos.

Recomenda-se que a periodicidade varie entre três e seis meses para todas as contas de usuário, devendo também ser executada para um usuário específico sempre que houver mudança de função ou cargo deste, ou o mesmo se desligar da organização.

11.3 – RESPONSABILIDADES DOS USUÁRIOS

Objetivo: prevenir o acesso não autorizado dos usuários e evitar danos ou roubo da informação e dos recursos de processamento da informação.

Obtida através de:

- Conscientização de usuários quanto a política de uso de senhas e equipamentos;
- Cooperação de usuários;
- Implementação de política de mesa limpa.

Nenhuma política de segurança seria eficaz sem a cooperação dos usuários autorizados. Por esse motivo, os mesmos devem estar cientes de suas responsabilidades para manter o controle de acesso, guardando a confidencialidade das senhas e a proteção dos equipamentos que utilizem.

11.3.1 – USO DE SENHAS

O uso de senhas requer certos cuidados que dependem do usuário e, portanto, a segurança depende do conhecimento deste no uso correto de senhas. Os usuários devem ter pleno conhecimento das políticas de senha e devem segui-las à risca.

Algumas diretrizes devem ser seguidas para manter esse nível de segurança, tais como:

a. evitar escrever a senha em papel ou armazená-la em arquivos ou memória de dispositivos móveis, como em agenda de celulares. Procure memorizar a senha e apagá-la da fonte de onde a recebeu (papel, e-mail, gravada em arquivo, etc...);

b. não compartilhar senhas;

c. manter a confidencialidade da senha;

d. ao menor indício de comprometimento de uma senha, altere-a imediatamente;

e. ao escolher uma senha, lembre-se de:

   i. evitar senhas muito curtas ou muito longas (oito dígitos no mínimo é o recomendável);

   ii. evite senhas óbvias, como seu sobrenome, datas de aniversário, nome da namorada, número de telefone, placa de carro, etc;

   iii. crie senhas com caracteres e números a fim de evitar ataques de dicionário;

   iv. não repita caracteres e não use caracteres seguidos do teclado (QWERT, LKJHGF, QAZWSX);

   v. Crie senhas distintas para sistemas distintos.

f. altere a senha a intervalos regulares e não repita senhas antigas.

11.3.2 – EQUIPAMENTOS DE USUÁRIO SEM MONITORAÇÃO

Em uma organização pode haver vários equipamentos que não são monitorados. Para assegurar a proteção dos mesmos, é recomendável orientar os usuários sobre como protegê-los adequadamente. Para isso, oriente-os a encerrar as sessões ativas, efetuar a desconexão dos sistemas ao fim da sessão e proteger os computadores e terminais através de bloqueio de tecla ou outro controle equivalente.

11.3.3 – POLÍTICA DE MESA LIMPA E TELA LIMPA

A política de mesa e tela limpa deve ser adotada e utilizada pelos funcionários e terceiros na organização, a fim de que papéis e mídias removíveis não fiquem expostos a acessos não autorizados.

Caso o usuário não esteja usando a informação, a mesma não deve ficar exposta. Para implantar essa política considere os seguintes quesitos:

a. armazene em lugar seguro todas as informações impressas;

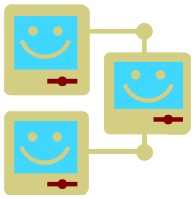
b. papéis e mídias que não estiverem sendo usadas, não devem ser deixadas sobre a mesa;

c. não deixe nenhum arquivo aberto quando não estiver usando o computador;

d. proteja os terminais e computadores com mecanismos de travamento de tela e teclados;
e. proteja pontos de entrada e saída de correspondências e qualquer tecnologia de reprodução;
f. fotocopiadoras devem ser utilizadas apenas por pessoal autorizado;
g. remova imediatamente os documentos impressos nas impressoras.

11.4 – CONTROLE DE ACESSO À REDE

Objetivo: Prevenir acesso não autorizado aos serviços de rede.



Obtida através de:

- Controles de acesso interno e externo aos serviços de rede;
- Uso de interfaces apropriadas entre a rede da organização e as redes de outras organizações e redes públicas;
- mecanismos de autenticação para usuários e equipamentos;
- Separação de redes em diferentes domínios;
- Controle de roteamento de rede com a verificação de endereços de origem e destinos.

O objetivo da infra-estrutura de TI é criar sistemas capazes de detectar e proteger a rede contra acesso não autorizado e, ao mesmo tempo, fornecer acesso imediato a usuários legítimos.

Da mesma forma, os acessos aos serviços de rede internos e externos devem ser controlados e, ao mesmo tempo, os usuários com acessos legítimos não podem comprometer a segurança dos serviços disponibilizados, fazendo-se necessários adotar medidas de controle eficazes para esse fim.

11.4.1 – POLÍTICA DE USO DOS SERVIÇOS DE REDE

Os acessos aos serviços de rede devem ser tal que os usuários tenham direitos e privilégios de acesso apenas ao que realmente precisam para desempenhar suas funções.

Recomenda-se que seja criada uma política de uso de redes, que englobe os procedimentos de autorização de acessos a serviços (discriminando quem pode acessar o que e quando pode fazê-lo), procedimentos de proteção dos acessos a conexões e serviços de redes, bem como dos meios usados para acessar a rede (condições para conexões discadas, por exemplo).

11.4.2 – AUTORIZAÇÃO PARA CONEXÃO EXTERNA DO USUÁRIO

Com o advento dos meios de conexão externa, como linhas discadas, conexão sem fio, banda larga e acessos dedicados, diversos usuários podem agora executar trabalhos remotos, se conectando à rede da organização estejam onde estiverem. Essas facilidades trazem um risco inerente ao acesso nas aplicações de negócio que é a dificuldade de identificação de quem está tentando o acesso. Logo, procedimentos de autenticação de acesso de usuários remotos devem ser criados, a fim de proteger as conexões externas.

Diversas técnicas estão disponíveis para obter a autenticação de usuários externos. Essas técnicas podem ser implementadas com o uso de VPNs (Virtual Private Network), além do uso de linhas privadas dedicadas. Algumas dessas técnicas são baseadas em:

a. criptografia, que é uma técnica para embaralhar, segundo um algoritmo pré-definido, as informações de credenciais de usuário, transmitidas e recebidas, durante o processo de autenticação;
b. tokens, que é um objeto que o usuário possui que o diferencia de outras pessoas e o habilita a acessar um recurso. Por exemplo, cartões magnéticos. É como usar a chave de sua casa. Apenas você pode abrir a porta de sua casa, uma vez que só você possui a chave correta;
c. protocolos de desafio/resposta, como protocolos EAP (Enhanced Authentication Protocol) que colocam um desafio ao sistema do usuário, a fim de que ele responda corretamente.

Conexões remotas não autorizadas aos recursos de uma organização podem ser evitadas com o uso de procedimentos de controle de discagem reversa, em que o usuário é autenticado em sua tentativa de conexão à rede. A norma, porém recomenda que esse controle não use transferências de chamadas. Além disso, o processo de discagem reversa deve assegurar a desconexão no lado da organização.

11.4.3 – IDENTIFICAÇÃO DE EQUIPAMENTOS EM REDE

Além da identificação de usuário, sistemas de identificação de equipamentos que podem acessar a rede devem ser considerados, a fim de garantir que os acessos serão feitos de um local ou equipamento autorizado. A identificação pode ser obtida através, por exemplo, do endereço MAC de uma placa de rede, usando-se filtros de acesso que controlam qual equipamento tem permissão de acessar a rede. Esse tipo de filtro é comum em redes sem fio. Dessa forma, somente equipamentos cadastrados no recurso poderão ter acesso à rede.

Após a identificação do equipamento, procede-se a identificação do usuário. Equipamentos com acesso permitido devem ter seu acesso físico também protegido, o que pode ser conseguido com instalação dos mesmos em local de acesso restrito e/ou implementando procedimentos de travamento de teclado e telas.

11.4.4 – PROTEÇÃO E CONFIGURAÇÃO DE PORTAS DE DIAGNÓSTICO REMOTAS

Portas de diagnóstico permitem que o responsável pela rede execute conexões, configurações e testes específicos nos dispositivos de rede e nos computadores a ela conectados. Proteger essas portas contra acessos não autorizados requer uma combinação de técnicas, como o uso de teclas de bloqueio além do controle de acesso físico às mesmas.

Nos computadores, as portas que não estiverem sendo utilizadas, bem como aquelas instaladas especificamente para diagnóstico devem ser desabilitadas por padrão, sendo habilitadas apenas por pessoal autorizado quando necessário.

11.4.5 – SEGREGAÇÃO DE REDES

Atualmente as redes não podem mais ser protegida cuidando apenas de seu perímetro. As organizações estão conectadas à Internet em redes convergentes, o que expôs o ambiente que antes era reservado e controlado. Este ambiente está agora aberto a parceiros em extranets, conexões de pontos de venda, além de funcionários com trabalhos remotos. Os dispositivos usados para acessar essas redes podem ser um canal para ataques e usos inadequados.

Uma forma de controlar a segurança da informação é separar as redes em domínios diferentes, por exemplo, redes internas e externas, protegendo cada uma por um perímetro de segurança definido. Esse perímetro pode ser implementado com a utilização de um gateway, como um firewall, entre as redes, que controlará o acesso e fluxo de informação entre elas.

Também é uma boa medida de segurança a utilização de VLAN (Virtual Local Area Network), caso haja switches camada 3 para roteamento de pacotes entre as VLANs.

Redes sem fio requerem especial atenção, uma vez que o perímetro físico da rede não é bem definido, haja vista se tratar de um sinal de radiofreqüência que

se espalha pelo ambiente e pode ultrapassar os limites da organização. Implementações de comunicação criptografada nesse meio são imprescindíveis para a segurança da informação, aliada a forte autenticação de usuários e autorização de equipamentos móveis. Deve ser considerada a separação de redes sem fio de redes internas, fazendo uso de firewalls, além de implementar conexões seguras com o uso de VPN.

11.4.6 – CONTROLE DE CONEXÕES DE REDE

O acesso dos usuários à rede deve ser restringido através de regras predefinidas, implementadas em gateways que filtram o tráfego. Essas restrições devem ser aplicadas a qualquer tipo de transferência de informação, como e-mails, transferência de arquivos e acessos a aplicações.

Controles de acesso entre redes com limitação de horários de uso também fazem parte de uma boa política de controle de conexões entre redes.

11.4.7 – CONTROLE DE ROTEAMENTO DE REDE

A fim de garantir a integridade da informação trafegando entre redes, devem ser implementadas medidas de validação de endereços de origem e destino dos pacotes, nos pontos de controle de rede interna e externa. Essa tarefa pode ser executada nos gateways de segurança.

Controlar o tráfego entre redes é uma tarefa cada vez mais complexa e os implementadores devem estar cientes da força e deficiência dos mecanismos que implantarem. O surgimento de interfaces de aplicativos com base em protocolos de mensagens, como o XML (Extensible Markup Language), facilitou o comércio eletrônico, porém introduziu vulnerabilidades e ataques que precisam ser combatidos. Dados que antes estavam em vários protocolos de rede e podiam ser facilmente filtrados por políticas de firewall, agora estão combinados em um único protocolo de transporte (HTTP na porta 80). Isso dificulta a identificação do pacote pelo cabeçalho e torna necessária a verificação do payload do pacote, o que vai além das defesas clássicas da rede. Como as organizações passam cada vez mais a utilizar criptografia do tráfego de aplicativos através de protocolos SSL/TLS (Socket Layer/Transport Layer Security) e HTTPS (Http Secure Socket), também torna-se cada vez mais difícil a aplicação de políticas de acesso aos pontos de rede porque é mais difícil inspecionar o payload dos pacotes desses tipos de fluxos [12]. Assim, recomenda-se a análise de controles para restringir a capacidade de conexão dos usuários.

11.5 – CONTROLE DE ACESSO AO SISTEMA OPERACIONAL

Objetivo: prevenir o acesso aos sistemas operacionais.

Obtidos com:

- Autenticação de usuários autorizados;
- Registros de sucessos ou falhas nas tentativas de acesso ao sistema;
- Registros do uso de privilégios especiais do sistema;
- Disparo de alarmes quando da violação da segurança do sistema;
- Restrições do tempo de conexão dos usuários.

Os sistemas operacionais devem ter o acesso restrito apenas a usuários autorizados, valendo-se para isso do uso de recursos de segurança da informação.

Os recursos de segurança devem levar em conta a política de acesso definida para organização, além de permitir o registro de acessos e uso de privilégios do sistema. Também deve permitir a implantação de sistemas de alerta através de alarmes caso haja violação da segurança, além de restringir o tempo de conexão dos usuários.

11.5.1 – PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA (LOG-ON)

Os usuários dos sistemas são identificados e autenticados durante o processo do log-on. Os processo de log-on permitem conceder acesso às informações e aplicativos em um sistema.

Para a maior proteção dos acessos, é conveniente que o procedimento de log-on divulgue o mínimo de informações sobre o sistema, não fornecendo assim, informações detalhadas a um usuário não autorizado. O procedimento de log-on eficiente deve :

a. ocultar senhas que estão sendo digitadas;

b. não transmitir senhas com textos claros;

c. mostrar um aviso que o computador só pode ser acessado por pessoas autorizadas;

d. não mostrar mensagens que possam auxiliar um usuário não autorizado;

e. validar informações de entrada somente quando todos os dados tiverem sido fornecidos e caso ocorra um erro, não indicar qual parte do dado de entrada está incorreto;

f. limitar o número de tentativas de log-on sem sucesso (três tentativas no máximo é o recomendado). O procedimento de log-on deverá:

   i. registrar as tentativas com sucesso e as inválidas;

   ii. estipular um tempo de espera antes de permitir nova tentativa de log-on ou rejeitar qualquer tentativa posterior sem autorização específica;

   iii. encerrar a conexão com o computador;

   iv. enviar alerta para o console do sistema no caso de exceder o número de tentativas permitido;

g. limitar o tempo máximo para o procedimento de log-on, encerrando o procedimento caso o limite seja excedido;

h. quando o procedimento de log-on for completado com sucesso, mostrar informações de data e hora do último log-on com sucesso, além de detalhes de tentativas inválidas.

11.5.2 – IDENTIFICAÇÃO E AUTENTICAÇÃO DE USUÁRIO

A norma recomenda que a identificação de usuário seja única e de uso exclusivo. Esta identificação permite o controle de ações de usuários através de logs de acesso.

Os procedimentos de identificação e autenticação de usuários descritas no item 11.2.1 podem ser aplicados no presente item para os acessos a sistemas operacionais.

O uso de senhas conforme descrito nos itens 11.3.1 e 11.5.3, são métodos aplicáveis de identificação e autenticação de usuários.

11.5.3 – SISTEMAS DE GERENCIAMENTO DE SENHA

Além dos procedimentos para uso de senhas propostos no item 11.3.1, algumas outras práticas garantem um eficaz gerenciamento de senhas:

a. permita que usuários escolham e modifiquem sua própria senha;
b. obrigue troca de senhas temporárias no primeiro acesso;
c. mantenha o registro de senhas anteriores utilizadas, a fim de bloquear sua reutilização;
d. não mostre senhas na tela, ocultando-as quando da digitação;
e. armazene os arquivos de senhas separados dos dados do sistema de aplicação;
f. armazene e transmita senhas de forma segura.

11.5.4 – USO DE UTILITÁRIOS DE SISTEMAS

A maioria dos sistemas operacionais possui programas utilitários capazes de sobrepor os controles dos sistemas e aplicações. Por isso o uso dos mesmos deve ser restrito e controlado, através de procedimentos de identificação, autenticação e autorização para utilitários de sistema. Assim, considere:

a. a separação dos utilitários do sistema das aplicações;
b. permissão do mínimo possível de usuários de utilitários;
c. autorização para o uso de utilitários de sistemas não previstos;
d. o registro de todo o uso de utilitários de sistemas;
e. remover ou desabilitar os utilitários de sistema desnecessários;

11.5.5 DESCONEXÃO DE TERMINAL POR INATIVIDADE

É comum que fiquemos um bom tempo sem executar nenhuma operação em um terminal. É comum ainda que nos afastemos do terminal deixando para traz várias sessões abertas. Por mais que sejamos orientados a evitar esse tipo distração, ainda estamos sujeitos a ela.

Para evitar que outras pessoas tenham acesso ao nosso terminal quando não estamos por perto, ou mesmo distraídos, devem ser implementadas medidas de desconexão de terminais, concomitante com a limpeza automática de tela depois de decorrido um período definido que reflita a segurança da área.

11.5.6 – LIMITAÇÃO DE HORÁRIO DE CONEXÃO

Os usuários de uma organização normalmente têm horários determinados para o trabalho. A fim de prover uma segurança adicional para aplicações, é recomendável implementar restrições de acesso de horários de conexão, que reflitam a necessidade de uso de cada usuário ou recurso.

Assim, ao conceder acesso aos usuários, é importante que a concessão restrinja o horário de acesso apenas ao turno de trabalho do usuário. Acessos extras poderão ser concedidos mediante solicitação específica, quando necessário.

Também deve ser considerada a duração de sessões ativas a fim de evitar que os usuários mantenham sessões abertas.

Aplicações computacionais de alto risco devem ter horários de conexão definidos, em especial aquelas com terminais em locais públicos ou externos.

11.6 – CONTROLE DE ACESSO À APLICAÇÃO E À INFORMAÇÃO

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

Obtido através de:

- Restrição de acesso à informação usando:
  - . Menus de acesso;
  - . Controle de direito de acesso (leitura, modificação, exclusão);
  - . Controle de dados de saída.
- Isolamento de sistemas sensíveis com criação de ambiente dedicado para estes.

Para prevenir acesso não autorizado à informação contida nos sistemas de aplicação, recursos de segurança da informação devem ser utilizados para restringir o acesso apenas a usuários autorizados, através de controles específicos.

11.6.1 – RESTRIÇÃO DE ACESSO À INFORMAÇÃO

Para suportar os requisitos de restrição de acesso, devem ser seguidas as diretrizes listadas no item 11.1, além de:

a. usar menus para controlar os acessos apenas àqueles aplicativos estritamente necessários;

b. controlar os direitos de acessos dos usuários (somente leitura, direito de escrever, excluir e executar);

c. garantir que as saídas dos sistemas de aplicações que tratam informações sensíveis contenham apenas informações pertinentes e que sejam encaminhadas para terminais e locais autorizados. Informações desnecessárias devem ser removidas.

11.6.2 – ISOLAMENTO DE SISTEMAS SENSÍVEIS

Sistemas sensíveis devem ser isolados de outros sistemas para fins de segurança de acesso. Determinar a sensibilidade de um sistema de aplicação é função do proprietário da aplicação, que deverá identificar e documentar o grau de sensibilidade da mesma.

Se o sistema sensível é executado em ambiente compartilhado, convém que sejam identificados os sistemas com os quais ele irá compartilhar recursos e os riscos inerentes.

11.7 – COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

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

Proteção de recursos da computação móvel:	Proteção de recursos da computação remota:
- Proteção física; - Controles de acesso; - Criptografia; - Cópias de segurança; - Proteção contra vírus.	- Segurança física do local; - Segurança de meios de comunicação; - Cuidados com acessos dos dados por outras pessoas - Direitos de propriedade; - Proteção contra vírus.

A computação móvel e o trabalho remoto trazem enormes benefícios para a organização, proporcionando mobilidade aos funcionários e agilidade nas atividades. Porém, também traz riscos associados ao trabalho em um ambiente desprotegido. Implementar medidas de segurança específicas poderão garantir a proteção adequada para esse tipo de acesso.

11.7.1 – COMPUTAÇÃO E COMUNICAÇÃO MÓVEL

Dispositivos de computação móvel (notebooks, palmtops, cartões inteligentes e telefones celulares), podem carregar informações sensíveis que devem ser protegidas adequadamente, através de políticas para o uso de computação móvel.

A política de computação móvel deve incluir:

a. requisitos de proteção física;
b. controle de acesso;
c. criptografia de dados;
d. cópias de segurança feitas regularmente;
e. proteção contra vírus;

f. recomendações de conexões à rede;

g. diretrizes sobre o uso de dispositivos móveis em locais públicos, evitando que as informações sejam captadas por pessoas não autorizadas;

h. atualização de procedimentos contra softwares maliciosos;

i. controle de acesso remoto, através de redes públicas, usando dispositivos móveis (obtido apenas após o sucesso da identificação e autenticação do usuário);

j. seguros dos dispositivos móveis;

k. orientação para que dispositivos móveis não sejam deixados sem observação;

l. proteção física dos dispositivos;

m. conscientização dos usuários de computação móvel sobre os riscos desta forma de trabalho e dos controles que devem ser implementados.

11.7.2 – TRABALHO REMOTO

O trabalho remoto agiliza a produtividade da organização. A execução desta atividade deve ser autorizada apenas depois que forem implementados controles de segurança, que evitem roubos e/ou perdas acidentais de equipamentos e informações.

Os seguintes pontos devem ser considerados para a proteção de trabalhos remotos:

a. segurança física do local de trabalho remoto;

b. segurança nos meios de comunicação que proporcionarão os acessos remotos aos sistemas internos da organização;

c. ameaças de acesso não autorizado à informação ou aos recursos por outras pessoas;

d. procedimentos para evitar disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular;

e. acordos de licenciamento de softwares que podem tornar as organizações responsáveis pelo licenciamento de softwar cliente em estações de trabalho de propriedade de funcionários;

f. requisitos de proteção contra vírus e requisitos de firewall.

Quanto à infra-estrutura do local de trabalho remoto, cabe considerar:

a. provisão de mobília para o local de trabalho remoto, restringindo seu uso a objetos da empresa;
b. definição do trabalho permitido, período de trabalho, tipo de informação que será tratada e os sistemas e serviços que o usuário terá acesso;
c. provisão de equipamentos de comunicação adequados, com métodos de acesso seguro;
d. segurança física;
e. restrições através de regras para o acesso de familiares e visitantes aos equipamentos e informações;
f. procedimentos de cópias de segurança e continuidade do negócio;
g. auditoria e monitoramento de segurança;
h. recolhimento de equipamentos e revogação de direitos de acesso quando o trabalho remoto cessar.

Normas técnicas

[1] ISO/IEC 13335-1 - Information technology - Guidelines for the management of IT Security - Part 1: Managing and Planning IT Security. ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).

[2] Silvio Aparecido Crepaldi – Auditoria Contábil – Teoria e Prática – Editora Atlas.

[3] Marcio Araújo - Governança em Tecnologia da Informação – Artigo Publicado em 05/04/2005 - www.issabrasil.org/artigos_0021.asp.

[4] GIOSA, Lívio Antonio. Terceirização: Uma Abordagem Estratégica. São Paulo: Editora Pioneira, 1997.

[5] Kleber Figueiredo. Gestão da Capacidade e da Demanda em Serviços Logísticos. Artigo publicado em http://www.cel.coppead.ufrj.br/fs-busca.htm?fr-gestao.htm - 2001.

[6] Reginald Tomas Yu-Lee - Essentials of Capaclty Mangement – Wiley Publishers – 2002.

[7] http://www.cic.unb.br/docentes/jhcf/MyBooks/ciber/doc-ppt-html/CodigoMovel.html.

[8] Apostila Módulo e-security – Segurança da Informação – Leonardo Soares Figueiredo – 2001 – DCC-UFMG.

[9] Segurança de Redes – Thomas ª Wadlow – Editora Campus – 2000.

[10] Entrevista de Marcello Rachlyn, diretor de operações da EuroSign Certificadora Digital, a câmara Brasileira de Comércio Eletrônico – 03/05/2006, obtida em http://www.camara-e.net/interna.asp?mostra=0&tipo=1&valor=3654.

[11] Segurança de redes – Thomas ª Wadlow – Editora campus – 2000.

[12] Elementos chaves da rede de auto defesa da Cisco – Estratégia de rede – Informe oficial Cisco