Entendendo e implementando a Norma NBR ISO/IEC 17799

Academia Latino-Americana de Segurança da Informação

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

Módulo 2

Entendendo e implementando a Norma NBR ISO/IEC 17799

AUTORES

Edison Fontes
Fernando Sérgio Santos Fonseca
Sérgio Toscano Dias Pereira

Apostila desenvolvida pelo Instituto Online em parceria com a Microsoft Informática

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

Revisão 1.0 – Abril de 2006

COORDENADORES TÉCNICOS

Arthur Roberto dos Santos Júnior
Fernando Sergio Santos Fonseca
Paulo Eustáquio Soares Coelho

COMO USAR ESSE MATERIAL

Este é um material de apoio para o curso Entendendo e implementando a NBR ISO/IEC 17799 ministrado pela Academia Latino-americana de Segurança da Informação. 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 seu roteiro está especificado sob o título.

VÍDEO

Indica que será apresentado um filme para ilustrar as práticas ou conceitos

ÍNDICE

Capitulo

7

7 – GESTÃO DE ATIVOS

POR FERNANDO FONSECA

NESTE CAPÍTULO, ESTUDAREMOS COMO EFETUAR A GERÊNCIA DOS ATIVOS DE INFORMAÇÃO, DISCUTIREMOS COMO PROTEGÊ-LOS IDENTIFICANDO SEUS PROPRIETÁRIOS, CLASSIFICANDO-OS E MANTENDO O CONTROLE SOBRE OS MESMOS.

OBJETIVOS

Os ativos de uma organização, são os bens móveis, imóveis e até mesmos intangíveis, como a informação armazenada em meios diversos.

Este capítulo aborda as responsabilidades pelos ativos, como inventariá-los, classificá-los e como rotular a informação.

Ao final deste capítulo você estará apto a:

- ❒ Entender o que são os ativos de informação;
- ❒ Porque eleger um responsável pelos ativos;
- ❒ Como classificar a informação;
- ❒ Como rotular a informação de forma segura.

7.1 – RESPONSABILIDADE PELOS ATIVOS

Ativos:

. Informações (dados, manuais, projetos, etc…)

. Equipamentos

. Softwares

. Serviços

. Reputação e imagem da organização

. Pessoas e suas qualificações

As informações (base de dados, manuais, software, etc) de uma organização podem ser identificadas como um ativo como tantos outros tradicionais (imóveis, móveis, equipamentos, etc...). Assim, ele possui um valor e deve ser classificado e valorado.

Existem vários tipos de ativos:

- Ativos de informação: base de dados de contratos e acordos, documentação de sistema e infra-estrutura, manuais, material de treinamento, procedimentos de suporte e operação, planos de continuidade de negócio, etc...;
- Ativos de softwares: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- Ativos físicos: equipamentos computacionais, de comunicação, mídias removíveis;
- Serviços: serviços de computação, comunicações, refrigeração, iluminação, eletricidade;
- Pessoas e suas qualificações, habilidades e experiências;
- Ativos intangíveis: reputação, credibilidade e imagem da organização.

Para que os ativos sejam protegidos, é necessário que possua um proprietário. O proprietário pode ser uma pessoa ou entidade autorizada à controlar o uso e a segurança dos ativos, tornando-se o responsável pelos mesmos.

7.1.1 – INVENTÁRIO DOS ATIVOS

Objetivo: procura classificar os ativos de informação, de acordo com sua importância para o negócio em si.

Algumas ferramentas para levantamento e controle dos ativos:

- ***Sistemas de gerenciamento de redes***
- ***Sistemas de inventários de computadores***
- ***Sistemas operacionais de rede***
- ***Ferramentas de gerência de documentos***
- ***Sistemas de controle de backup***
- ***Ferramentas de gestão empresarial***

O ponto inicial para a gestão dos ativos é a identificação do que é um ativo e quais são eles dentro de nossa organização. Para se ter um levantamento mais fidedigno, podemos agrupá-los por área e solicitar que a alta direção nomeie um gestor (proprietário) da informação.

Cada área deve realizar um levantamento, ou inventário, destes ativos. Para o sucesso desta etapa torna-se importante que os gestores sejam instruídos quanto aos tipos de ativos e como classificá-los, para manter um controle de seu estado e numa segunda etapa conceder as permissões de acesso adequadas a cada um.

Pelo dicionário Aurélio o termo inventário significa "***Lista discriminada, registro, relação, rol de mercadorias, bens, etc***...".

Quando se fala em inventário, o termo lembra os longos períodos de levantamento de itens em um estoque físico e o confronto com o estoque registrado no sistema (ou o lendário fichário "carbex", para quem está a mais tempo no mercado ou não acredita nessa tal de informática). Essa analogia explica em linhas gerais o que é um inventário, mas olhando pelo lado de ativos, o inventário vai além do estoque e procura classificar os ativos de informação, de acordo com sua importância para o

negócio em si.

Existem diversas ferramentas que nos auxiliam no levantamento e controle dos ativos. A seguir destacamos algumas:

- ***Sistemas de gerenciamento de redes***: Estes sistemas podem monitorar a existência e o estado de ativos da rede como servidores, switches, roteadores, etc. Existem implementações proprietárias e um protocolo padrão específico para realizar esta tarefa chamada SNMP (Simple Network Manager Protocol). Com o SNMP é possível criar quantos controles forem necessários, além dos básicos (uso de CPU, espaço em disco, etc).
- ***Sistemas de inventários de computadores***: Realizam um levantamento de todos os computadores conectados à rede com uma relação de software e hardware existentes nesses equipamentos.. Estes sistemas são úteis para se identificar qual o parque da empresa e quais ativos (softwares licenciados ou gratuitos) e passivos (softwares comerciais sem a devida licença) estão instalados nestes computadores. Estes softwares também são úteis para avisar ao administrador quando houver alguma alteração nos dados de inventário.
- ***Sistemas operacionais de rede***: Os sistemas operacionais de rede possuem DACL's (Discretionary Access Control Lists) que através de um banco de dados central de contas de usuários fornece acesso aos seus recursos (ativos de informação) somente a quem efetivamente necessita deste acesso.
- ***Ferramentas de gerência de documentos***: Estas ferramentas servem como uma camada adicional de proteção dos documentos limitando as ações que os usuários autorizados podem realizar com os ativos de informação (Ex: Pode ler, mas não imprimir). Além de limitar o acesso estas ferramentas podem também manter um registro das ações realizadas por cada usuário e das tentativas de executar ações não permitidas.
- ***Sistemas de controle de backup***: O Backup é uma cópia fiel de seus ativos de informação mais importantes. Por este motivo é desejável que se controle exatamente o que acontece com cada uma das mídias destinadas a este fim. Existem várias ferramentas capazes de controlá-las assim como seu uso e as informações contidas em cada uma delas.
- ***Ferramentas de gestão empresarial***: Estas ferramentas controlam toda a gestão da empresa. Uma boa ferramenta deste tipo é capaz de separar os proprietários para cada processo dentro da empresa.

7.1.2 - PROPRIETÁRIO (GESTOR) DOS ATIVOS

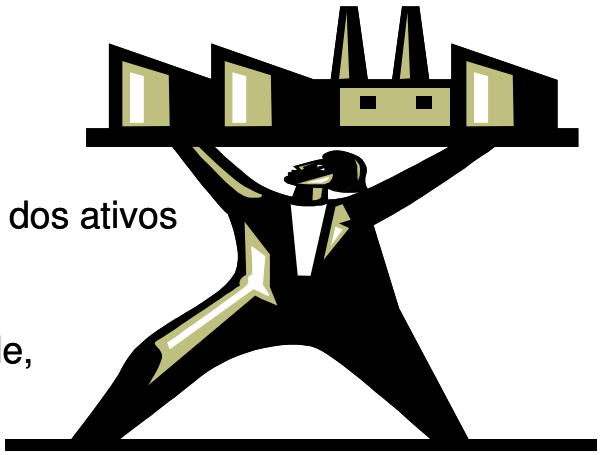
Responsável por:

. Responder pelo ativo

. Cuidar da manutenção dos ativos

. Classificá-lo quanto a:

- Confidencialidade,
- Integridade e
- Disponibilidade

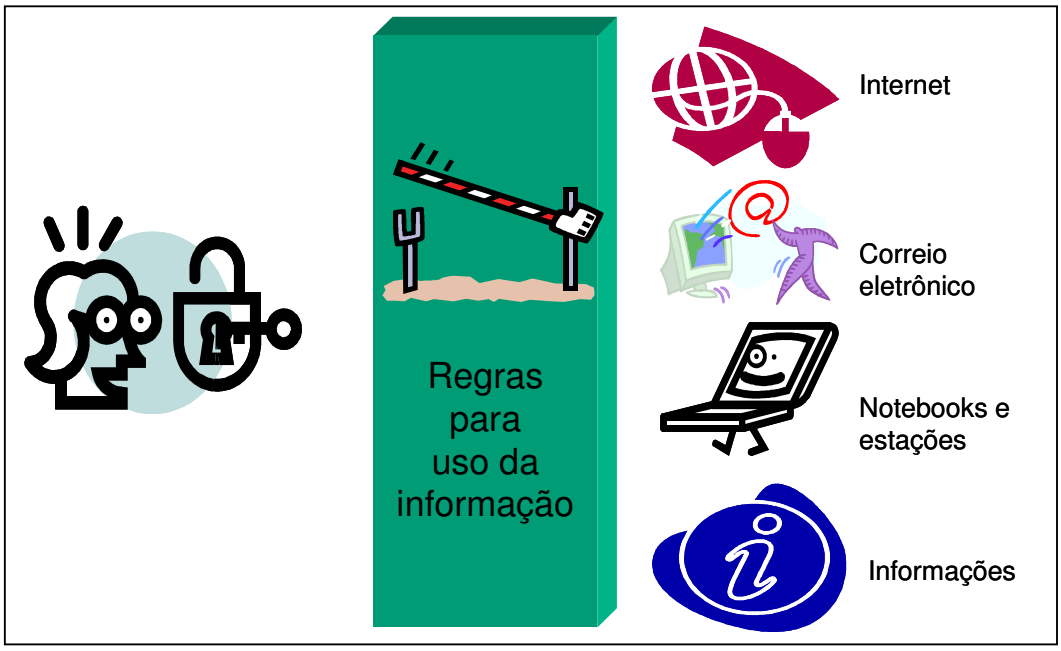


Para que se tenha um controle efetivo dos ativos é essencial que cada ativo de informação dentro de uma organização possua uma pessoa responsável, essa pessoa é denominada “proprietário” do ativo.

Apesar de a palavra proprietário expressar posse, o proprietário é apenas uma pessoa designada pela empresa para responder pelo ativo e classificá-lo quanto à sua necessidade de confidencialidade, integridade e disponibilidade. Por estes motivos muitos autores preferem chamá-lo de gestor do ativo. A utilização do termo “gestor” ao invés do termo “proprietário” pode evitar futuros problemas de interpretação. Sendo assim, este autor recomenda o uso do termo gestor da informação.

Os proprietários são os responsáveis por cuidar da manutenção dos ativos, e mesmo que parte deste processo seja delegada pelo proprietário a um terceiro, ele ainda continua sendo o responsável primário pela proteção adequada dos ativos.

7.1.3 – USO ACEITÁVEL DOS ATIVOS

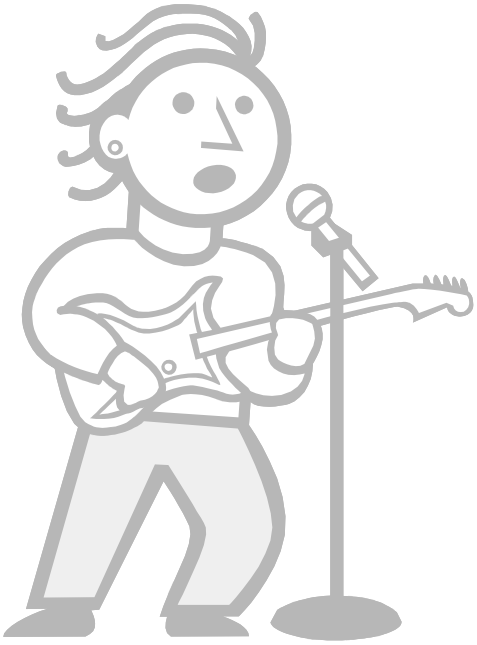


Além de proprietário, os ativos da empresa possuem usuários. É importante que sejam criadas regras que irão compor a política da empresa quanto a permissões de uso das informações e de ativos associados aos recursos de processamento das informações. Cada usuário deve conhecer e cumprir essa política para uso dos recursos, a fim de não comprometer a empresa e ao próprio usuário. Exemplos de ativos que necessitam de cuidados especiais quanto ao seu uso são:

- ***Internet***: Dentro de uma organização os usuários utilizam um sistema que está registrado para uso da mesma. Qualquer ato realizado em qualquer computador dentro da empresa é informado como proveniente do endereço IP destinado para o para uso dessa empresa. É importante que se especifique e divulgue a todos os usuários quais os tipos de acesso são permitidos ou proibidos, de acordo com a lei e com a política de segurança corporativa, além de manter o registro adequado de todas as comunicações oriundas da empresa.

- ***Correio eletrônico***: O correio eletrônico é uma ferramenta de comunicação que identifica o funcionário e a empresa perante o mundo como um nome e sobrenome separados pelo @ (leia-se “at” que no inglês significa “em”) Esta ferramenta deve ser utilizada somente para uso profissional e nunca, em hipótese alguma, deverá ser utilizada em alguma ação suspeita, ou isso poderá acarretar em comprometimento do usuário assim como da empresa, pois essa é a provedora do recurso que possibilita a comunicação com a Internet. Existem ferramentas para monitorar conteúdo impróprio em correio eletrônico, mas o indispensável é que todos os usuários evidenciem de que conhecem a política da empresa em relação ao uso de seus recursos, no processo de integração ou de solicitação de acesso.
- ***Estações de trabalho***: A estação de trabalho do usuário, assim como sua mesa ou cadeira pertence exclusivamente à empresa e deve ser tratado como um recurso precioso, sujeito à política corporativa e às normas estabelecidas para seu uso. O mau uso de estações de trabalho podem impactar na produtividade do usuário, na manutenção da confidencialidade dos dados por ele manipulados e na adequação da empresa às leis de direitos autorais dentre outros problemas.
- ***Notebooks***: Os dispositivos móveis circulam livremente dentro e fora do perímetro da empresa. É necessário nesse caso que a política seja bem definida quanto ao uso desses equipamentos e que esta seja bem divulgada e conhecida por todos os usuários de dispositivos móveis. Sempre que possível esta política deve ser reforçada por recursos de tecnologia uma vez que seu mau uso pode trazer ameaças a esses dispositivos e à outros ativos quando este retornar para dentro do perímetro de proteção da empresa.

7.2– CLASSIFICAÇÃO DA INFORMAÇÃO



"Quantos segredos que você guardava, hoje são bobos ninguém quer saber"

"A Lista",

Oswaldo Montenegro

Um dos maiores desafios da segurança da informação é a necessidade de termos a informação íntegra, correta e ao mesmo tempo disponível somente para os usuários que realmente devem acessá-la. Não haveria muita dificuldade em se proteger uma informação se ela não precisasse estar disponível para os usuários legítimos.

Uma vez que garantimos que a informação está disponível somente para os usuários corretos, é necessário garantir que eles façam o uso adequado dessas informações. Para alcançar este objetivo é necessário que um processo eficiente de classificação da informação seja estabelecido, garantindo que os usuários desses ativos conheçam a sua real importância para a corporação.

Outro aspecto relevante da informação é que ela não mantém o mesmo valor ao longo do tempo. Algumas tendem a se tornarem públicas ou simplesmente não interessar a mais ninguém.

7.2.1 – RECOMENDAÇÕES PARA CLASSIFICAÇÃO DA INFORMAÇÃO

. Identifique quem é o proprietário da informação;

. Especifique quais critérios serão utilizados para sua classificação;

. Converse com o proprietário da informação — esta deve ser enquadrada em alguma das categorias estipuladas;

. Indique qual o nível de segurança necessário para proteger cada categoria;

. Documente exceções;

. Crie rótulos para a informação impressa e digital;

. Defina o método que será utilizado para transferir a custódia da informação;

. Indique um procedimento para a desclassificação da informação;

. Treine e conscientize os usuários.

Cada informação dentro da empresa possui a necessidade de estar disponível para uma pessoa ou equipe, ao mesmo tempo em que há a necessidade de um controle que garanta que ela estará realmente disponível para os usuários legítimos. A classificação deve levar em conta estas premissas e principalmente o impacto nos negócios pela quebra na disponibilidade, integridade ou confidencialidade das mesmas.

Para alcançarmos este objetivo de forma eficaz é necessário definir categorias de informações que sejam bem objetivas quanto à criticidade de cada informação. Esta classificação deve ser feita pelo proprietário (gestor) de cada uma delas, em um momento inicial e posteriormente em prazos pré-definidos, onde uma informação pode ser reclassificada de acordo com os requisitos de confidencialidade que ainda representa para a organização.

Alguns ativos de informação perdem totalmente o valor depois de um determinado evento. O vencedor de um Oscar, por exemplo, passa de um dos segredos mais bem guardados do mundo para uma informação de domínio público em questão de horas. Esta informação já poderia ser classificada originalmente como “Top Secret” até a noite da entrega e “Unclassified” após esta data.

Para uma eficiente classificação da informação, a empresa necessita identificar o gestor do ativo, responsável por definir a classificação do mesmo. Uma empresa pode conduzir este processo conforme os critérios como os da lista abaixo [1]:

- Identifique quem é o proprietário da informação;
- Especifique quais critérios serão utilizados para sua classificação;
- Converse com o proprietário da informação — esta deve ser enquadrada em alguma das categorias estipuladas;
- Indique qual o nível de segurança necessário para proteger cada categoria;
- Documente exceções;
- Crie rótulos para a informação impressa e digital;
- Defina o método que será utilizado para transferir a custódia da informação;
- Indique um procedimento para a desclassificação da informação;
- Treine e conscientize os usuários – é importante que todos saibam como classificar e manusear diferentes tipos de informação.

7.2.2 – RÓTULOS E TRATAMENTO DA INFORMAÇÃO

. Sensíveis

. Confidenciais

. Privadas

. Proprietárias

. Públicas

Requisitos de Confidencialidade

Conforme visto anteriormente, os proprietários dos ativos são os responsáveis por atribuir as permissões de acesso aos ativos e revisá-las periodicamente para assegurar-se que o controle mais apropriado seja aplicado àquela informação. Esta classificação deve garantir que o princípio do mínimo privilégio (least privilege) seja aplicado, ou seja, cada usuário somente terá acesso ao que realmente necessita e as permissões conferidas a este serão somente as necessárias para a execução de sua tarefa relacionada àquela informação.

A classificação dos ativos deve ser clara e objetiva, estando presente em todas as informações, independente de seu meio de armazenamento. Os documentos eletrônicos confidenciais, por exemplo, devem conter dispositivos como mensagens de rodapé que garantam que a classificação da informação sobreviverá à passagem de seu conteúdo do meio digital para o meio físico impresso.

Cabe a cada empresa analisar quantos e quais níveis de classificação deverão ser utilizados para classificar seus ativos de informação quanto à sua confidencialidade,não existindo uma forma única definida para tal. Uma vez definidos estes níveis, deve haver procedimentos para tratamento e manuseio das informações associados a cada nível de classificação criado pela organização.

Na tabela 1 vemos alguns exemplos de classificação de ativos.

Decreto Federal 4.553/2002 para administração pública	Classificação da informação comercial	Classificação Militar
Ultra-secretos: Informações cujo conhecimento possa acarretar em dano excepcionalmente grave à segurança nacional	**Confidencial**: Se for revelada pode afetar seriamente a empresa. .	Ultra secretos (Top Secret)
Secretos: Informações cujo conhecimento possa acarretar em dano grave à segurança nacional.	**Privada**: Informação sobre o corpo funcional.	**Secreto (secret)**
Confidenciais: Aquele cuja revelação pode frustrar seus objetivos ou causar dano à segurança da sociedade e ao estado	**Sensível**: Requer precauções especiais	**Confidencial (Confidential)**
Reservados: Aquele cuja revelação pode frustrar seus objetivos ou causar dano à segurança da sociedade e ao estado.	**Proprietária**: se revelada, pode reduzir a margem competitiva.	Sensível mas não Classificada (Sensitive but unclassified)
	Pública: se revelada não afetará a organização.	Não classificada (Unclassified)

Requisitos de Integridade

Uma outra classificação que se deve fazer dos ativos é quanto à sua integridade. As necessidades de integridade podem ter vários níveis (baixo, médio, alto, crítico, etc), de acordo com a necessidade da empresa.

Requisitos de Disponibilidade

Pela ótica da disponibilidade, a classificação da informação acontece de acordo com a extensão do impacto que sua falta ocasionará para a organização. Novamente não temos categorias pré-definidas, mas podemos classificar por intervalo de tempo (minutos, horas ou dias) ou por categorias que correspondam a estes intervalos (curto, médio, longo). Estes critérios podem definir também o tempo de retenção de uma determinada informação, muitas vezes estabelecido por clausulas legais.

Capítulo

8

8 – SEGURANÇA EM RECURSOS HUMANOS

POR EDISON FONTES

TRATAREMOS NESTE CAPÍTULO SOBRE OS ASPECTOS HUMANOS DA SEGURANÇA DA INFORMAÇÃO. QUAIS OS CUIDADOS NA CONTRATAÇÃO E DEMISSÃO DE PESSOAL, NO QUE TANGE À SEGURANÇA DA INFORMAÇÃO QUAIS AS RESPONSABILIDADES DE CADA FUNCIONÁRIO E DE TERCEIROS PARA COM A SEGURANÇA DA INFORMAÇÃO

OBJETIVOS

A implantação da segurança depende mais das pessoas que a conduzem do que dos recursos utilizados. Não basta que se utilizem as melhores ferramentas, sem que os usuários estejam comprometidos com a segurança da informação.

Este capítulo aborda a segurança em recursos humanos. Ao final deste capítulo você estará apto a:

- ❒ Selecionar candidatos para contratação avaliando suas características e alinhamento com regras pré-definidas;
- ❒ Conscientizar o profissional contratado sobre suas responsabilidades quanto à política de segurança da informação;
- ❒ Conduzir o processo de encerramento ou mudança de contratação.

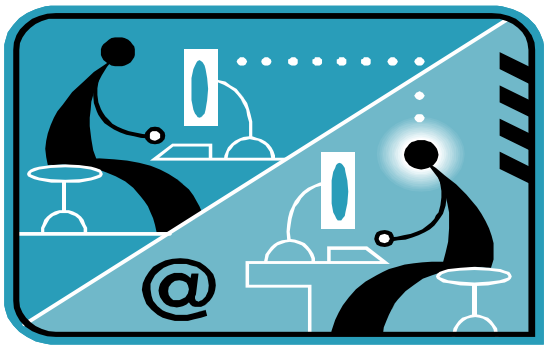
8.0 – SEGURANÇA EM RECURSOS HUMANOS

Leva em conta os usuários em três momentos:

. Antes da contratação

. Durante a execução das funções

. No encerramento da atividade profissional



O processo de segurança da informação deve contemplar a pessoa humana que é o recurso que faz efetivamente acontecer a proteção. Segundo Edison Fontes [2] "... a implementação de regras, regulamentos, políticas, normas, bem como o uso de programas de proteção da informação, são ações importantes. No entanto, são partes da solução. Essas ações conseguem construir apenas metade da ponte que nos leva à efetiva proteção. A parte restante, crucial, para que a ponte cumpra o seu objetivo é construída quando as pessoas da organização (funcionários, prestadores de serviço, executivos e acionistas) tornam-se conscientes desse assunto." Também complementa [3] "Neste processo de segurança, a atitude de cada pessoa é fundamental. De certa forma, o sucesso da implantação da segurança depende da pessoa humana. Podemos ter os melhores esquemas e ferramentas, mas se não tivermos cada pessoa comprometida com a segurança da informação, a possibilidade de fracasso aumenta."

Desta forma é necessário que consideremos os usuários (funcionários, fornecedores e terceiros) em três momentos de sua vida profissional na organização: antes da contratação, durante a execução das suas funções profissionais e quando do encerramento de suas atividades profissionais para a organização. Para esta última fase devemos considerar também situações de mudança de tipo de atividade que exigirá diferentes acessos à informação.

8.1 – ANTES DA CONTRATAÇÃO

. Explique ao candidato sua função profissional e o papel que irá desempenhar.

. Defina em documento, as responsabilidades do cargo e suas características.

. Avalie se o candidato está alinhado com as regras.

Cada função profissional deve ter suas responsabilidades explicitamente definidas e de conhecimento das pessoas que vão exercer um cargo na organização. Antes da contratação o candidato deve entender sua função profissional e concordar com o papel que vai desempenhar. As responsabilidades do cargo e suas características devem estar definidas em um documento que descreve as condições de contratação.

Todo candidato a exercer uma atividade profissional na organização deve ser analisado em relação à sua capacidade de exercê-la, inclusive considerando: características pessoais, alinhamento às regras, exercício da responsabilidade, experiência profissional, tratamento adequado de informações de diferentes níveis de confidencialidade e concordância com a política de segurança da organização.

8.1.1 – PAPÉIS E RESPONSABILIDADES

Crie descrição de função, incluindo:

. Exigências a seguir quanto a política de segurança;

. Requisitos de proteção de ativos;

. Executar tarefas de segurança da informação;

. Responsabilidades por relatar situações de risco.

Na descrição da função profissional, as responsabilidades relativas à segurança da informação devem incluir exigências de seguir a política de segurança, proteger ativos, executar as orientações e relatar situações de riscos.

8.1.2 – SELEÇÃO

Deve-se levar em consideração os aspectos relativos a:

. Privacidade;

. Legislação;

. Proteção de dados pessoais;

. Referências pessoais e profissionais;

. Exatidão de informações fornecidas;

. Verificações de ordem financeira e criminal.

Quando da seleção da pessoa deve-se considerar que todas as verificações obedeçam às leis vigentes, as regulamentações e os princípio éticos. Essas verificações devem considerar o respeito à privacidade aos dados pessoais de quem será contratado.

Em relação à análise das informações prestadas pelo candidato, devemos verificar;

a. Se as informações da experiência profissional estão adequadas ao cargo/função;
b. Se as informações prestadas são verdadeiras: dados acadêmicos, documentos de identificação pessoal;
c. A situação de crédito na praça e registros criminais.

A seleção deve ser feita por profissionais qualificados, sejam da própria organização ou sejam prestadores de serviço. Quando feito por terceiros é importante que exista um contrato para essa prestação, que descreva a responsabilidade desse prestador em relação ao profissional que ele está selecionando para a organização.

As responsabilidades e ações em relação à segurança da informação devem estar destacadas na descrição das responsabilidades de cada função profissional.

É importante que a pessoa formalize o conhecimento dessas regras assinando um documento.

Algumas dessas responsabilidades devem continuar um certo tempo após o término de relação profissional entre a organização e a pessoa.

Algumas empresas se resguardam juridicamente solicitando que o candidato autorize formalmente que uma verificação dos dados apresentados seja conduzida para a continuidade do processo de seleção.

8.1.3 – TERMOS E CONDIÇÕES DE CONTRATAÇÃO

Devem refletir a política de segurança, esclarecendo e declarando a funcionários, fornecedores e outros usuários:

. Assinatura de termo de confidencialidade;

. Responsabilidades legais e direitos;

. Responsabilidades pela classificação da informação e pelo gerenciamento de ativos;

. Responsabilidade pelo tratamento da informação recebida;

. Responsabilidades fora da organização;

. Acões em caso de desrespeito aos requisitos de segurança.

A existência de um Código de Conduta ou Código de Ética facilita o entendimento e esclarecimento de vários aspectos relativos à segurança da informação bem como explícita mais ainda como é a filosofia da organização para o tratamento de seus recursos. O objetivo é que as pessoas que estejam na organização saibam claramente as regras da mesma, a responsabilidade de cada função e possa de maneira consciente ser um profissional na organização, desde que esteja de acordo com todo esse ambiente de controle.

8.2– DURANTE A CONTRATAÇÃO

Deve ser observado:

. Responsabilidades da direção;

. Conscientização, educação e treinamento em segurança da informação;

. Processo disciplinar

Durante o exercício das funções profissionais para a organização, precisamos garantir que a pessoa:

- Esteja consciente dos controles necessários para a manutenção do nível adequado de segurança;
- Saiba quais são suas responsabilidades;
- Apóie a política de segurança e demais regulamentos.

Isto é, a pessoa precisa estar conscientizada em segurança da informação.

8.2.1 – RESPONSABILIDADE DA DIREÇÃO

A direção da empresa deve estar engajada no processo de segurança da informação e deve solicitar aos funcionários e parceiros que sigam as diretrizes da política de segurança, da informação, assegurando que todos estejam instruídos de suas responsabilidades.

8.2.2 – CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

Como conscientizar, define Edison Fontes [2, XIII] "Defino essa conscientização como sendo mais do que um simples conhecimento: estar conscientizado em proteção da informação é internalizar os conceitos e agir com naturalidade no cumprimento dos regulamentos. Significa que a segurança da informação deve fazer parte do dia-a-dia e não ser considerada um peso em nossas responsabilidades profissionais para com a organização. Significa também que os executivos da organização devem avaliar e estar comprometidos com o nível estabelecido para a proteção."

As pessoas devem ser constantemente:

a. instruídas sobre suas responsabilidades e uso correto quando do acesso à informação;
b. motivadas a cumprir todos os regulamentos de segurança da informação;
c. conscientizadas em relação à segurança da informação;
d. capacitadas para atender os requisitos de segurança exigidos.

Segundo Fontes [2, pág. 131] um dos dez direitos do usuário é: "Receber treinamento adequado sobre os mecanismos de segurança de informação, que devem ser de fácil utilização."

Deve existir um processo de conscientização, educação e treinamento em segurança. da informação. Esse processo deve contemplar todos os usuários e deve ter como conteúdo os conceitos gerais de segurança da informação e as regras específicas da organização.

A conscientização pode variar de ações simples até campanhas de grande porte. O mais importante é que a conscientização e treinamento em segurança da informação sejam atividades periódicas e que existam enquanto existir a organização.

Contar com a participação da área de Recursos Humanos e com especialistas em comunicação (Marketing e Publicidade) é uma ação positiva e que deve ser levada em consideração. O profissional de segurança conhece os conceitos e regras que devem ser comunicadas, porém a forma de como comunicar deve ser definida e executada por profissionais que entendem de comunicação e são responsáveis pelo fator humano dentro da organização.

8.2.3 – PROCESSO DISCIPLINAR

No treinamento e conscientização deve estar especificado que o não cumprimento dos regulamentos acarretará sanções e eventual processo disciplinar. É importante que esse processo disciplinar esteja esclarecido, que seja justo, feito de forma correta e tenha como objetivo principal sempre:

"***Fazer com que a organização através das pessoas que a formam , esteja conscientizada e alcance/mantenha o nível de proteção adequado ao negócio***".

8.3– ENCERRAMENTO OU MUDANÇA DA CONTRATAÇÃO

Ações a serem tomadas para:

. Encerramento de atividades

. Devolução de ativos

. Retirada de direitos de acesso

O processo que acontece quando as pessoas (funcionários, fornecedores e terceiros) deixam a organização ou mudam o tipo de trabalho, deve ser realizado de forma ordenada e controlada. As pessoas relacionadas a esses procedimentos devem estar cientes da suas responsabilidades. O usuário que está saindo da organização ou mudando o seu tipo de trabalho internamente deve conhecer as regras relacionadas à segurança da informação.

8.3.1 – ENCERRAMENTO DE ATIVIDADES

Quando do encerramento do trabalho ou mudança do tipo de atividade o usuário deve perder o acesso aos recursos de informação que não mais precisará acessar. Deve-se ter definido como ficarão as informações da organização que eram utilizadas pelo usuário que está encerrando suas atividades ou mudando de tipo de trabalho. A orientação básica é que o funcionamento do negócio não pode ser impactado.

Quando da situação de mudança, os acessos atuais para a informação, bem como os acessos físicos, devem ser eliminados e os novos acessos devem ser concedidos para o usuário exercer sua nova função, desde que autorizado pelo Gestor da respectiva informação.

Normalmente o processo geral de desligamento é realizado pela área de recursos humanos. Desta forma as questões de segurança da informação devem ser um dos itens desse processo.

8.3.2 – DEVOLUÇÃO DE ATIVOS

É importante que os bens de informação que são de responsabilidade do usuário que está sendo desligado ou transferido, sejam devolvidos e/ou repassados a outras pessoas autorizadas dentro da organização para que o processo de negócio não sofra interrupção.

8.3.3 – RETIRADA DE DIREITOS DE ACESSO

Devemos ter cuidado com a situação real que acontece em várias organizações: o usuário possui várias identificações para o acesso lógico à informação nas diversas plataformas. Nessa situação o corte do acesso deve acontecer em todas as identificações relacionadas ao usuário no momento em que o mesmo tome conhecimento de seu desligamento.

Para que a retirada de direitos seja eficiente, a área de RH deve ser instruída a comunicar o fato com determinada antecedência às áreas envolvidas para que as mesmas tomem as providências necessárias em tempo hábil.

8.4 - CONCLUSÃO

O recurso humano é crítico para que o processo de segurança funcione de forma adequada e que possibilite que a organização tenha um nível de proteção suficiente para o tipo do negócio da organização. Devemos dar atenção a todos os eventos relacionados à pessoa humana. Esse é um aspecto fundamental para alcançarmos o nível de proteção adequado para a organização. Como o Fontes [2, pág. XV] acredita:".. Quando o usuário conhece os motivos da segurança da informação ele segue os procedimentos e as ações para efetivar essa proteção."

Capítulo

9

9 – SEGURANÇA FÍSICA DO AMBIENTE

POR SÉRGIO DIAS

TRATAREMOS NESTE CAPÍTULO SOBRE COMO PROTEGER O AMBIENTE E AS ESTRUTURAS FÍSICAS QUE SUPORTAM A OPERAÇÃO DOS EQUIPAMENTOS.

OBJETIVOS

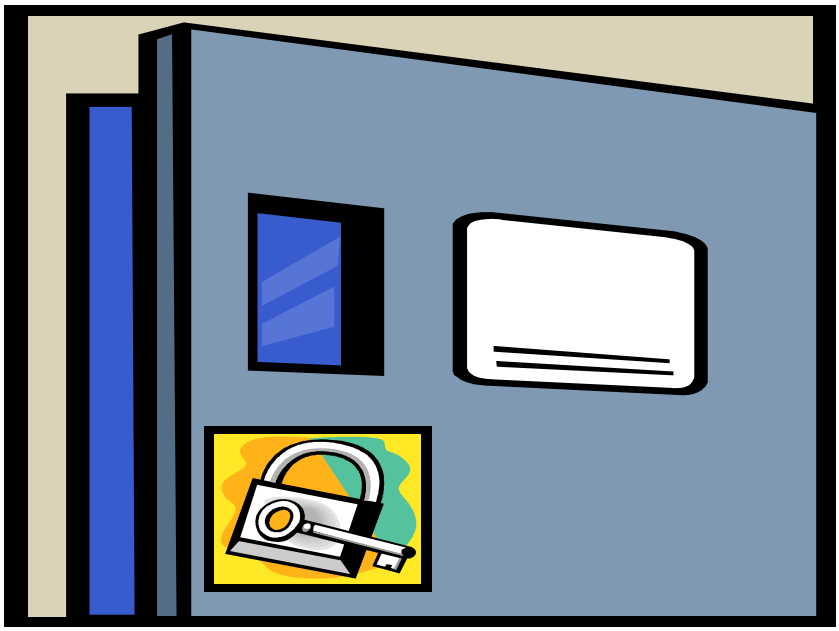
O objetivo de segurança física é o de prover um ambiente seguro para todos os ativos da organização, incluindo atividades envolvendo sistemas de informação.

Ao final deste capítulo você estará apto a:

- ❒ Determinar quais são as ameaças à segurança física da informação;
- ❒ Estabelecer o perímetro de segurança física;
- ❒ Empregar controles de entrada e saída dos ambientes;
- ❒ Estabelecer métodos de segurança dos locais onde ocorrem atividades envolvendo segurança da informação;
- ❒ Proteger o ambiente físico contra ameaças externas e de desastres do meio ambiente;
- ❒ Trabalhar com áreas seguras;
- ❒ Proteção das instalações que garantem a operação dos equipamentos.

9.1 – INTRODUÇÃO A SEGURANÇA FÍSICA

Objetivo: Proteção ao ambiente onde estão os ativos.



Com a evolução da computação, os ativos de informação, que na época dos mainframes estavam centralizados e faziam uso de uma única sala com poucos acessos, se espalharam pela empresa. Nos atuais ambientes distribuídos e de computação móvel, a abrangência e demanda de proteção física do ambiente aumentou significativamente.

A Segurança Física prevê proteção ao ambiente onde estão hospedados os ativos da empresa, utilizando-se de recursos como trancas, guardas, alarmes, câmeras de vigilância, entre outros.

A importância da Segurança Física é que uma vez que ela esteja subjugada, pode-se contornar vários controles de segurança lógicos, concedendo acesso direto ao ativo. Um exemplo disso é que, mesmo com vários controles, como Firewalls, Antivírus, etc. uma pessoa má intencionada pode, através do uso de disquetes, CDs, e atualmente Pen-Drives, reiniciar um servidor com outro sistema operacional e ter acesso irrestrito aos dados.

A Disponibilidade e integridade dos dados são facilmente destruídas caso se ultrapasse os dispositivos de segurança física.

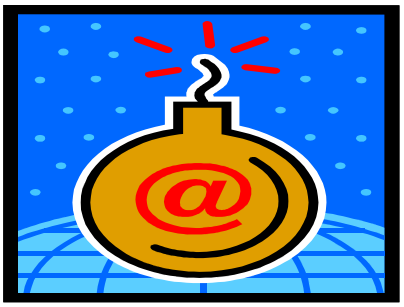
9.1.1 – AMEAÇAS A SEGURANÇA FÍSICA

. Efeitos da natureza

. Falhas em sistemas de suprimento

. Ameaças humanas (sabotagens, armas, etc…)

. Ameaças por motivação política (terrorismo, espionagem industrial)



As seguintes ameaças podem comprometer o ambiente físico das organizações e são objetos dos controles de segurança física:

- ***Naturais e do ambiente***: Estas ameaças são de difícil controle quando ocorrem e não temos como antecipá-las. Exemplos são: tempestades, erupções vulcânicas, furacões, tornados, incêndios e enchentes. No Brasil não temos muitos efeitos naturais como em outros países, mas as chuvas trazendo enchentes e o calor gerando incêndios em nossas matas são preocupações que o profissional de segurança deve estar atento;

- ***Sistemas de suprimento (utilidades)***: Correspondem aos elementos que fazem a operação funcionar e são essenciais em toda a infra-estrutura física. Como exemplo temos: energia, comunicação e encanamento. É importante que a disposição desses elementos esteja protegida, pois existem casos conhecidos de tratores que partiram fibras óticas subterrâneas que ligavam prédios, ou um cano estourar nas instalações que contenham equipamentos elétricos ou mesmo no datacenter. A energia elétrica deve ser sempre mensurada para suportar o ambiente físico e elementos críticos devem ter proteções adicionais como veremos ainda neste módulo.

- ***Humanas***: As diversas pessoas internas ou externas que tenham acesso direto ou indireto aos ativos da empresa com a possibilidade de afetá-los estão

incluídos em ameaças de origem humana. Como exemplo desses tipos de ameaças, temos: sabotagens, armas ou agentes químicos, ataque cracker.

- ***Motivações Políticas***: Muitas vezes uma empresa pode, dependendo de sua posição no mercado, sofrer ameaças de terroristas ou competição acirrada. Isso aumenta com a presença no mercado global, com os produtos que fabrica e com suas posições político-econômicas. Por exemplo, a empresa pode sofrer com ataques a bombas ou espionagem industrial, entre outros.

A melhor forma de identificar nosso grau de exposição às diversas ameaças a segurança física é através da realização de uma análise de riscos.

9.2 – ÁREAS SEGURAS

Chamamos áreas seguras todo o ambiente que suporta os ativos da organização, incluindo o Datacenter. É importante que o profissional de segurança da informação defina qual a área que deve ser protegida e utilize como forma de proteção controles adequados à organização e ao ativo a ser protegido.

Podemos considerar cada local (área) a ser protegido como Site. Uma organização pode ter várias localidades (sites) e todos estes devem ser devidamente e individualmente protegidos.

Uma vez que todos os sistemas estão interconectados, a sua segurança final será tão forte como a segurança de seu site menos seguro. Imagine por exemplo que sua empresa possui um servidor de serviços de diretório (como um domain controller do Windows) em uma localidade remota para que os usuários se autentiquem. Este servidor possui os mesmos dados que o servidor principal que se encontra em uma sala cofre com vigilância 24 horas, e podemos dizer que a segurança física dos dados de seus usuários equivale à segurança aplicada àquele servidor da filial.

9.2.1 – PERÍMETRO DE SEGURANÇA FÍSICA

. *Áreas exteriores das instalações*: use cercas, portões de acesso, monitoramento de entrada e saída;

. *Fronteiras (áreas externas)*: use vigilância armada e câmeras;

. *Entradas das instalações*: restrições de acesso de entrada por janelas, portas e outros locais de acesso;

. *Andares e escritórios*: use identificação de pessoas com crachás, e restrições de acesso a áreas de processamento de dados;

. *Locais de trabalho e processamento*: use travas, racks, cadeados para equipamentos

O ambiente de segurança física é disposto de forma a proteger a infra-estrutura do site contra roubo, destruição e acessos não autorizados, através da adoção de medidas e controles que garantam a proteção dos diversos ambientes internos à organização.

Quando tratamos a proteção de perímetro de segurança física, podemos estruturar o ambiente em diversas camadas, conforme a seguir:

1. ***Áreas exteriores das instalações***: Esta área é a que tem menos controle. Normalmente recomenda-se o uso de cercas, portões de acesso e monitoração de entrada do local até a área sob domínio da organização;

2. ***Fronteiras (áreas externas)***: É a área sob responsabilidade da empresa, mas que não possuem ativos a serem protegidos. São normalmente estacionamentos, jardins e o uso de controles de vigilância armada e câmeras de monitoração são suficientes;

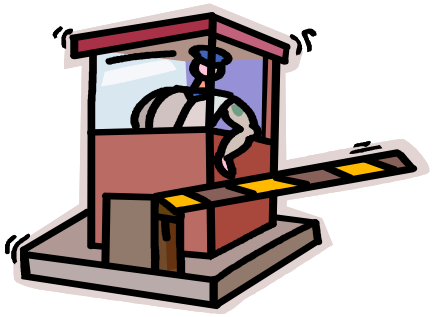
3. ***Entradas das instalações***: Todos os locais de acesso, incluindo portas, janelas, escadas de incêndio e outros que podem não ser tão comuns mas que permitem acesso à organização. Devem ter controles que trate o acesso e identifique o acesso indevido a uma dessas entradas;

4. ***Andares e escritórios***: Áreas de acesso aos locais onde possui dados sensíveis. Todas as pessoas, incluindo funcionários, terceiros e visitantes

devem estar identificados, sendo que pelo menos os funcionários e terceiros devem possuir identificação com foto. Os visitantes só poderão ter acesso a áreas de processamento e manipulação de dados acompanhados de funcionário ou terceiro identificado, que seja responsável pelo visitante. O Acesso a estas áreas dependerá também de uma autorização de acesso para o colaborador e seu convidado;

5. ***Locais de trabalho e processamento***: São os recursos tecnológicos propriamente ditos, que ficam dentro dos escritórios, incluindo computadores, fax, sistemas de comunicação, entre outros. Esses ativos devem ser protegidos contra o acesso indevido, além de roubo dos mesmos. O uso de travas nos Racks dos servidores, bem como cadeado para desktops, notebooks e impressoras vem crescendo nas organizações.

9.2.2– CONTROLE DE ENTRADA FÍSICA



Uso de:

. Funcionários e terceiros sempre identificados atravéz de crachá com foto;

. Visitantes devem ser identificados e acompanhados por um responsável;

. Controles adicionais em locais com informações sensíveis;

. Revisão periódica dos controle de acesso.

Conforme visto anteriormente, todos os acessos devem ser controlados e protegidos.

Como forma de controle de acesso às diversas áreas da organização devemos registrar quem está acessando e o que pode ser acessado.

O acesso começa com a entrada na empresa. Funcionários e terceiros devem estar sempre identificados com o uso de documento com fotos. O acesso de terceiros a áreas seguras deve ser monitorado.

Os visitantes devem também ser identificados e sempre acompanhados por uma pessoa responsável da empresa, sempre que estiver em uma área não pública (exemplos de áreas públicas são recepções e salas de reunião). Mesmo em uma área pública pode-se encontrar diversas informações sensíveis em papéis de rascunho, flip charts, etc.

O acesso a áreas que contenham informações sensíveis, como o datacenter, deve possuir controles adicionais, desde autorização justificada, controles biométricos, até monitoração e auditoria.

Recomenda-se que os acessos sejam revisados periodicamente para verificar se acessos não mais utilizados ainda estão presentes, bem como remover acessos indevidos.

9.2.3– SEGURANÇA EM ESCRITÓRIOS, SALAS E INSTALAÇÕES

Os escritórios, salas e instalações são locais onde ocorrem atividades envolvendo a manipulação das informações em diversas mídias. As informações estão nas telas dos computadores, nos papéis deixados nas impressoras ou em cima de uma mesa e até mesmo em rascunho ou em simpáticos lembretes amarelos colados em lugares diversos.

Nesses locais deve-se garantir que proteções adicionais sejam implementadas a fim de evitar a identificação de quais locais ou que funcionários estão envolvidos com esse tipo de atividade. Outra preocupação importante é assegurar a saúde e segurança das pessoas que trabalhem nas instalações da empresa. Os colaboradores das empresas são valiosos ativos de informação.,e além de garantir um ambiente saudável a todos, a empresa deve garantir que nenhum sistema de proteção poderá ser adotado se em algum momento ameaçar a integridade de seus colaboradores.

Isso fica mais claro quando vemos centros de pesquisas de uma nova tecnologia ou produto ou mesmo em bases militares aonde existe o planejamento estratégico. Todos os ativos de informação, incluindo pessoas são objetos de segurança física.

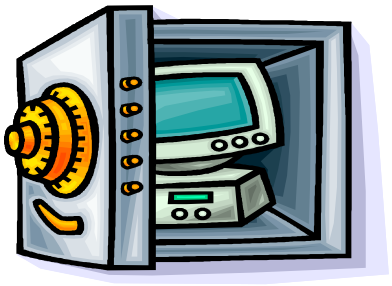
9.2. 4 – PROTEÇÃO CONTRA AMEAÇAS EXTERNAS E DO MEIO AMBIENTE

. Revise as instalações elétricas e hidráulicas;

. Evite material de fácil combustão nessas áreas;

. Se possível use sala-cofre para proteção máxima;

. Crie backups e armazene-os em local distante deste ambiente.



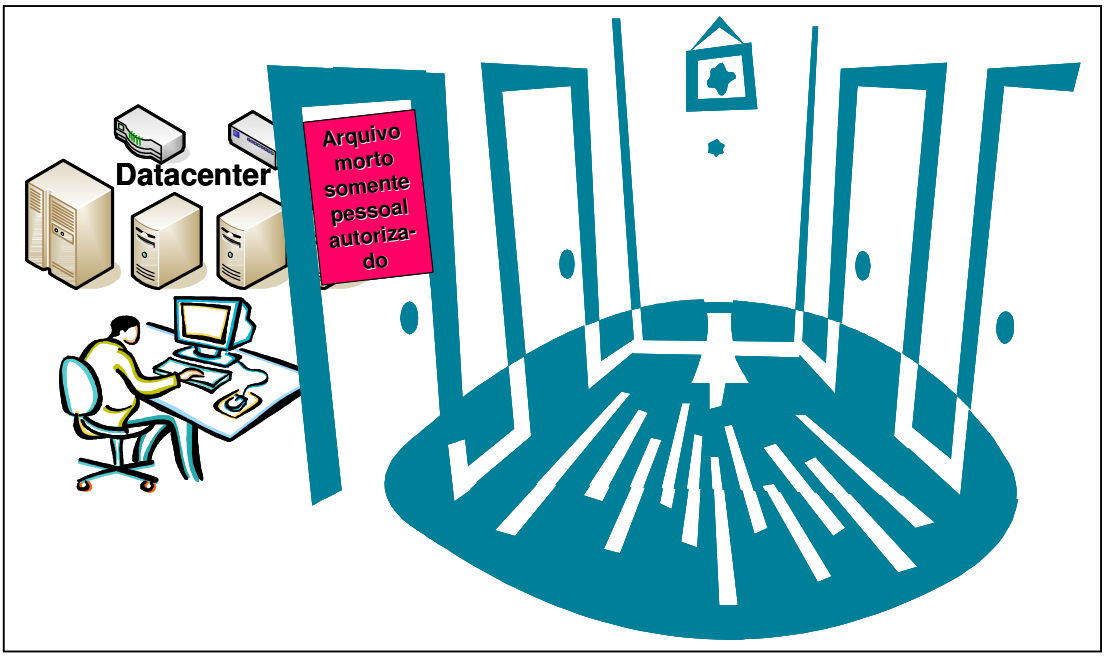
Conforme visto no item de ameaças, várias são suas origens e vários são os meios de ataque aos ativos de informação a serem protegidos. Recomenda-se que seja dada especial atenção ao ambiente físico onde as informações estarão armazenadas, de forma a evitar que ele seja afetado por esses tipos de ameaças.

Para garantir esta proteção deve-se revisar periodicamente as instalações elétricas e hidráulicas, evitar que material de fácil combustão fique próximo a áreas protegidas,e garantir que os equipamentos de proteção como mangueiras e extintores de incêndio estejam em local de fácil acesso e sejam revisados periodicamente.

Deve-se dar especial importância ao armazenamento de mídias de backup nestes locais. O correto é que as mesmas sejam removidas periodicamente para áreas distantes geograficamente e igualmente protegidas para que sejam resgatadas em caso de perda de parte ou de todo o site.

Uma consideração importante a se fazer quanto ao local de armazenamento das mídias de backup é que elas possuem o conjunto das informações mais importantes para seu negócio e caso sejam interceptadas em seu transporte ou furtadas em seu local de armazenamento representam uma grande quebra de confidencialidade.

9.2. 5 – TRABALHANDO EM ÁREAS SEGURAS



Como vimos as áreas seguras devem ser protegidas ao máximo. A melhor forma de fazer isso é utilizarmos o conceito de necessidade de conhecimento (Need to Know).

Ambientes considerados seguros não devem ser identificados a fim de dificultar sua localização por quem não é autorizado para estar lá. Somente aqueles que precisarem acessá-lo devem conhecer sua localização dentro da organização e quais os métodos de acesso e mecanismos de proteção dos mesmos.

Na estruturação de um datacenter, devemos colocar a área de operação em local separado dos equipamentos que estão processando os dados. No caso de uma visita essa primeira seria a única a ser apresentada aos visitantes. Deve-se evitar e até proibir registros de imagens (fotos e filmes) destes locais.

Manutenções em equipamentos, sistemas elétricos, sistema de refrigeração, ou qualquer outro sistema que suporte a operação da empresa só poderão ser feitas após a programação ser aprovada pelo responsável por TI e com supervisão ininterrupta de algum colaborador da empresa.

9.2. 6 – ACESSO DO PÚBLICO, ÁREAS DE ENTREGA E DE CARREGAMENTO

O acesso a área de entrega deve:

. Materiais sejam inspecionados e registrados;

. Não dar acesso a outras áreas;

. Protegidas enquanto abertas;

. Separar o que entra e o que sai.

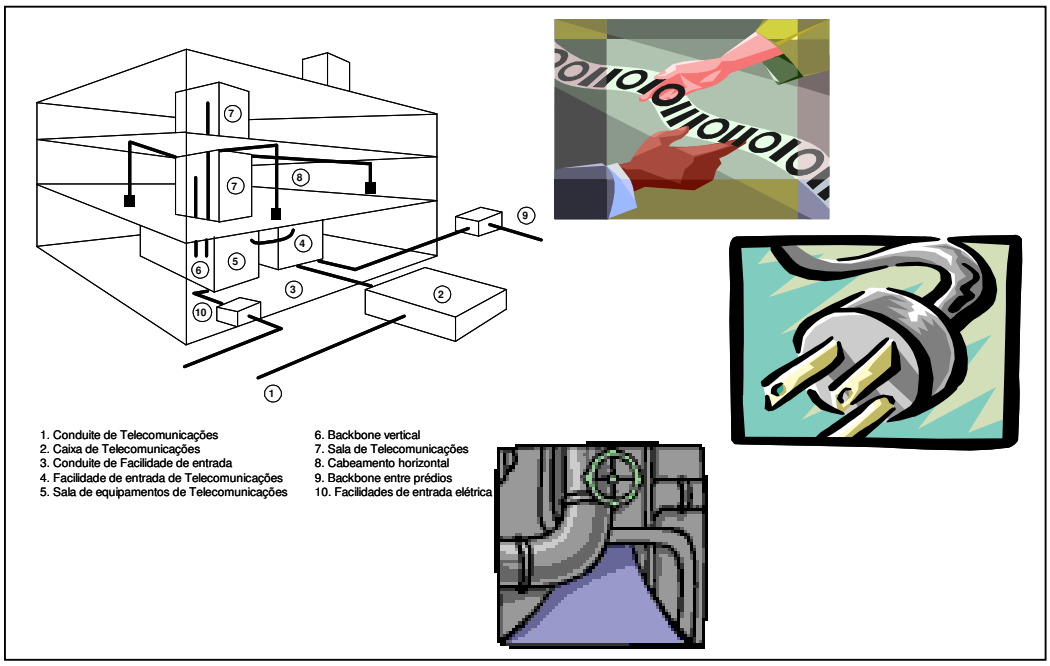
. Ser restrito a pessoal autorizado;

É comum que a área de carga e descarga de materiais esteja localizada próximo às áreas seguras e o acesso e controle destas áreas não seja tão eficaz como o aplicado às áreas seguras.

A norma é bem clara quanto ao cuidado especial que deve ser feito a este tipo de acesso às instalações. O acesso das pessoas que estão levando o material deve ser feito em local protegido do acesso a área interna da organização e o material deve ser inspecionado, verificado e autorizado antes do mesmo ter sua entrada permitida.

Em especial, recomenda-se que esta área seja distante das áreas consideradas seguras.

9.3– SEGURANÇA DE EQUIPAMENTOS



O perímetro de segurança física termina na proteção dos equipamentos em si. Nesta parte, veremos com mais detalhes as proteções aos equipamentos (ou ativos e informação) de Tecnologia da Informação.

9.3.1 – INSTALAÇÃO E PROTEÇÃO DO EQUIPAMENTO

Nos locais de instalação de equipamentos, deve-se observar:

. Devem ser instalados em locais que dificultem a visão

. Se possível isolar equipamentos que requerem proteção especial

. Instalados em locais com proteção física contra incêndios, roubo, fumaça, água, etc…

. Controlar uso de alimentos e cigarro

. Monitorar temperatura e umidade

. Proteção contra descarga elétrica

Assim como temos vários controles lógicos de segurança (normalmente chamados Hardening ou fortalecimento) durante a implementação de equipamentos, também temos que nos preocupar com controles físicos.

Esses controles começam com a disponibilização do equipamento. Deve ser evitado que os dados que estão sendo manipulados sejam facilmente visualizados pelo público ou por transeuntes (mesmo que funcionários identificados) e que os dados de armazenamento fiquem em locais protegidos. Os controles continuam com a disponibilização de infra-estrutura elétrica, cabeamento, refrigeração, umidificação e todos aqueles que visem manter o ativo em perfeito funcionamento.

Controles que vimos para proteção de áreas seguras devem estar disponíveis para proteger os equipamentos, como proteções elétricas e hidráulicas.

Adicionalmente deve se evitar o consumo de alimentos e fumo próximo aos equipamentos a ser protegidos. Este trabalho é feito inicialmente pela política de segurança e reforçado pela campanha de conscientização.

Para equipamentos que processem dados sensíveis é importante que tenham segurança física reforçada, como alojar os mesmos em locais de difícil acesso e controlar esses acessos, através de identificação e auditorias.

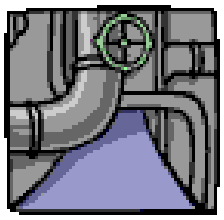
9.3. 2 – UTILIDADES

Definição: sistemas que suportam a operação dos equipamentos.

Deve-se inspecionar e proteger as instalações contra interrupções de fornecimento de:

. Energia elétrica (uso de no-breaks, geradores e linhas alternativas);

. Suprimento de água (o ar condicionado e sistemas de umidificação dependem da água);



. Ventilação e calefação.

Quando abordamos as ameaças vimos que muitas delas afetam as instalações (facilities em inglês). Estas utilidades garantem a operação dos equipamentos através do fornecimento de energia e de outros componentes como fornecimento de água (para refrigeração) e comunicação.

O fornecimento de energia é vital para a operação dos equipamentos, bem como para funcionamento de outras utilidades como ar-condicionado. A interrupção abrupta pode causar a perda dos dados que estavam sendo processados no momento da interrupção nos equipamentos de computação.

Para garantir o fornecimento de energia deve-se fazer uso de sistemas de UPS (do inglês uninterruptible power supply ou suprimento ininterrupto de energia) por um período suficiente para continuar a operação até o desligamento normal dos equipamentos. Para equipamentos que não possam ficar parados, deve-se considerar o uso de geradores elétricos, que contemplem inclusive o sistema de refrigeração do datacenter.

O fornecimento de água também é importante, pois abastece os sistemas de umidificação e refrigeração (ar-condicionado).

O fornecimento de utilidades deve ser monitorado continuamente e o não fornecimento ou fornecimento inadequado deve ser alertado (pode se considerar o uso de alarmes).

9.3. 3 – SEGURANÇA DO CABEAMENTO

Proteja o cabeamento com:

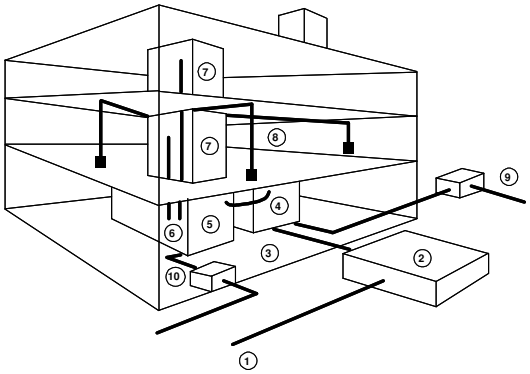
. Cabos externos subterrâneos

. Afastando-o de interferências eletromagnéticas ou usando fibra óptica

. Fazendo inspeção físicas periódicas em busca de traps

. Identifique os cabos

. Crie documentação das conexões



1. Conduite de Telecomunicações
2. Caixa de Telecomunicações
3. Conduite de Facilidade de entrada
4. Facilidade de entrada de Telecomunicações
5. Sala de equipamentos de Telecomunicações
6. Backbone vertical
7. Sala de Telecomunicações
8. Cabeamento horizontal
9. Backbone entre prédios
10. Facilidades de entrada elétrica

Tanto o fornecimento de energia quanto a comunicação dos dados (lembremos que hoje existem ambientes de tecnologia da informação distribuídos e convergentes) são feitos normalmente através de cabos ou de comunicação em redes sem fio.

Todo o cabeamento deve ser, portanto, protegido quanto a sua interrupção, devendo os mesmo passar por locais protegidos fisicamente e recomenda-se que cheguem ao datacenter pelo subterrâneo, longe do conhecimento público.

Os princípios de cabeamento estruturado exigem distância entre os cabos lógicos (redes) e elétricos (energia) para evitar que o campo magnético do cabo elétrico afete a transmissão dos dados (nos caso dos cabos passarem por campos elétricos deve-se usar fibra ótica que evita a interferência elétrica).

Deve-se dar especial atenção aos cabos de comunicação, para evitar que o mesmo não seja usado para interceptação não autorizada dos dados. Para tanto se deve fazer uso de passagens protegidas por canaletas e/ou conduítes. Periodicamente deve-se fazer uma inspeção física para verificar se equipamentos espiões (chamados de traps) foram colocados irregularmente devendo os mesmos ser removidos.

Para complementar a segurança física e pode-se utilizar de alguns controles lógicos adicionais como o IPSec e a autenticação 802.1X, ambos nativos nos principais sistemas de redes atuais. Conheça mais em:
http://www.microsoft.com/brasil/technet/Artigos/Seguranca/sm121504.mspx
http://www.microsoft.com/brasil/security/guidance/topics/ipsec/default.mspx)
http://www.microsoft.com/brasil/technet/artigos/Seguranca/AvisoSeguranca/303.aspx)

9.3. 4 – MANUTENÇÃO DOS EQUIPAMENTOS

. Devem ser periódicas e haver registros de execução

. Obedecer recomendações de fabricantes

. Feitas por pessoal autorizado

. Falhas devem ser registradas

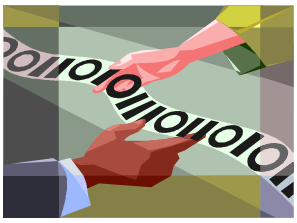
Como os equipamentos são mecânicos e estão sujeitos a uma série de efeitos externos (como poeira, umidade, etc.) os mesmos devem sofrer revisão e manutenção preventiva periodicamente. Esta medida tem por finalidade a garantia de integridade e disponibilidade dos equipamentos.

Como forma de controle de falhas, todas as ocorrências devem ser registradas e casos repetidos devem ser tratados o mais breve possível (normalmente através da substituição do componente falho).

Deve-se tomar cuidado adicional com a manutenção de equipamentos que armazenem informações sensíveis de forma que os mesmos sejam manuseados por pessoas de confiança (ou monitorados em suas atividades), e ainda se assegurar que as informações sensíveis foram removidas dos equipamentos antes da manutenção.

9.3. 5 – SEGURANÇA DE EQUIPAMENTOS FORA DAS DEPENDÊNCIAS DA ORGANIZAÇÃO

Deve haver:



. Autorização da gerência

. Proteção contra exposição eletromagnética

. Transportados de maneira disfarçada

. Acessos remotos através de comunicação criptografada

. Armazenagem de dados criptografada

. Seguro dos equipamentos

A computação atual está cada vez mais portátil. Isso se reflete dentro e fora da empresa. Muitas vezes equipamentos são levados para áreas de campo, em viagens a trabalho ou para as residências dos colaboradores.

Normalmente as posições de maior responsabilidade dentro da organização fazem uso de equipamentos móveis, como notebooks. Essas pessoas são as que justamente têm acesso às informações mais sensíveis e as levam consigo em viagens e para suas residências, onde muitas vezes acessam informações da empresa remotamente.

Nos locais de grande tráfego de executivos (aeroportos é o principal alvo) está crescendo o mercado de roubo de notebooks. Sendo assim é recomendável que eles sejam sempre levados em bagagens que não evidenciem o que está sendo transportado. Também se recomenda que estes equipamentos não sejam abertos em locais públicos (isso deve constar na política de segurança e fazer parte do treinamento dos funcionários e terceiros). Como solução para mitigar o prejuízo com o roubo de equipamentos, deve-se considerar do ponto de vista físico, o seguro desses ativos, e do ponto de vista lógico, a criptografia dos dados armazenados localmente (veja como criptografar dados no Windows XP em http://www.technetbrasil.com.br/Artigos/Seguranca/AvisoSeguranca/202.aspx ou ainda: http://www.microsoft.com/brasil/windowsxp/pro/usando/artigos/comp_cripto.mspx).

Para os equipamentos de uso em campo se deve verificar com os fabricantes as especificações técnicas dos mesmos, principalmente relacionado à resistência contra campos eletromagnéticos.

Os trabalhos realizados em casa por funcionários devem obedecer à política de segurança (que pode usar conceitos como o de mesa limpa, que é o de não deixar documentos visíveis quando ausente do ambiente de trabalho, entre outros). Muitas vezes é necessário realizar acesso remoto para atividades de trabalho, que deve ser feito através de comunicação segura. Como forma de proteção nestas comunicações, o uso de autenticação forte e IPSec em redes VPN é hoje a melhor opção disponível. Além disso, o uso de recursos de quarentena que fazem inspeções lógicas podem ser utilizados.

Mais informações neste documento de Liou Kuo Chin para a Rede Nacional de Ensino e Pesquisa (RNP): http://www.rnp.br/newsgen/9811/vpn.html.

9.3. 6 – REUTILIZAÇÃO E ALIENAÇÃO SEGURA DOS EQUIPAMENTOS

No descarte substituição ou recuperação de equipamentos:

. Remova todos os dados sensíveis

. Destrua fisicamente em caso de descarte

. Em caso de recuperação, avalie a necessidade real

Quando o equipamento fica obsoleto o mesmo precisa ser descartado. No entanto esse descarte deve ser feito com as preocupações devidas dentro dos padrões da segurança da informação. A principal é a de remoção completa das informações armazenadas em discos de armazenamentos.

Atualmente uma série de técnicas para recuperação de dados, mesmo em discos defeituosos estão crescendo aceleradamente. Isso é útil quando no caso do famoso desastre de 11 de setembro de 2000, muitas informações foram recuperadas, mas pode ser perigoso quando dados são recuperados com o intuito de usar a informação para fins ilícitos como espionagem industrial por exemplo.

Dependendo do grau de sensibilidade dos dados, os dispositivos de armazenamento devem ser completamente destruídos de forma controlada.

Outra situação é no caso de falha de equipamentos. Deve ser avaliado se os eles serão recuperados ou substituídos. Nos casos de recuperação, essa deve seguir os mesmos passos usados na manutenção de equipamentos e nos casos de substituição, deve-se tomar os mesmos cuidados que temos para o descarte como vimos há pouco.

9.3. 7 – REMOÇÃO DE PROPRIEDADE

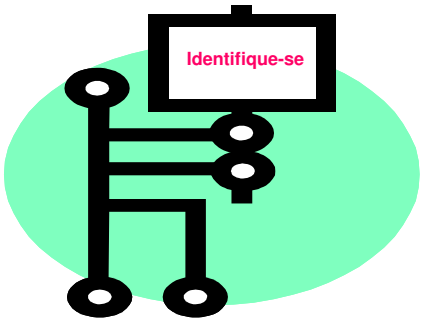
Deve ser feita:

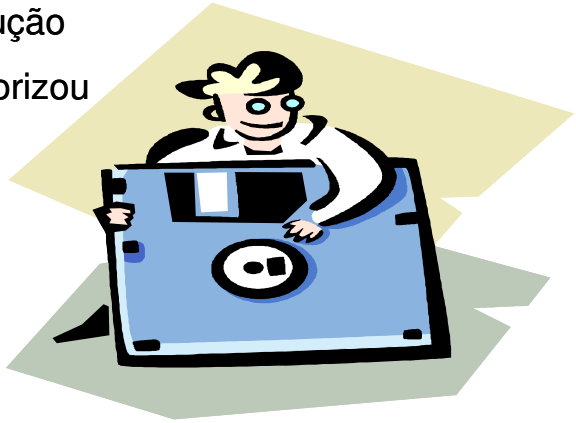
. Com autorização específica do proprietário do ativo

. Por tempo limitado

. Registro de saída e devolução

. Identificação de quem autorizou





Toda retirada de equipamento da organização deve ser feita de forma controlada e protegida, evitando-se que equipamentos que contenham informações sensíveis sejam retirados da empresa sem a devida autorização.

Muitas vezes a entrada e saída de equipamentos dentro da empresa não são devidamente controladas ou por se tratar de pessoa conhecida, essa saída é permitida.

Para que os equipamentos possam sair da empresa devem possuir autorização específica que deverá ser dada por pessoas claramente identificada e que essa identificação seja pública.

Como forma adicional de controle, pode-se estabelecer limites para período de saída de equipamentos além do registro do mesmo ocorre a retirada dele e o seu retorno.

Referências:

[1] Artigo publicado em http://www.infoguerra.com.br/infonews/talk/1027662193,47860,.shtml de autoria de F.F. Ramos.

[2] Fontes, Edison. Segurança da Informação: O usuário faz a diferença!, Editora Saraiva, 2006, São Paulo, 173pp.

[3] Fontes, Edison. Vivendo a Segurança da Informação. Editora Sicurezza, 2000, São Paulo, 207pp