
Curso Básico de Segurança da Informação

Academia Latino-Americana de Segurança da Informação

Introdução à Segurança da Informação

Módulo 1

Apostila desenvolvida pelo Módulo Security e revisada pelo capítulo Brasil da ISSA, em parceria com a Microsoft Informática



www.modulo.com.br

<http://www.issabrasil.org>

Revisão 1.1 – Dezembro de 2006

COORDENADOR TÉCNICO

Fernando Fonseca

REVISORES:

Anchises de Paula

Augusto Paes de Barros

Dimitri Abreu

Luciana Vartuli

Luciano Barreto

COMO USAR ESSE MATERIAL

Este é um material de apoio para o curso “Introdução à Segurança da Informação” ministrado pela Academia de Segurança Microsoft. Um vídeo será explicando os conceitos deste material estará disponível na academia para auxiliar no entendimento dos conceitos aqui explicados.

VÍDEO



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

CONCEITO-CHAVE



Indica um ponto importante para se assimilar melhor a matéria.

PERGUNTAS PARA PENSAR



Indica uma pergunta que estimula um raciocínio lógico para auxiliar o aprendizado

VULNERABILIDADES



Indica uma vulnerabilidade atribuída a um conceito sendo estudado

INTRODUÇÃO	6
Notícias pelo Mundo	7
Objetivos.....	8
Conteúdo da unidade:	9
INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO	10
1.1 Introdução	10
Notícias pelo Mundo	11
1.2 - Objetivos.....	Error! Bookmark not defined.
1.3 - Implementação de um sistema de segurança	13
1.4 Conceitos básicos	14
1.4.1 Princípios básicos da segurança da informação	17
1.4.2 - Princípio da Integridade da Informação	18
Proteger a Integridade da Informação	19
1.4.3 - Princípio da Confidencialidade da Informação.....	20
Proteger a Confidencialidade da Informação	21
1.4 .4 - Princípio da Disponibilidade das Informações	23
Proteger a Disponibilidade da Informação	24
1.5 - Evolução da segurança da Informação	25
1.6 Lições Aprendidas.....	29
ATIVOS	31
2.1 Introdução	31
Notícias pelo Mundo	32
2.2 Objetivos	33

2.3 Tipos de Ativos	34
2.3.1 - Informações	35
2.3.2 - Software (B1).....	36
2.3.2 - Hardware (B2).....	37
2.3.2 - Organização (B3).....	38
2.4 - Usuários	39
2.6 - Lições aprendidas	40
AMEAÇAS E PONTOS FRACOS.....	41
3.1 Introdução	41
Notícias pelo Mundo	42
3.2 - Objetivos.....	43
3.3 - As Ameaças.....	44
3.4 - Vulnerabilidades	47
3.5 - Lições Aprendidas	54
RISCOS, MEDIDAS E CICLO DE SEGURANÇA.....	55
4.1 Introdução	55
Notícias pelo Mundo	56
4.2 Objetivos	57
4.3 Riscos	58
4.4 Medidas de Segurança	59
4.5 Ciclo de Segurança.....	62
4.6 Lições Aprendidas.....	64
4.7 Referência Bibliográfica	65

INTRODUÇÃO

No mundo atual a posse e o uso do conhecimento passou a ser um fator estratégico decisivo para muitas empresas e corporações. Estamos vivendo a época batizada como "Era da Informação". Mas a informação é volátil. é frágil. Hoje, ela pode desaparecer na velocidade de um pulso elétrico.

Muitas empresas tem seus ativos físicos e suas informações constantemente expostos a diversas ameaças, que poderiam representar prejuízos de milhares ou milhões de dólares se forem concretizadas. As vulnerabilidades e fragilidades em nossos sistemas de informação podem causar problemas graves ao negócio, por isso é muito importante compreender os conceitos necessários para combatê-las e, assim, nos defendermos de possíveis ataques às informações estratégicas.

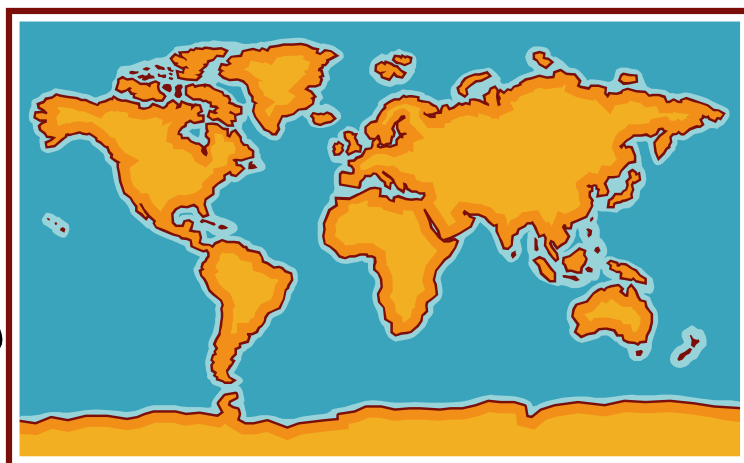
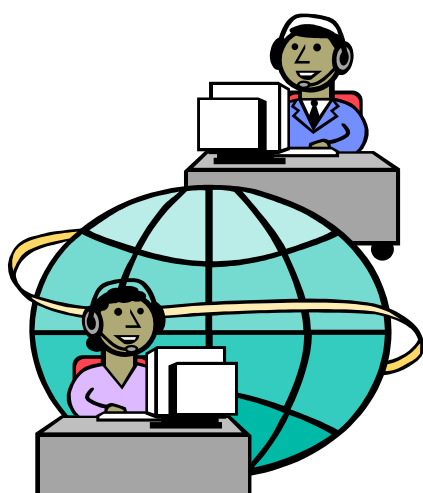
Exemplos destas ameaças são os vírus e os worms (vermes) que se aproveitam de falhas na segurança dos sistemas e circulam pela Internet em busca de máquinas vulneráveis nas quais possa realizar seu ataque. Na maioria das vezes, estes ataques resultam em perder de dados e destruição de informações valiosas.

Exemplos claros de como as vulnerabilidades presentes em nossos sistemas computacionais podem ser aproveitadas por Crakers (pessoas que se dedicam a criar pestes eletrônicas e invadir sistemas) são danos causados no mundo todo pelos vermes Blaster, Ninda e Slammer.

Os fabricantes de software e a comunidade de software livre se esforçam para corrigir estas vulnerabilidades através de atualizações (patches), mas um fator mais importante nos chama a atenção: Será que as empresas conhecem os riscos aos quais estão expostas e se preparam para reduzi-los?

Há poucos anos atrás, a resposta seria um sonoro não. Prova disso é que estes worms causaram um estrago enorme mesmo tendo atacado vulnerabilidades que já haviam sido corrigidas meses antes. Faltou um processo de manutenção da segurança do ambiente para que as correções fossem aplicadas e bilhões de dólares fossem perdidos. A boa notícia é que depois de tanto prejuízo as empresas começam a valorizar estes processos.

O objetivo deste curso é capacitar um número maior de profissionais nos conceitos e boas práticas em segurança da Informação e, assim, fazer com que os processos necessários para a redução dos riscos e proteção dos ativos sejam criados e que a cultura de segurança se espalhe cada vez mais pelas empresas.



NOTÍCIAS PELO MUNDO

Montadora de aviões tem notebook roubado e pode ter informações expostas

A Boeing, uma das maiores montadoras de aviões do mundo, teve um notebook roubado. O equipamento continha nomes e números da previdência social de cerca de 382 mil funcionários e aposentados, que já começaram a ser notificados do ocorrido. Este é o terceiro portátil da companhia que desaparece em 13 meses. A informação é do site BetaNews.

O sumiço de tais informações pode fazer com que funcionários tenham suas identidades roubadas, além de haver riscos de fraudes com cartões de crédito. Dados como endereços residenciais, datas de nascimento e telefones de contato estavam presentes no notebook. A Boeing declarou que dados de fornecedores ou clientes não estavam armazenados no dispositivo, mas não divulgou em qual de seus escritórios ocorreu o furto. Segundo a companhia, para o ladrão visualizar os dados do notebook, ele teria de conseguir a senha de acesso do laptop, coisa que um cracker de competência média pode conseguir sem muito trabalho. Na tentativa de evitar golpes com tais informações, a empresa oferecerá um serviço de monitoração de crédito por um período de três anos

Fonte: *Módulo Security News* (www.modulo.com.br)



- ☐ Conhecer os conceitos básicos que fundamentam os estudos sobre segurança da informação
- ☐ Conhecer as diferentes categorias de ativos existentes em uma empresa.
- ☐ Compreender o conceito de pontos fracos para identificar as possíveis vulnerabilidades e as ameaças existentes nos ativos.
- ☐ Interpretar a classificação proposta das possíveis ameaças encontradas nos diferentes processos da empresa.
- ☐ Revisar os conceitos de integridade, confidencialidade e disponibilidade da informação.
- ☐ Conhecer o conceito de risco e sua implicação no ciclo de segurança das informações da empresa.
- ☐ Distinguir a diferença entre aplicar ou não medidas de segurança nos diferentes aspectos de nossa empresa.
- ☐ Compreender os conceitos básicos de análise de riscos e política de segurança, dois pontos muito importantes para definir as ações em matéria de segurança aplicáveis às empresas.

CONTEÚDO DA UNIDADE:

- ☐ Conceitos básicos
- ☐ Ativos
- ☐ Ameaças e pontos fracos
- ☐ Riscos, medidas e ciclo de segurança

INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

1.1 INTRODUÇÃO

Neste capítulo, veremos alguns conceitos fundamentais para a compreensão da segurança da informação e das metodologias para sua implantação nas organizações.

Desde o surgimento da raça humana na Terra, a informação esteve presente através de diferentes formas e técnicas. O homem buscava representar seus hábitos, costumes e intenções com diversos meios que pudessem ser utilizados por ele e por outras pessoas e que pudessem ser levados de um lugar para outro. As informações importantes eram registradas em objetos preciosos e sofisticados e pinturas magníficas, entre outros, que eram armazenados com muito cuidado em locais de difícil acesso. A eles só tinham acesso aqueles que tivessem autorização para interpretá-la.

Atualmente, as informações constituem o objeto de maior valor para as empresas. O progresso da informática e das redes de comunicação nos apresenta um novo cenário, no qual os objetos do mundo real estão representados por bits e bytes, que ocupam lugar em diversos meios e possuem formas diferentes das originais, sem deixar de ter o mesmo valor que os objetos reais e, em muitos casos, chegando a ter um valor maior.

Por esse e outros motivos a segurança da informação é um assunto tão importante para todos, pois afeta diretamente todos os negócios de uma empresa ou de um indivíduo.

Segurança é um termo que transmite conforto e tranquilidade a quem desfruta de seu estado. Entender e implementar este “estado” em um ambiente organizacional exigem conhecimento e práticas especializadas que somente são possíveis com o emprego e uso de um código de práticas de segurança, contidos em uma norma, como a ABNT NBR ISO/IEC 17799:2005.



NOTÍCIAS PELO MUNDO

Pesquisa revela falta de padrões de segurança em grandes empresas

Um estudo recente feito pela empresa britânica de consultoria Pentasafe revela que a falta de procedimentos de segurança por parte de funcionários coloca informações confidenciais das grandes empresas em risco.

Foram entrevistados 15 mil funcionários de 600 grandes empresas dos EUA e da Europa. A pesquisa constatou que 60% dos funcionários têm poucos conhecimentos sobre planos de segurança. 90% dos entrevistados admitiram abrir ou executar arquivos desconhecidos anexados em e-mails.

No entanto, muitas empresas também são responsáveis pelos problemas relacionados à segurança. Em um terço delas os empregados não são obrigados a ler a política de segurança existente. 50% admitiram nunca terem recebido qualquer tipo de treinamento específico sobre o tema.

Fonte: <http://www.modulo.com.br/>



- ☐ Compreender os conceitos básicos da segurança da informação para obter uma melhor idéia de suas implicações.
- ☐ Entender a importância da informação nos negócios atualmente para agir de forma mais ágil na sua proteção.
- ☐ Conhecer os princípios básicos da segurança da informação: confidencialidade, disponibilidade e integridade, com a finalidade de entender como as ameaças e vulnerabilidades podem atingir a cada um deles e saber quais as medidas de proteção mais adequadas para cada informação.
- ☐ Conhecer a evolução da segurança da informação como disciplina de estudos desde o seu nascimento até os dias de hoje.

1.3 - IMPLEMENTAÇÃO DE UM SISTEMA DE SEGURANÇA



Podemos representar a implantação de um sistema de segurança da informação na empresa como a escalada de uma grande montanha, na qual pouco a pouco iremos subindo e passando os níveis em termos de conceitos, ferramentas e conhecimento do ambiente tecnológico da empresa. Mais tarde veremos que não basta chegar ao topo da montanha; a segurança é um processo contínuo, o chamado ciclo de segurança.



Este é o nosso acampamento base no qual teremos como tarefa conhecer os conceitos a partir do

CICLO DA SEGURANÇA DA INFORMAÇÃO

Esta situação é bem parecida com a que encontramos na maioria das organizações:

Desconhecimento do ambiente;

Ativos Desprotegidos;

Falta de Conscientização de Segurança;

Administração insegura da Informação.

1.4 CONCEITOS BÁSICOS

Nesta primeira etapa da escalada, você conhecerá os conceitos básicos da segurança da informação.

Depois de entender cada conceito, você receberá uma nova ferramenta para ajudar a montar sua barraca e, assim, poder continuar a escalada da montanha, avançando até os próximos capítulos para compreender como se implementa a segurança da informação.

Nesta etapa, você ainda não possui essas ferramentas, por isso vai começar a escalada com um acampamento básico. Esse acampamento ilustra a situação em que se encontram as empresas na etapa inicial da implementação da segurança: baixo controle do ambiente, alto índice de risco, processo de segurança pessoal e intuitivo, entre outros.

Então vamos conhecer os principais conceitos da segurança da informação e por que ela é necessária para o sucesso dos negócios de uma empresa.

O objetivo deste estudo é obter um ambiente seguro para a informação. Mas o que é informação?

Segundo o dicionário Aurélio [¹], informação é o conjunto de dados acerca de alguém ou de algo. Estendendo esse conceito, podemos dizer que a informação é a interpretação desses dados. De nada vale um conjunto de dados sem que se faça a interpretação dos mesmos para se extrair um conhecimento útil.

As organizações necessitam da informação para tomar decisões objetivando seus fins (o sucesso). Isto mostra o quão poderosa é a informação. Sem ela não há estratégias, não há mudanças ou até mesmo não existiria a empresa. Uma consequência natural da importância da informação é a extrema vulnerabilidade a que cada empresa se expõe caso haja perda de dados vitais, como plantas de projetos, planilhas de custos, documentos contábeis, financeiros, etc. Quanto maior for a organização maior será sua dependência da informação.

A informação pode estar armazenada de várias formas: impressa em papel, em meios digitais (discos, fitas, CDs, DVDs, disquetes), na mente das pessoas, em imagens armazenadas em fotografias e filmes. Quando lidamos com segurança da informação, é necessário pensar em sua confidencialidade, integridade e disponibilidade em qualquer um desses meios, utilizando todos os recursos disponíveis, e não somente os tecnológicos.

Devemos tratar a informação como um ativo da empresa com a mesma importância que qualquer outro bem palpável. Por isso, deve ser protegido contra roubo, problemas ambientais, vandalismo, dano acidental ou provocado.

Quanto mais interconectada for uma empresa, maior será a complexidade dos sistemas por onde trafegam e são armazenadas as informações e, conseqüentemente, maior será a preocupação com o nível de segurança a ser implantado a fim de garantir a confidencialidade, confiabilidade, disponibilidade e integridade da informação que ela detém.

A disciplina de segurança da informação trata do conjunto de controles e processos que visam preservar os dados que trafegam ou são armazenados em qualquer meio.

As modernas tecnologias de transporte, armazenamento e manipulação dos dados, trouxeram enorme agilidade para as empresas, mas, ao mesmo tempo, trouxeram também novos riscos. Ataques de crackers (black hat hackers), de engenharia social, vírus, worms, negação de serviço, espionagem eletrônica são noticiadas pela imprensa todos os dias. Diante deste cenário, a segurança da informação torna-se imprescindível para as organizações, sejam elas do setor público ou privado.



**Idéias-
chave**

A **segurança da informação** tem como propósito proteger as informações registradas, sem importar onde estejam situadas: *impressas em papel, nos discos rígidos dos computadores ou até mesmo na memória das pessoas que as conhecem.*



Perguntas para pensar

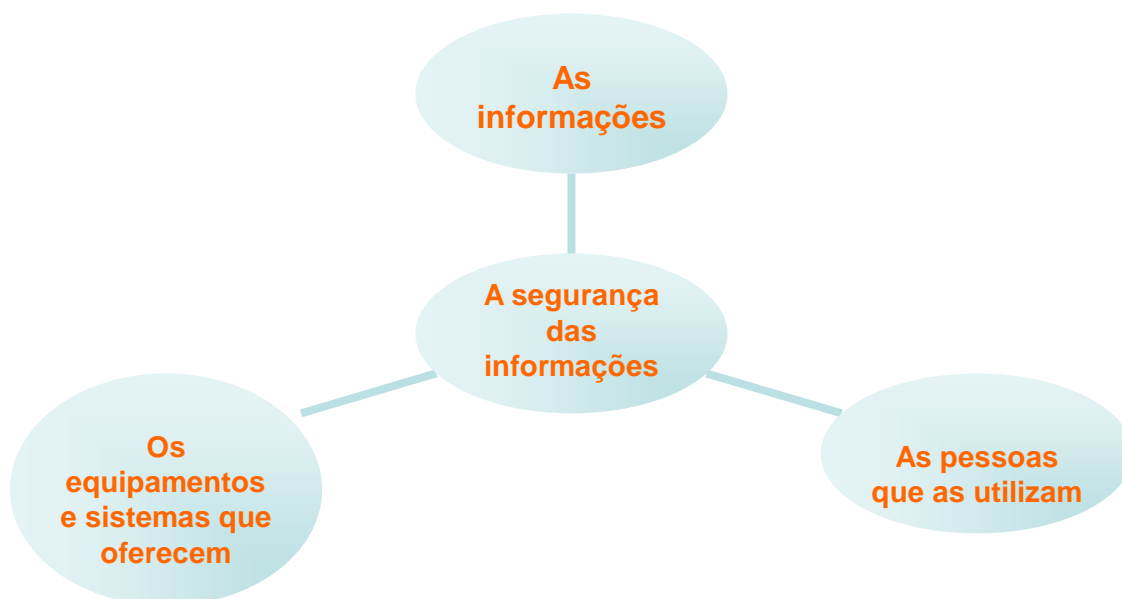
Os objetos reais ou tangíveis (entendendo-os como coisas de valor físico – jóias, pinturas, dinheiro etc.) estão protegidos por técnicas que os isolam atrás de grades ou dentro de caixas fortes, sob a mira de câmeras ou seguranças. Mas, e as informações encontradas dentro de servidores de arquivos, que transitam pelas redes de comunicação ou que são lidas na tela de um computador? O que fazer para protegê-las, já que não é possível usar as mesmas técnicas de proteção de objetos reais?

Para responder essas perguntas, convidamos você a continuar revendo o conteúdo temático desta unidade, onde conheceremos com detalhes os princípios que permitirão proteger a informação. Por enquanto, neste capítulo, encerraremos dizendo que...

... uma das preocupações da segurança da informação é proteger os elementos que fazem parte da comunicação. Assim, para começar, é necessário identificar os elementos que a segurança da informação tenta proteger:

- ☐ As informações
- ☐ Os equipamentos e sistemas que oferecem suporte a elas
- ☐ As pessoas que as utilizam

Além disso, é importante que todos os funcionários da empresa tenham consciência de como devem lidar com as informações de forma segura, já que de nada serve qualquer sistema de segurança, por mais complexo e completo que seja, se os funcionários, por exemplo, facilitam o acesso ou fornecem seu nome de usuário e senha a pessoas estranhas à empresa e, com isso, deixam aberta a porta para possíveis ataques ou vazamento de informações críticas para fora da empresa.



1.4.1 PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

Agora aprofundaremos os princípios básicos que nos ajudarão a proteger o ativo de mais valor nos negócios modernos: a informação.

Proteger os ativos significa adotar medidas para evitar a concretização de ameaças que podem afetar a informação:

- ☐ Corrompendo-a,
- ☐ tendo acesso a ela de forma indevida, ou mesmo
- ☐ eliminando-a ou furtando-a

Por isso, entendemos que a segurança da informação busca proteger os ativos de uma empresa ou indivíduo com base na preservação de três princípios básicos:

- ☐ **Integridade**
- ☐ **Confidencialidade** e
- ☐ **Disponibilidade** da informação

Nas próximas páginas, você encontrará informações mais detalhadas sobre cada um desses princípios.

1 **Pilares da Segurança da Informação**

INTEGRIDADE

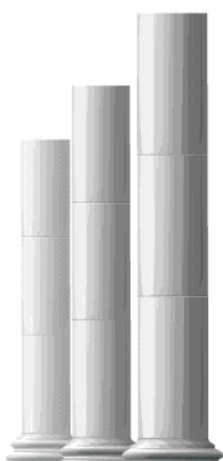
Não é a mesma coisa que exatidão. Se a informação estiver correta, deve continuar correta; se estiver errada, deve continuar errada.

Pode se ter integridade sem exatidão, mas não se pode ter exatidão sem integridade.

O controle de integridade protege a informação de ameaças involuntárias e intencionais: controla o direito acessos indevidos de terceiros e limita o acesso aos funcionários de acordo com as necessidades dos serviços.

*Leia esta matéria sobre
quebra de Integridade publicada pelo informativo
Comunidade de Segurança em 1998: Ataques no Japão*

Garantia que a informação que é armazenada será a mes



1.4.2 - PRINCÍPIO DA INTEGRIDADE DA INFORMAÇÃO

O primeiro dos três princípios da segurança da informação que aplicamos é a integridade, a qual nos permite garantir que a informação não tenha sido alterada de forma não autorizada e, portanto, é íntegra.

Uma informação íntegra é uma informação que não foi alterada de forma indevida ou não-autorizada.

Para que a informação possa ser utilizada, ela deve estar íntegra. Quando ocorre uma alteração não-autorizada da informação em um documento, isso quer dizer que o documento perdeu sua integridade.

A integridade da informação é fundamental para o êxito da comunicação.

O receptor deverá ter a segurança de que a informação recebida, lida ou ouvida é exatamente a mesma que foi colocada à sua disposição pelo emissor para uma determinada finalidade. Estar íntegra quer dizer estar em seu estado original, sem ter sofrido qualquer alteração por alguém que não tenha autorização para tal. Se uma informação sofre alterações em sua versão original, então ela perde sua integridade, o que pode levar a erros e fraudes, prejudicando a comunicação e o processo de decisões.

A quebra de integridade ocorre quando a informação é corrompida, falsificada ou indevidamente alterada.

Uma informação poderá ser alterada de várias formas, tanto em seu conteúdo quanto no ambiente que lhe oferece suporte. Portanto, a quebra da integridade de uma informação poderá ser considerada sob dois aspectos:

1. **Alterações do conteúdo** dos documentos – quando são realizadas inserções, substituições ou exclusões de parte de seu conteúdo.
2. **Alterações nos elementos que oferecem suporte à informação** – quando são realizadas alterações na estrutura física e lógica onde a informação está armazenada.

Exemplo:

Quando as configurações de um sistema são alteradas para permitir acesso de escrita a informações restritas, quando são superadas as barreiras de segurança de uma rede de computadores. Todos são exemplos de situações que podem levar a quebra da integridade, afetando a segurança. Portanto, a prática da segurança da informação tem como objetivo impedir que ocorram eventos de quebra de integridade, que causam danos às pessoas e às empresas



**Perguntas
para
pensar**

Quão importante é para você que as informações sobre os salários dos funcionários de sua empresa não sejam alteradas por acidente ou delito?
Você sabe se as informações sobre os projetos de negócios confidenciais estão seguras e não podem ser alteradas por terceiros?

Vejamos algumas observações finais sobre o propósito que queremos alcançar ao proteger a integridade da informação.

PROTEGER A INTEGRIDADE DA INFORMAÇÃO

Buscar a integridade é tentar assegurar que apenas as pessoas ou sistemas autorizados possam fazer alterações na forma e no conteúdo de uma informação, ou que alterações causadas por acidentes ou defeitos de tecnologia não ocorram, assim como no ambiente no qual ela é armazenada e pela qual transita, ou seja, em todos os ativos.

Logo, para proteger a integridade, é preciso que todos os elementos que compõem a base da gestão da informação se mantenham em suas condições originais definidas por seus responsáveis e proprietários.

Em resumo: proteger a integridade é um dos principais objetivos para a segurança das informações de um indivíduo ou empresa

1 **Pilares da Segurança da Informação**

CONFIDENCIALIDADE

Informações críticas nem sempre são informações sigilosas.
Sigilo requer confidencialidade.

Alguns itens que necessitam de confidencialidade: dados pessoais, registro de fornecedores e clientes, estratégias de marketing, políticas financeiras.

A perda de confidencialidade acarreta em custos para a empresa: perda de sigilo, perda de clientes, perda de funcionários, perda de imagem pública, processos jurídicos e perda de faturamento.

O controle de confidencialidade deve ser focado nos direitos pessoais e na classificação das informações.

*Leia esta matéria sobre quebra de confidencialidade:
Dados de 24 mil Britânicos são violados*

Garantia de que a



1.4.3 - PRINCÍPIO DA CONFIDENCIALIDADE DA INFORMAÇÃO

O **princípio da confidencialidade** da informação tem como objetivo garantir que apenas a pessoa correta tenha acesso à informação.

As informações trocadas entre indivíduos e empresas nem sempre deverão ser conhecidas por todos. Muitas informações geradas pelas pessoas se destinam a um grupo específico de indivíduos e, muitas vezes, a uma única pessoa. Isso significa que esses dados deverão ser conhecidos apenas por um grupo controlado de pessoas, definido pelo responsável da informação

Por isso, dizemos que a informação possui um grau de confidencialidade que deverá ser mantido para que as pessoas não-autorizadas não tenham acesso a ela.

Ter confidencialidade na comunicação é ter a segurança de que o que foi dito a alguém ou escrito em algum lugar só será escutado ou lido por quem tiver autorização para tal.

Perda de confidencialidade significa perda de segredo. Se uma informação for confidencial, ela será secreta e deverá ser guardada com segurança, e não divulgada para pessoas não-autorizadas.

Exemplo:

Pensemos no caso de um cartão de crédito. O número do cartão só poderá ser conhecido por seu proprietário e pela loja onde é usado. Se esse número for descoberto por alguém mal-intencionado, como nos casos noticiados sobre crimes da Internet, o prejuízo causado pela perda de confidencialidade poderá ser muito elevado, pois esse número poderá ser

usado por alguém para fazer compras na Internet, trazendo prejuízos financeiros e uma grande dor de cabeça para o proprietário do cartão.

O mesmo ocorre no caso de uso indevido de senhas de acesso a sistemas bancários, por exemplo. Milhares de dólares são roubados diariamente pela ação de criminosos virtuais que se dedicam a invadir sistemas para quebrar a confidencialidade das pessoas e empresas.



Perguntas para pensar

- ☐ Você sabe quem pode ter acesso a suas informações?
- ☐ Elas estão guardadas de forma suficientemente segura para que pessoas não-autorizadas não tenham acesso a elas?
- ☐ O envio e o armazenamento de informações confidenciais são feitos de forma segura, e os meios pelos quais transitam são controlados, conhecidos e seguros?

Se a resposta para alguma dessas perguntas for negativa, então chegou o momento de pensar na segurança da informação para proteger a confidencialidade das informações na sua empresa.

PROTEGER A CONFIDENCIALIDADE DA INFORMAÇÃO

Proteger a confidencialidade é um dos fatores determinantes para a segurança e uma das tarefas mais difíceis de implementar, pois envolve todos os elementos que fazem parte da comunicação da informação, partindo do emissor, passando pelo caminho percorrido e chegando até o receptor. Além disso, informações tem diferentes graus de confidencialidade, normalmente relacionados ao seus valores. Quanto maior for o grau de confidencialidade, maior será o nível de segurança necessário na estrutura tecnológica e humana que participa desse processo: uso, acesso, trânsito e armazenamento das informações.

Deve-se considerar a confidencialidade com base no valor que a informação tem para a empresa ou a pessoa e os impactos causados por sua divulgação indevida. Assim, deve ser acessada, lida e alterada somente por aqueles indivíduos que possuem permissão para tal. O acesso deve ser considerado com base no grau de sigilo das informações, pois nem todas as informações importantes da empresa são confidenciais.

Como mencionado, o primeiro passo para proteger a confidencialidade das informações é através do estabelecimento do grau de sigilo. Vejamos a seguir esse conceito fundamental:



**Conceito-
chave**

Grau de sigilo: As informações geradas pelas pessoas têm uma finalidade específica e destinam-se a um indivíduo ou grupo. Portanto, elas precisam de uma classificação com relação à sua confidencialidade. É o que chamamos de grau de sigilo, que é uma graduação atribuída a cada tipo de informação com base no grupo de usuários que possuem permissões de acesso. O grau de sigilo faz parte de um importante processo de segurança de informações, a **classificação da informação**.

Dependendo do tipo de informação e do público para o qual se deseja colocar à disposição a informação, define-se um grau de sigilo. Um exemplo de graus de sigilo pode ser:

- ☐ Confidencial
- ☐ Restrito
- ☐ Sigiloso
- ☐ Público

DISPONIBILIDADE

A informação deve estar disponível no momento em que se precisa dela.

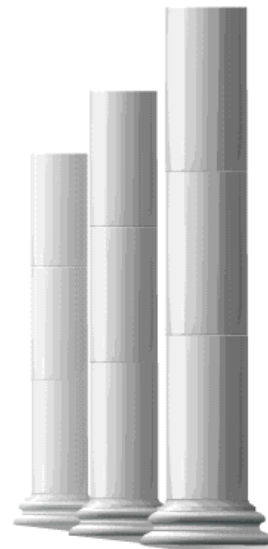
Os recursos tecnológicos devem manter as informações disponíveis aos usuários.

Os recursos tecnológicos devem ser mantidos em bom funcionamento e devem poder ser recuperados de maneira rápida e completamente, em caso de acidentes e desastres.

Hackers Brasileiros já contribuíram para tornar indisponível diversos sites no mundo. Veja a matéria: Brasileiros tentam invadir sites do Havaí.



Garantia que a informação será sempre

**1.4.4 - PRINCÍPIO DA DISPONIBILIDADE DAS INFORMAÇÕES**

Além de trabalharmos para que a informação chegue apenas aos destinatários ou usuários adequados e de forma íntegra, devemos fazer com que esteja disponível no momento oportuno. É disso que trata o terceiro princípio da segurança da informação: a disponibilidade

Para que uma informação possa ser utilizada, ela deve estar disponível. A disponibilidade é o terceiro princípio básico da segurança da informação.

Refere-se à disponibilidade da informação e de toda a estrutura física e tecnológica que permite o acesso, o trânsito e o armazenamento.

A disponibilidade da informação permite que:

- ☐ Seja utilizada quando necessário
- ☐ Esteja ao alcance de seus usuários e destinatários
- ☐ Possa ser acessada no momento em que for necessário utilizá-la.

Esse princípio está associado à adequada estruturação de um ambiente tecnológico e humano que permita a continuidade dos negócios da empresa ou das pessoas, sem impactos negativos para a utilização das informações.

Assim, o ambiente tecnológico e os suportes da informação deverão estar funcionando corretamente para que a informação armazenada neles e que por eles transita possa ser utilizada pelos usuários.

Exemplo:

- ☐ Durante uma reunião de altos executivos da empresa, os serviços de banco de dados falham, o que impede que se tome uma decisão central em termos de negócios.
- ☐ Devido a um incêndio em um dos escritórios, as informações de vendas da empresa foram destruídas e não se contava com um suporte para as mesmas



**Perguntas
para pensar**

A informação necessária para a tomada de decisões críticas para o negócio se encontra sempre disponível?
Você sabe se existem vulnerabilidades que impeçam isso?
Você conta com sistemas de suporte de informação?

PROTEGER A DISPONIBILIDADE DA INFORMAÇÃO

Para que seja possível proteger a disponibilidade da informação, é necessário conhecer seus usuários, para que se possa organizar e definir, conforme cada caso, as formas de disponibilização, seu acesso e uso quando necessário.

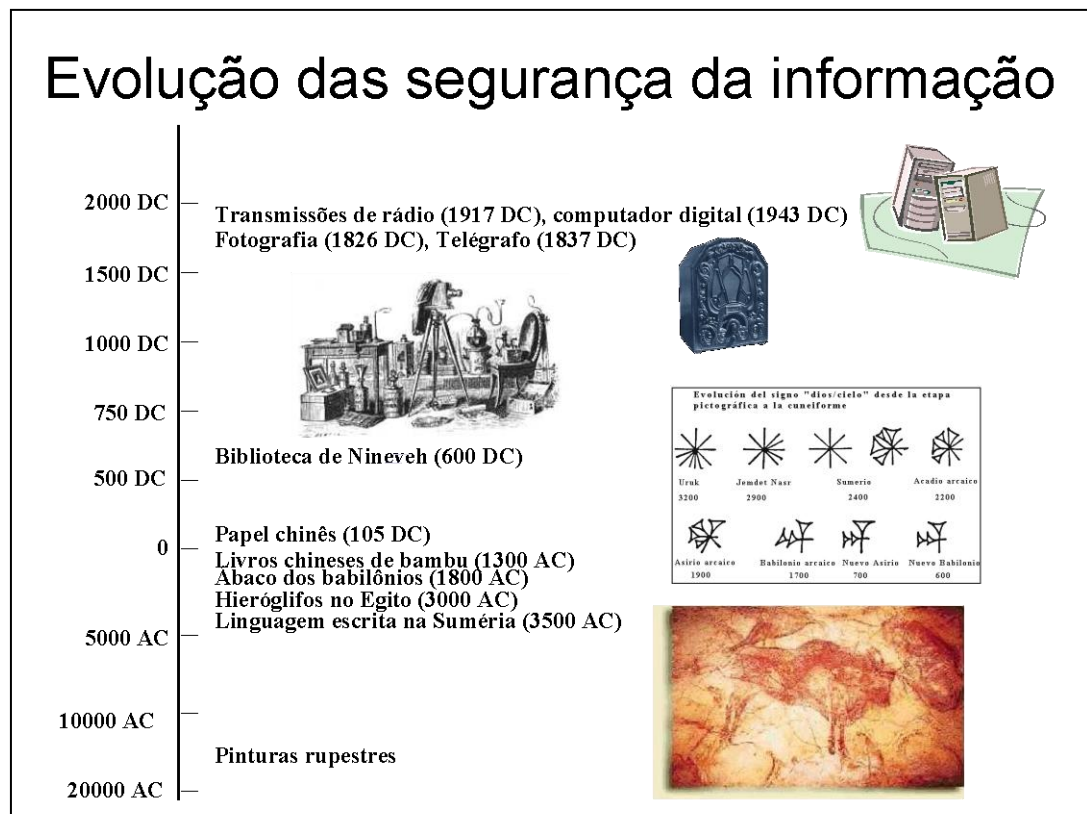
A disponibilidade da informação deve ser considerada com base no valor que a informação tem e no impacto resultante de sua falta de disponibilidade.

Para proteger a disponibilidade, muitas medidas são levadas em consideração. Entre elas, destacamos:

- ☐ A configuração segura de um ambiente em que todos os elementos que fazem parte da cadeia de comunicação estejam dispostos de forma adequada para assegurar o êxito da leitura, do trânsito e do armazenamento da informação.
- ☐ Também é importante fazer cópias de segurança – backup. Isso permite que as mesmas estejam duplicadas em outro local para uso caso não seja possível recuperá-las a partir de sua base original

Para aumentar ainda mais a disponibilidade da informação, deve-se:

- ☐ Definir estratégias para situações de contingência.
- ☐ Estabelecer rotas alternativas para o trânsito da informação, para garantir seu acesso e a continuidade dos negócios, inclusive quando alguns dos recursos tecnológicos, ou humanos, não estejam em perfeitas condições de funcionamento.



Desde a pré-história, cerca de 2000 anos antes de Cristo (AC), o homem já sentia necessidade de transmitir e perpetuar a informação. Usava pinturas nas pedras para expressar seu cotidiano. Em 3500 AC, registrou-se o primeiro sistema de linguagem escrita na Suméria. A partir daí várias civilizações desenvolveram seus próprios métodos de registro e transmissão da informação, dentre eles podemos destacar:

- Os hieróglifos e o papiro no antigo Egito, em 3000 AC;
- O ábaco dos babilônios, 1800 AC;
- Os primitivos livros chineses de bambu ou madeira presos por cordas datados de 1300 anos AC;
- O processo chinês de fabricação de papel, de 105 DC alcançando Bagdá em 753 DC;
- A fotografia de 1826;
- O telégrafo eletromagnético de Samuel Morse, em 1837;
- As primeiras transmissões de rádio em broadcast em 1917;
- O primeiro computador digital em 1943.

Todo este processo milenar nos levou até as modernas tecnologias de transmissão e armazenamento digital de dados no século 20 [2].

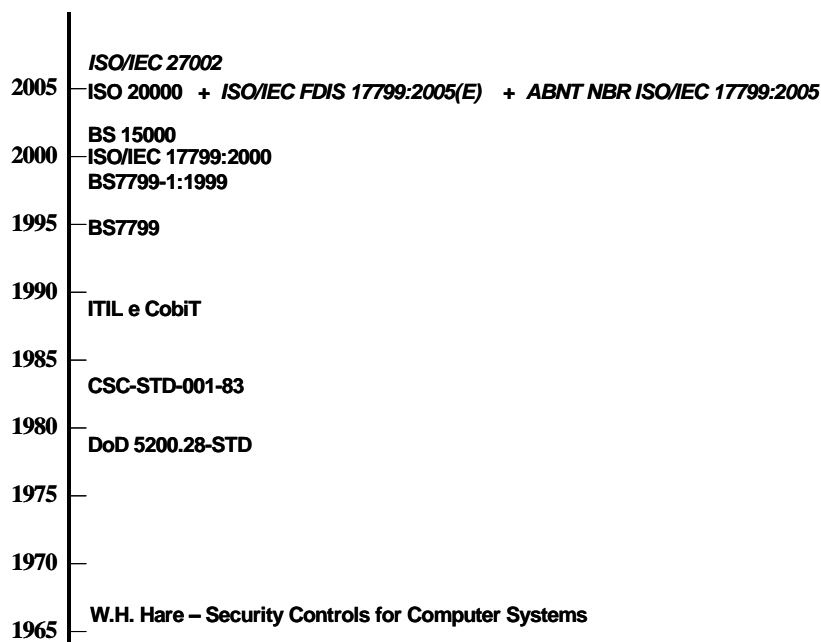
Todos aqueles métodos de armazenamento padeciam de um problema: como preservar essas informações para que fossem acessadas após sua geração? No ano 600 da era cristã o rei Ashurbanipal em Nineveh organizou a primeira biblioteca, cujo acervo sobrevive até os dias atuais com cerca de 20000 placas. É um exemplo clássico da necessidade da transmissão da informação armazenada.

Desde o início, o desafio era conter as diversas ameaças à informação, algumas das quais enfrentamos até hoje: incêndios, saques, catástrofes naturais, deterioração do meio de armazenamento.

À medida que a sociedade evoluía, a preocupação com a segurança das informações aumentava, principalmente no quesito confidencialidade. Foram criados vários processos de cifragem da informação, que tinham a função de alterar o conteúdo das mensagens antes de seu envio. Ao capturar uma mensagem o inimigo obtinha apenas um texto cifrado e não a mensagem original. Isso permitiu que segredos e estratégias fossem trocados de forma segura entre aliados. Por exemplo, a cifragem de César foi usada para troca de informações entre os exércitos durante o império romano; a máquina de cifrar “Enigma” foi utilizada como uma grande arma de guerra pelos alemães durante o período da segunda grande guerra. Atualmente a criptografia e a esteganografia continuam sendo largamente utilizadas em diversas aplicações de transferência e armazenamento de dados.

O surgimento dos computadores e de sua interconexão através de redes mundialmente distribuídas permitiu maior capacidade de processamento e de distribuição das informações. Com essa capacidade de comunicação, surgiu também a necessidade da criação de mecanismos que evitassem o acesso e a alteração indevida das informações. Como resultado surgiram várias propostas e publicações de normas de segurança em todo o mundo.

Evolução da segurança da informação



Conforme Chappman [3], o ano de 1967, foi o ano em que a segurança de computadores passou a ter atenção oficial nos Estados Unidos. Nesta época foi criada uma força tarefa cujo foco era a construção de mecanismos de segurança de computadores que deveriam ser desenvolvidos para prover a proteção de informações classificadas e do compartilhamento de recursos do sistema; este esforço resultou em um documento denominado *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security* editado por W. H. Ware [4]. Este relatório representou o trabalho inicial de identificação e tratamento do problema clássico de segurança de computadores.

Em 1978, o Departamento de Defesa dos Estados Unidos, publicou um conjunto de regras para avaliação da segurança nas soluções disponibilizadas. Ficou conhecido como “The Orange Book”. Em 1978, teve início o processo de escrita do Orange Book, denominado DoD 5200.28-STD, que foi concluído em 15 de agosto 1983, com o documento *CSC-STD-001-83 - Library No. S225,711 - DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC)* [5]. Paralelamente foi publicado o documento *An Introduction to Computer Security: The NIST Handbook* [6], proposto pelo National Institute of Standards and Technology - U.S. Department of Commerce.

Para facilitar sua aplicação, as normas de segurança foram divididas em vários controles. Cada controle seria responsável por atender a um dos quesitos da norma. O uso de controles permite uma visão modular da questão da segurança e a aplicação contextualizada das normas às organizações.

À medida que as organizações cresciam, as redes de computadores e os problemas de segurança também cresciam. Não demorou muito para ficar claro que proteger somente os sistemas operacionais, as redes e as informações que trafegavam por elas não era o suficiente. Com isto, foram criados comitês com o objetivo de desenvolver mecanismos mais eficientes e globais de proteção à informação. Desses pode-se destacar o Comercial Computer Security Centre, criado pelo governo britânico e que publicaria mais tarde a norma BS-7799.

A BS-7799 foi a primeira norma homologada a apresentar soluções para o tratamento da informação de uma maneira mais ampla. Segundo esta norma, todo tipo de informação deve ser protegido, independente da sua forma de armazenamento, seja analógica ou digital, e de seu valor para a organização. No ano de 2000, houve a homologação da primeira parte da BS-7799 pela ISO. Esta homologação originou a Norma Internacional de Segurança da Informação - ISO/IEC 17799, sendo composta por 10 macros controles, cada qual subdividido em controles específicos.

Em abril de 2001, a versão brasileira da norma ISO foi disponibilizada para consulta pública. Em setembro do mesmo ano a ABNT homologou a versão brasileira que passou a ser denominada NBR ISO/IEC 17799:2000. A Norma trouxe mais do que vários controles de segurança. Ela permitiu a criação de um mecanismo de certificação das organizações, através da BS 7799-2 e posteriormente através da ISO 27001.

Em 30 de setembro de 2005, passou a ter validade a segunda edição atualizada da norma brasileira. Foi publicada sob o número ABNT NBR ISO/IEC 17799:2005, que é equivalente à norma ISO/IEC 17799:2005, entrando em vigor a partir de novembro de 2005.

Uma família de normas está atualmente em desenvolvimento e adotará um esquema de numeração usando uma série de números 27000 em seqüência. Incluem normas sobre requisitos de sistemas de gestão da segurança da informação, gestão de riscos, métricas e medidas, e diretrizes para implementação, tais como [7]:

- ISO 27000 - Contém vocabulário e definições utilizados nas normas da série ISO 27000. Em desenvolvimento, tem sua publicação prevista para 2008 e deve absorver a ISO Guide 73 - Risk Management Vocabulary.
- ISO 27001 - publicada em outubro de 2005, substitui a BS7799-2, tornando-se a norma para certificação da segurança da informação. Nesta norma são organizados os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar o SGSI (Sistema de Gestão da Segurança da Informação, ou ISMS, Information Security Management System da sigla em inglês).
- ISO 27002 - organiza os controles de segurança da informação, reunindo as melhores práticas para a segurança da informação realizada mundialmente. Trata-se na realidade da ISO 17799:2005.
- ISO 27003 – Não oficialmente tratar-se-á de um guia de implementação.

- ISO 27004 - Information Security Management Metrics and Measurement, voltada para a medição da efetividade da implementação do SGSI e dos controles de segurança da informação implementados. Encontra-se em desenvolvimento e a sua publicação deverá ocorrer em 2007.
- ISO 27005 - Novo padrão para gerenciamento de riscos, deverá substituir a BS7799-3 em 2007. Reunirá diretriz e orientação para a identificação, avaliação, tratamento e gestão suportada dos riscos sobre os recursos do escopo compreendidos no SGSI.
- ISO 27006 - Este documento tem o título provisório de "Guidelines for information and communications technology disaster recovery services", baseada na SS507, padrão de Singapura para continuidade do negócio e recuperação de desastres. Ainda sem previsão para publicação.

Diversas iniciativas de organizações governamentais já aplicam normas específicas internas baseadas em normas internacionais e nacionais. No Brasil a política de segurança da Informação nos órgãos e nas entidades da administração pública federal é regulamentada através do Decreto Presidencial Nº 3.505, de 13 de junho de 2.000. Esse decreto enfatiza em seu artigo 3º inciso I, o seguinte objetivo:

“Dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis” [8].

Esse decreto representa a importância que as entidades devem dar à segurança da informação. Atendendo a esse decreto, diversos organismos governamentais desenvolvem seus códigos de boas práticas em segurança da informação que devem ser seguidos pelas pessoas que de alguma forma estão relacionadas com os ambientes informatizados.

Empresas privadas também se valem dos códigos de conduta propostos pelas normas, a fim de obterem a certificação de segurança da informação, garantindo relações de negócio com seus parceiros e clientes, em que a mútua confiança no sigilo da informação é imprescindível.

1.6 LIÇÕES APRENDIDAS

- ☐ Aprendemos ao longo deste capítulo os conceitos gerais que configuram a segurança da informação.
- ☐ Compreendemos a importância atual que tem para a empresa proteger a informação utilizada e que permite a realização de seus negócios.
- ☐ Conhecemos o que deve ser protegido em um sistema de segurança de informação: as informações, os equipamentos e sistemas que a utilizam ou oferecem suporte a ela e as pessoas que a utilizam.
- ☐ Aprendemos que a informação deve ter: integridade, confidencialidade e disponibilidade para que seja útil à organização.
- ☐ Conhecemos o caminho da Segurança da Informação desde a antiguidade até os dias de hoje.

ATIVOS

2.1 INTRODUÇÃO

Toda e qualquer informação, que seja um elemento essencial para os negócios de uma organização, deve ser preservada pelo período necessário, de acordo com sua importância. A informação é um bem como qualquer outro e por isso deve ser tratada como um “ativo”.

De forma mais genérica, os ativos são elementos que a segurança busca proteger. Os ativos possuem valor para as empresas e, como consequência, precisam receber uma proteção adequada para que seus negócios não sejam prejudicados.

Na visão de segurança da informação, são três os elementos que compõem o que chamamos de ativos:

- ☐ as informações;
- ☐ os equipamentos e sistemas que oferecem suporte a elas;
- ☐ as pessoas que as utilizam.

Neste capítulo revisaremos com um pouco mais de detalhes os diferentes tipos de ativos, identificando também algumas das diversas vulnerabilidades que podem afetá-los.



NOTÍCIAS PELO MUNDO

“Você sabia que 94% das empresas que perdem seus dados desaparecem? *

Segundo um estudo realizado pela Universidade do Texas, apenas 6% das empresas que sofrem um desastre informático sobrevivem. Os demais 94% desaparecem, mais cedo ou mais tarde. Pesquisas do Gartner Group, ainda que mais moderadas, confirmam essa tendência ao indicar que duas de cada cinco empresas que enfrentam grandes ataques ou danos em seus sistemas deixam de existir

É por isso que a Hitachi Data Systems assegura que o mercado de armazenamento de dados crescerá cerca de 12% ao ano no Chile até 2008.

Enrique Mosiejko, diretor regional da América Latina Sul da Hitachi Data Systems (HDS), explica que “os dados de uma empresa podem desaparecer ou sofrer danos de muitas formas. Devido a má administração da informação, erros humanos, vírus, hackers, ataques terroristas ou até mesmo desastres naturais. No Chile, por exemplo, os terremotos e as inundações são uma séria ameaça para os equipamentos que armazenam a informação crítica das empresas.”

Como se pode observar na notícia, é importante conhecer os ativos da empresa e detectar suas vulnerabilidades para proteger a confidencialidade, a disponibilidade e a integridade da informação. É por isso que, neste capítulo, abordaremos esses temas.

*Fonte: http://www.mundoonline.cl/noticia.php?noticia_id=638&categoria_id=35

2.2 OBJETIVOS



- ☐ Conhecer os diferentes tipos de ativos na empresa para identificar tudo aquilo que a segurança da informação deveria proteger.
- ☐ Detectar possíveis vulnerabilidades relacionadas com esses ativos para nos prepararmos para sua proteção.



2.3 TIPOS DE ATIVOS

Os ativos são elementos que a segurança busca proteger. Os ativos possuem valor para as empresas e, como consequência, precisam receber uma proteção adequada para que seus negócios não sejam prejudicados.

São três os elementos que compõem o que chamamos de ativos:

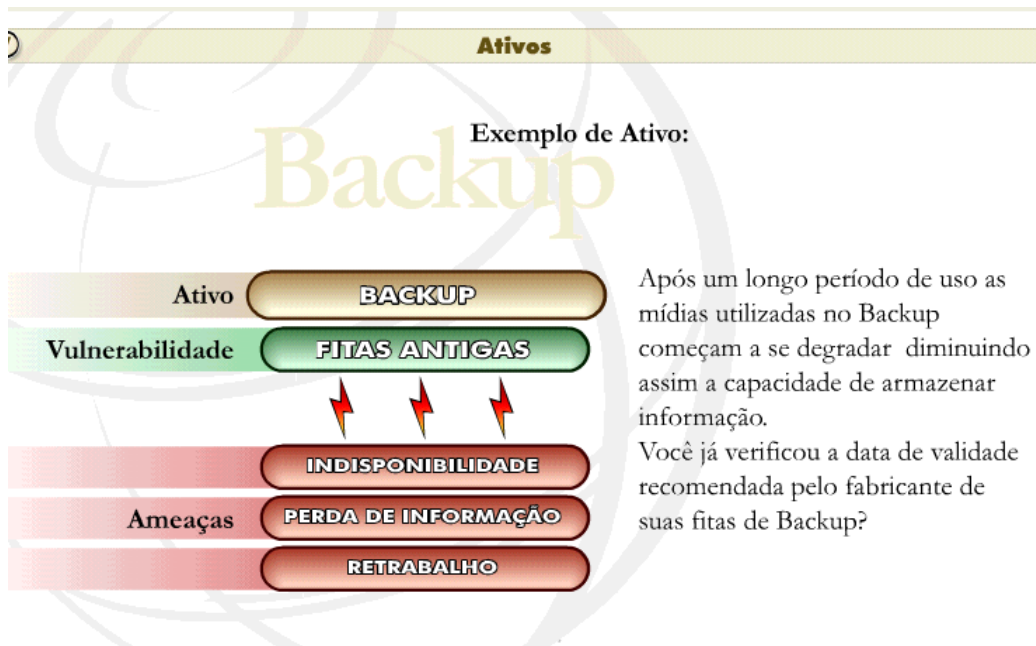
- ☐ as informações;
- ☐ os equipamentos e sistemas que oferecem suporte a elas;
- ☐ as pessoas que as utilizam.

Revisaremos com um pouco mais de detalhes os diferentes tipos de ativos. Para isso, consideramos esta classificação:

a. Informações	
b. Os equipamentos e sistemas que oferecem suporte a elas:	b.1 Software b.2 Hardware b.3 Organização
c. Pessoas que as utilizam ou usuários:	



Um ativo é todo elemento que manipula a informação, inclusive ela mesma, passando pelo seu emissor, o meio pelo qual ela é transmitida ou armazenada, até chegar a seu receptor.



2.3.1 - INFORMAÇÕES

Neste grupo estão os elementos que contêm informação registrada, em meio eletrônico ou físico. Qualquer tipo de informação, independente do tipo de meio em que esteja armazenada, que seja importante para a empresa e seus negócios. Cultura é importante, exemplos desses ativos são:

- ☐ documentos
- ☐ relatórios
- ☐ livros
- ☐ manuais
- ☐ correspondências
- ☐ patentes
- ☐ informações de mercado
- ☐ código de programação
- ☐ linhas de comando
- ☐ arquivos de configuração
- ☐ planilhas de remuneração de funcionários
- ☐ plano de negócios de uma empresa etc.



Possíveis vulnerabilidades

Documentos abandonados em locais públicos, informações publicadas em sistemas sem proteção de acesso, correspondência em envelope não lacrado.



2.3.2 - SOFTWARE (B1)

Este grupo de ativos contém todos os programas de computador utilizados para a automatização de processos, isto é, acesso, leitura, trânsito, armazenamento e processamento das informações. Dentre eles citamos:

- ☐ os aplicativos comerciais
- ☐ programas institucionais
- ☐ sistemas operacionais

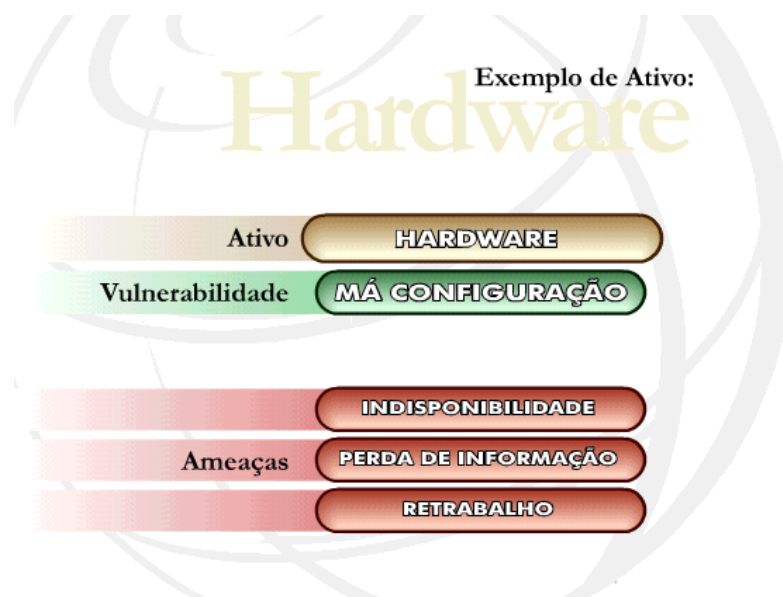
A segurança da informação busca avaliar a forma em que as aplicações são criadas, como são colocadas à disposição e como são utilizadas pelos usuários e pelos demais sistemas para detectar e corrigir problemas existentes na comunicação entre eles.

Os aplicativos deverão estar seguros para que a comunicação entre os bancos de dados, outros aplicativos e os usuários ocorra de forma segura, atendendo aos princípios básicos da segurança da informação, a confidencialidade, a integridade e a disponibilidade

São exemplos desse tipo de ativo os sistemas operacionais (Unix, Windows, Linux, etc.), sistemas informatizados, aplicativos específicos, programas de correio eletrônico e sistemas de suporte, entre outros.



Falhas conhecidas e não reparadas que podem ser exploradas para permitir acessos não autorizados aos computadores. Sistema de autenticação por senha que permite o uso de senhas em branco.



2.3.2 - HARDWARE (B2)

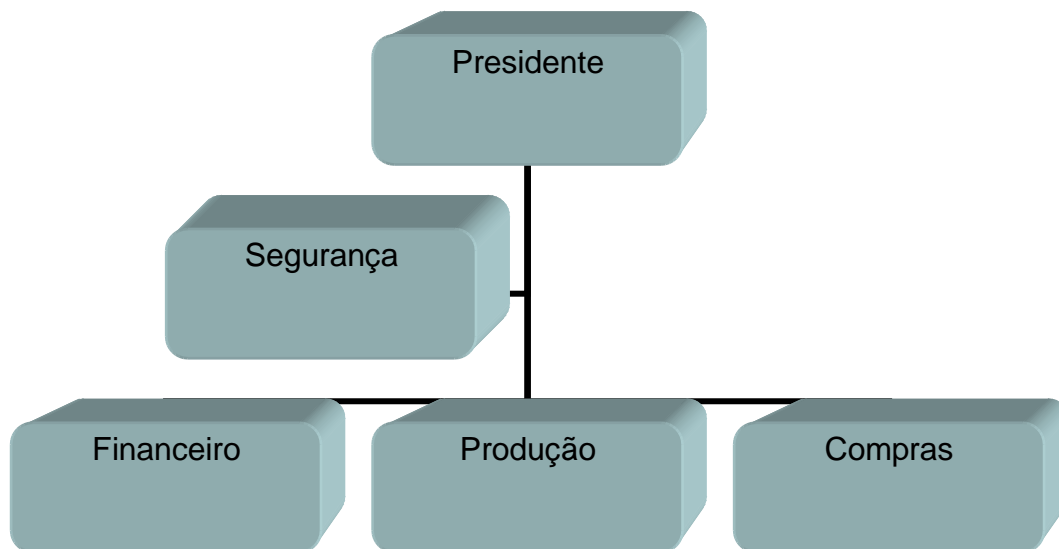
Esses ativos representam toda a infra-estrutura tecnológica que oferece suporte à informação durante seu uso, trânsito, processamento e armazenamento. Faz parte desse grupo qualquer equipamento no qual se armazene, processe ou transmita as informações da empresa:

- ☐ as estações de trabalho
- ☐ os servidores
- ☐ os computadores portáteis
- ☐ os mainframes
- ☐ as mídias de armazenamento



Possíveis
vulnerabilidades

Infra-estrutura elétrica sujeita a falhas que danifiquem os equipamentos, centros de computação sujeitos a inundações, computadores portáteis sem vigilância em locais públicos.



2.3.2 - ORGANIZAÇÃO (B3)

Neste grupo, estão incluídos os aspectos que compõem a estrutura física e organizacional das empresas. Refere-se à organização lógica e física do pessoal dentro da empresa em questão. Como exemplos de estrutura organizacional, temos, entre outros:

- ☐ a estrutura departamental e funcional
- ☐ o quadro de alocação dos funcionários
- ☐ a distribuição de funções e os fluxos de informação da empresa os servidores

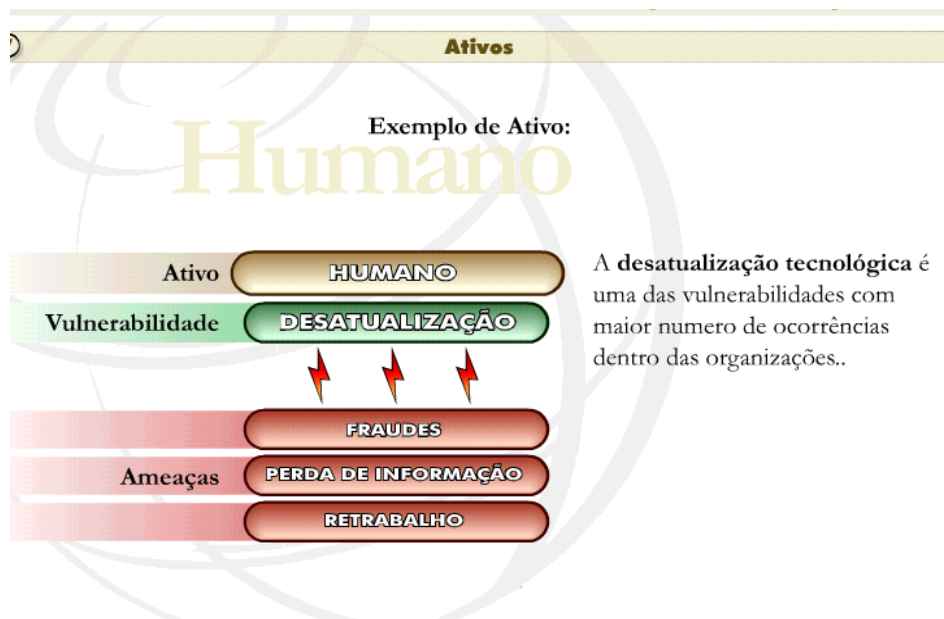
Em relação ao ambiente físico, entre outros, são considerados:

- ☐ salas e armários onde estão localizados os documentos, fototeca, sala de servidores de arquivos



Possíveis vulnerabilidades

- ☐ Localização insegura de documentos, equipamentos ou pessoas.
- ☐ Estrutura organizacional que não permita mudanças em termos de segurança.
- ☐ Ausência de equipe dedicada de segurança.



2.4 - USUÁRIOS

O grupo usuários refere-se aos indivíduos que utilizam a estrutura tecnológica e de comunicação da empresa e que lidam com a informação.

O enfoque da segurança nos usuários está voltado para a formação do hábito da segurança em todos os funcionários de uma empresa para tomar decisões e empreender ações, desde a alta direção até os usuários finais da informação, incluindo os grupos que mantêm em funcionamento a estrutura tecnológica, como técnicos, operadores e administradores de ambientes tecnológicos.

São exemplos deste tipo de ativo:

- ☐ Funcionários da área de contabilidade.
- ☐ Direção da empresa



Possíveis vulnerabilidades

- ☐ Desconhecimento dos métodos de escolha de senhas fortes.
- ☐ Resistência de funcionários a adotar práticas de segurança.
- ☐ Descuido por parte dos usuários na manipulação da informação.

2.6 - LIÇÕES APRENDIDAS

- ☐ Este capítulo permitiu conhecer vários conceitos novos de segurança da informação, o que permitirá acelerar nosso processo rumo à criação de uma política de segurança.
- ☐ Categorizamos os diferentes tipos de ativos na empresa e identificamos possíveis vulnerabilidades. Isso ajudará a saber em quais ativos deve-se dedicar mais atenção em matéria de segurança.

AMEAÇAS E PONTOS FRACOS

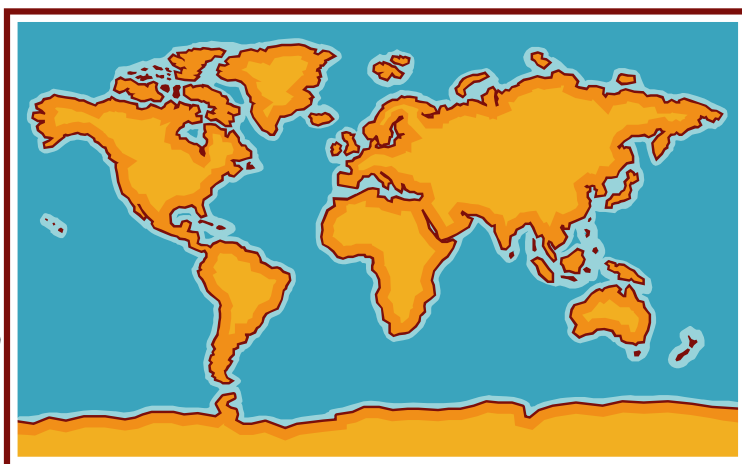
3.1 INTRODUÇÃO

No capítulo anterior conhecemos os ativos que devemos proteger através de medidas de segurança da informação. Para cada um dos grupos apresentados foram identificadas vulnerabilidades.

Vulnerabilidades não seriam um problema se não houvesse elementos capazes de explorá-las, causando danos. Estes elementos são conhecidos como Ameaças.

Neste capítulo conheceremos os diversos tipos de Ameaças que podem causar danos aos ativos, assim como suas diferentes classificações.

Também serão conhecidos os tipos de Vulnerabilidades e pontos fracos existentes nos ativos de uma empresa.



NOTÍCIAS PELO MUNDO

A Atos Origin, parceira tecnológica mundial do Comitê Olímpico Internacional (COI), anunciou em Londres, no dia 17 de setembro de 2004, que a solução de segurança implementada na infra-estrutura tecnológica dos Jogos Olímpicos de Atenas 2004 conseguiu resolver sem problemas os ataques de vírus e hackers ocorridos durante o evento, garantindo a não-interrupção das transmissões e uma retransmissão precisa e em tempo real dos resultados tanto para os meios de comunicação para o resto do mundo. Durante os 16 dias que durou a competição, foram registrados mais de cinco milhões de alertas de segurança nos sistemas de informação dos Jogos, dos quais 425 foram graves e 20, críticos. Entre os invasores, encontravam-se pessoas autorizadas que pretendiam desconectar o sistema INFO 2004 – a Intranet dos Jogos Olímpicos, que oferecia os resultados e o calendário de provas, além de informações sobre os atletas –, com a finalidade de conectar os computadores portáteis para obter acesso à Internet. A equipe responsável conseguiu oferecer uma resposta rápida a todos esses alertas e evitar acessos não-autorizados.

“Devido ao enorme aumento no número de ataques e vírus de computador dos últimos anos, a Atos Origin transformou a segurança tecnológica em sua prioridade máxima, melhorando-a de forma significativa em relação à de Salt Lake City”, afirma o diretor de tecnologia do COI, Philippe Verveer. “A Atos Origin gerenciou de forma eficiente e eficaz o grande número de alertas de segurança registrados durante os Jogos, garantindo que sua infra-estrutura tecnológica não fosse afetada.”

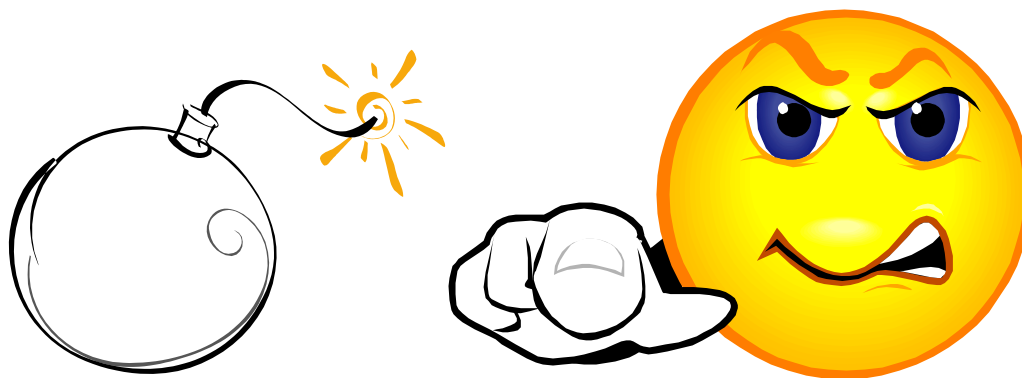
Fonte: http://www.sema.es/noticia_extendida_home.asp?id=64

A notícia apresentada nos leva a confirmar que conhecer perfeitamente as possíveis ameaças e riscos aos quais se encontram expostos nossos ativos permite que nosso trabalho possa se transformar em um caso de sucesso. Neste capítulo, vamos examinar o que se refere a ameaças e pontos fracos.

3.2 - OBJETIVOS



- ☐ Conhecer os diferentes tipos de ameaças que podem aparecer em todos os ativos da empresa para reconhecer sua importância e nos permitir minimizar o impacto que geram.
- ☐ Identificar os diferentes tipos de vulnerabilidades dos ativos e saber como eles podem permitir que as ameaças alterem a disponibilidade, a confidencialidade ou a integridade das informações.



3.3 - AS AMEAÇAS



Conceito-chave

As ameaças são causa potencial de um incidente indesejado, que caso se concretize pode resultar em dano. Ameaças exploram as falhas de segurança, que denominamos pontos fracos, e, como consequência, provocam perdas ou danos aos ativos de uma empresa, afetando os seus negócios.

Os ativos estão constantemente sob ameaças que podem colocar em risco a integridade, a confidencialidade e a disponibilidade das informações. Essas ameaças sempre existirão e estão relacionadas a causas que representam riscos, as quais podem ser:

- ☐ causas naturais ou não-naturais
- ☐ causas internas ou externas

Dessa forma, entendemos que um dos objetivos da segurança da informação é impedir que as ameaças explorem os pontos fracos e afetem um dos princípios básicos da segurança da informação (integridade, disponibilidade, confidencialidade), provocando danos ao negócio das empresas.

Dados a importância das ameaças e o impacto que elas pode ter para as informações das organizações, vamos revisar agora a sua classificação.

As ameaças são constantes e podem ocorrer a qualquer momento. Essa relação de frequência-tempo se baseia no conceito de risco, o qual representa a probabilidade de que uma ameaça se concretize por meio de uma vulnerabilidade ou ponto fraco. Elas podem se dividir em três grandes grupos:

1. **Ameaças naturais** – condições da natureza e a intempérie que poderão provocar danos nos ativos, tais como fogo, inundação, terremotos.
2. **Intencionais** – são ameaças deliberadas, fraudes, vandalismo, sabotagens, espionagem, invasões e furtos de informações, entre outros.
3. **Involuntárias** – são ameaças resultantes de ações inconscientes de usuários, por vírus eletrônicos, muitas vezes causados pela falta de conhecimento no uso dos ativos, tais como erros e acidentes.

Entre as principais ameaças, a ocorrência de vírus, a divulgação de senhas e a ação de hackers estão entre as mais frequentes.

Com a importância estratégica que vem conquistando as tecnologias da informação, os prejuízos com as invasões e incidentes na Internet provocam a cada ano um impacto mais profundo nos negócios das empresas brasileiras.

O mercado está mais atento aos novos perigos que resultam da presença e do uso da Internet. Sete de cada dez executivos entrevistados acreditam que haverá um aumento no número de problemas de segurança em 2000; 93% reconhecem a grande importância da proteção dos dados para o sucesso do negócio, sendo que 39% a consideram vital para o ambiente corporativo.

O controle daquilo que ocorre nas redes corporativas foi um dos pontos mais fracos nas empresas brasileiras. Destacamos os seguintes fatores críticos detectados pela pesquisa a ser analisada a seguir:

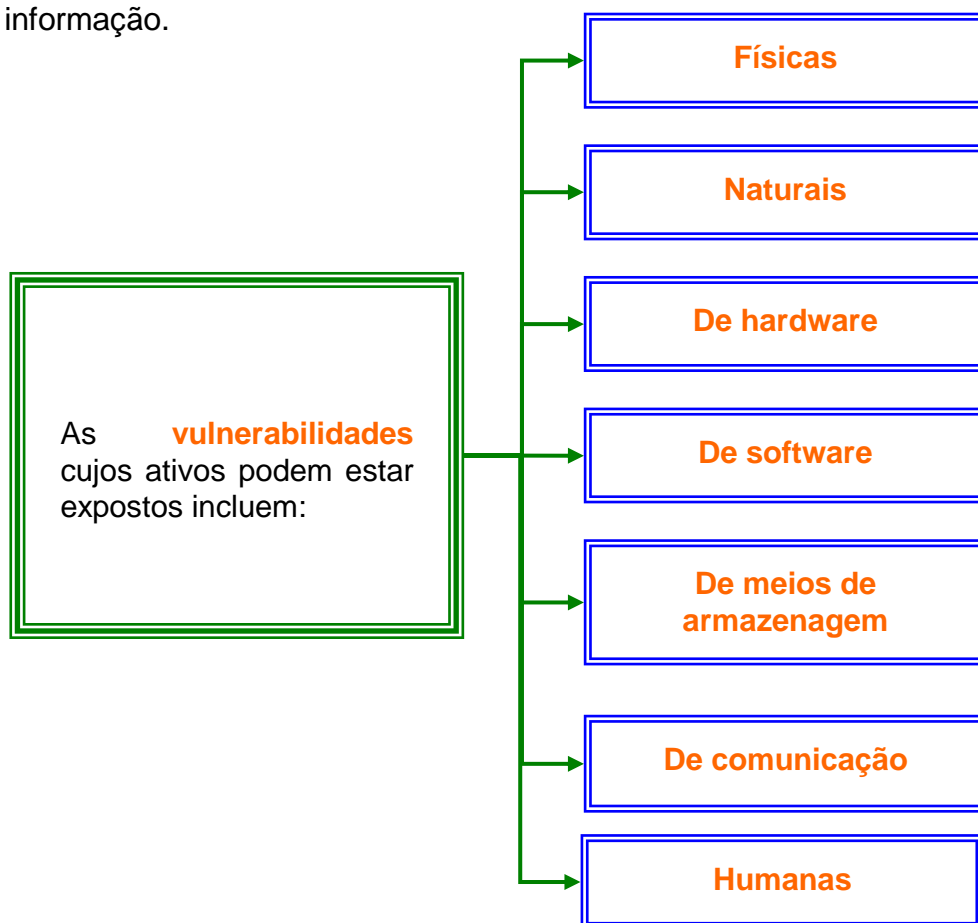


- ☐ Somente 27% afirmam nunca ter sofrido algum tipo de ataque.
- ☐ Cerca de 41% nem sequer sabem que foram invadidos, revelando o grande risco que as organizações correm em não conhecer os pontos fracos da intranet.
- ☐ Para 85% das empresas, não foi possível quantificar as perdas causadas por invasões ou contingências ocorridas.
- ☐ O acesso à Internet por modem é permitido em 38% das empresas. Este é um grande perigo indicado pela pesquisa, já que as empresas não destacaram a utilização de medidas de segurança para esse uso.
- ☐ Setenta e cinco por cento das empresas mencionam que os vírus são a maior ameaça à segurança da informação nas empresas. Embora 93% das corporações afirmem ter adotado sistemas de prevenção contra vírus, 48% viram seus sistemas contaminados nos últimos seis meses e apenas 11% das empresas entrevistadas declaram nunca ter sido infectadas.
- ☐ A divulgação de senhas foi indicada como a segunda maior ameaça à segurança, sendo mencionada por 57% das empresas. Os hackers, tradicionalmente os maiores vilões da Internet, aparecem em terceiro lugar (44%), e os funcionários insatisfeitos (42%) em quarto lugar.



3.4 - VULNERABILIDADES

As ameaças sempre existiram e é de se esperar que, à medida que a tecnologia progride, também surjam novas formas através das quais as informações podem ficar expostas; portanto, é importante conhecer a estrutura geral de como se classificam as vulnerabilidades ou pontos fracos que podem fazer com que essas ameaças causem menos impactos em nossos sistemas, comprometendo os princípios da segurança da informação.



As vulnerabilidades são os elementos que, ao serem explorados por ameaças, afetam a confidencialidade, a disponibilidade e a integridade das informações de um indivíduo ou empresa. Um dos primeiros passos para a implementação da segurança é rastrear e eliminar os pontos fracos de um ambiente de tecnologia da informação.

Ao se identificarem as vulnerabilidades ou pontos fracos, será possível dimensionar os riscos aos quais o ambiente está exposto e definir as medidas de segurança apropriadas para sua correção.

As vulnerabilidades dependem da forma como se organizou o ambiente em que se gerenciam as informações. A existência de vulnerabilidades está relacionada à presença de elementos que prejudicam o uso adequado da informação e da mídia que ela está utilizando.

Podemos compreender agora outro objetivo da segurança da informação: a correção de vulnerabilidades ou pontos fracos existentes no ambiente em que se usa a informação, com o objetivo de reduzir os riscos a que ela está submetida, evitando, assim, a concretização de uma ameaça.

Agora aprofundaremos um pouco mais a descrição de cada um desses tipos de vulnerabilidades:

a) Vulnerabilidades físicas



Físicas

Exemplo:

Os pontos fracos de ordem física são aqueles presentes nos ambientes em que estão sendo armazenadas ou gerenciadas as informações.

Como exemplo desse tipo de vulnerabilidade distinguem-se os seguintes: instalações inadequadas do espaço de trabalho, ausência de recursos para o combate a incêndios; disposição desorganizada dos cabos de energia e de rede, não-identificação de pessoas e de locais, entre outros.

Esses pontos fracos, ao serem explorados por ameaças, afetam diretamente os princípios básicos da segurança da informação, principalmente a disponibilidade.

b) Vulnerabilidades naturais



Naturais

Os pontos fracos naturais são aqueles relacionados às condições da natureza que podem colocar em risco as informações.

Exemplo:

Entre as ameaças naturais mais comuns, podemos citar:

- ☐ ambientes sem proteção contra incêndios,
- ☐ locais próximos a rios propensos a inundações,
- ☐ infra-estrutura incapaz de resistir às manifestações da natureza, como terremotos, maremotos, furacões, etc.

Muitas vezes, a umidade, o pó e a contaminação podem provocar danos aos ativos. Por isso, eles devem ficar protegidos para poder garantir suas funções.

A probabilidade de estar expostos às ameaças naturais é fundamental na escolha e na preparação de um ambiente. Devem ser tomados cuidados especiais com o local, de acordo com o tipo de ameaça natural que possa ocorrer em uma determinada região geográfica.

c) Vulnerabilidades de hardware



Os possíveis defeitos de fabricação ou configuração dos equipamentos da empresa que poderiam permitir o ataque ou a alteração dos mesmos.

De hardware

Exemplo:

- ☐ A falta de configuração de suportes ou equipamentos de contingência poderia representar uma vulnerabilidade para os sistemas da empresa.

Existem muitos elementos que representam pontos fracos do hardware. Dentre eles, podemos mencionar:

- ☐ a ausência de atualizações de acordo com as orientações dos fabricantes dos programas utilizados e
- ☐ a conservação inadequada dos equipamentos.
- ☐ Por isso, a segurança da informação busca avaliar:
 - ☐ se o hardware utilizado está dimensionado corretamente para as suas funções.
 - ☐ se possui área de armazenamento suficiente, processamento e velocidade adequados.

d) Vulnerabilidades de softwares



Os pontos fracos dos aplicativos permitem que ocorram acessos indevidos aos sistemas de computador, inclusive sem o conhecimento de um usuário ou administrador de rede.

De software

Exemplo:

- ☐ Programas de email que permitem a execução de códigos maliciosos, editores de texto que permitem a execução de vírus de macro, etc. – esses pontos fracos colocam em risco a segurança dos ambientes tecnológicos.
- ☐ Também poderão ter pontos fracos os programas utilizados para edição de texto e imagem, para a automatização de processos e os que permitem a leitura das informações de uma pessoa ou empresa, como os navegadores de páginas da Internet.
- ☐ Esses aplicativos são vulneráveis a várias ações que afetam sua segurança, como, por exemplo, a configuração e a instalação inadequadas, a ausência de atualizações, programação insegura, etc.

Os pontos fracos relacionados ao software poderão ser explorados por diversas ameaças já conhecidas.

Dentre eles, destacamos:

- ☐ A configuração e a instalação indevidas dos programas de computador, que poderão levar ao uso abusivo dos recursos por parte de usuários mal-intencionados. Às vezes, a liberdade de uso implica aumento do risco.

- ☐ Os aplicativos são os elementos que fazem a leitura das informações e que permitem que os usuários acessem determinados dados em mídia eletrônica e, por isso, se transformam no objetivo preferido dos agentes causadores de ameaças.
- ☐ Os sistemas operacionais, como Microsoft® Windows® e Unix®, que oferecem a interface para configuração e organização de um ambiente tecnológico. Esses são o alvo dos ataques, pois, através deles, será possível realizar qualquer alteração na estrutura de um computador ou rede.

e) Vulnerabilidades dos meios de armazenamento

Os meios de armazenamento são os suportes físicos ou magnéticos utilizados para armazenar as informações.

Entre os tipos de suporte ou meios de armazenamento das informações que estão expostos, podemos citar os seguintes:

- ☐ disquetes
- ☐ CD-ROMs
- ☐ fitas magnéticas
- ☐ discos rígidos dos servidores e dos bancos de dados, bem como o que está registrado em papel.

Portanto...



**De meios de
armazenamento**

Exemplos

Se os suportes que armazenam as informações não forem utilizados de forma adequada, seu conteúdo poderá estar vulnerável a uma série de fatores que poderão afetar a integridade, a disponibilidade e a confidencialidade das informações.

Os meios de armazenamento podem ser afetados por pontos fracos que podem danificá-los ou deixá-los indisponíveis. Dentre os pontos fracos, destacamos os seguintes:

- ☐ prazo de validade e expiração
- ☐ defeito de fabricação
- ☐ uso incorreto
- ☐ local de armazenamento em locais insalubres ou com alto nível de umidade, magnetismo ou estática, mofo, etc.

f) Vulnerabilidades de comunicação



De comunicação

Esse tipo de ponto fraco abrange todo o tráfego de informações.

Onde quer que transitem as informações, seja por cabo, satélite, fibra óptica ou ondas de rádio, deve existir segurança. O sucesso no tráfego dos dados é um aspecto fundamental para a implementação da segurança da informação.

Exemplos

- ☐ A ausência de sistemas de criptografia nas comunicações poderia permitir que pessoas alheias à organização obtivessem informações privilegiadas.
- ☐ A má escolha dos sistemas de comunicação para envio de mensagens de alta prioridade da empresa poderia fazer com que elas não alcançassem o destino esperado ou que a mensagem fosse interceptada no meio do caminho.

Há um grande intercâmbio de dados através dos meios de comunicação que rompem as barreiras físicas, como telefone, Internet, WAP, fax, telex, etc.

Dessa forma, esses meios deverão receber tratamento de segurança adequado com o propósito de evitar que:

- ☐ Qualquer falha na comunicação faça com que uma informação fique indisponível para os seus usuários, ou, pelo contrário, fique disponível para quem não possua direitos de acesso.
- ☐ As informações sejam alteradas em seu estado original, afetando sua integridade.

Assim, a segurança da informação também está associada ao desempenho dos equipamentos envolvidos na comunicação, pois se preocupa com: a qualidade do ambiente que foi preparado para o tráfego, tratamento, armazenamento e leitura das informações.

g) Vulnerabilidades humanas



Essa categoria de vulnerabilidade relaciona-se aos danos que as pessoas podem causar às informações e ao ambiente tecnológico que lhes oferece suporte.

Humanas

Exemplo

Senhas fracas, falta de uso de criptografia na comunicação, compartilhamento de identificadores como nome de usuário ou credencial de acesso, entre outros.

Os pontos fracos humanos também podem ser intencionais ou não. Muitas vezes, os erros e acidentes que ameaçam a segurança da informação ocorrem em ambientes institucionais. A maior vulnerabilidade é o desconhecimento das medidas de segurança adequadas que são adotadas por cada elemento do sistema, principalmente os membros internos da empresa.

A seguir são destacados os pontos fracos humanos de acordo com seu grau de frequência:

- ☐ a falta de capacitação específica para a execução das atividades inerentes às funções de cada um,
- ☐ a falta de consciência de segurança para as atividades de rotina, os erros, omissões, descontentamentos, etc.

No que se refere às vulnerabilidades humanas de origem externa, podemos considerar todas aquelas que podem ser exploradas por ameaças como:

- ☐ vandalismo,
- ☐ fraudes,
- ☐ invasões, etc.

3.5 - LIÇÕES APRENDIDAS

- ☐ Este capítulo nos forneceu a oportunidade de saber que as ameaças podem ser divididas em três grandes grupos: naturais, involuntárias e intencionais.
- ☐ Além disso, aprendemos que as ameaças não provêm unicamente de pessoas alheias à empresa, podendo vir também de eventos naturais ou de erros humanos. Isso incrementa nosso panorama em torno da segurança.
- ☐ Identificamos algumas categorias dos diferentes pontos fracos ou vulnerabilidades que é possível encontrar nos ativos da empresa.
- ☐ Reconhecemos alguns exemplos dos pontos fracos e vulnerabilidades existentes em elementos físicos, humanos, de comunicação, entre outros. Isso nos permitiu ter uma idéia muito mais clara dos riscos que nossa empresa enfrenta.

RISCOS, MEDIDAS E CICLO DE SEGURANÇA

4.1 INTRODUÇÃO

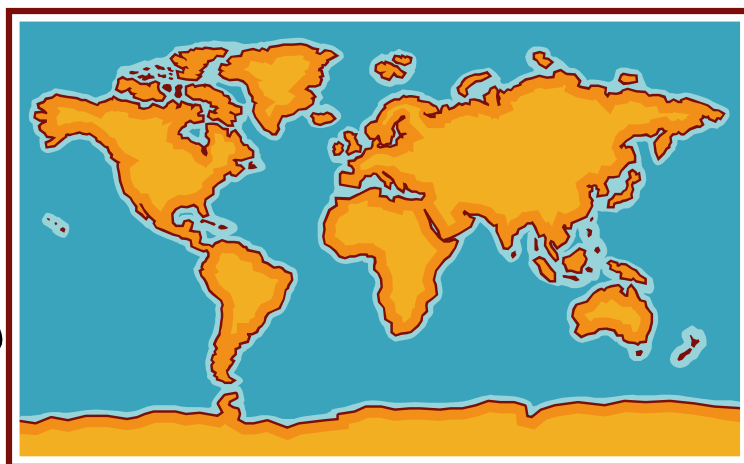
Segundo Thomas A. Wadlow [⁹], “A segurança deverá ser proporcional ao valor do que se está protegendo”. Ou seja, a implantação do sistema de segurança da informação tem de apresentar uma relação custo benefício que torne a tentativa de ataque tão cara que desestimule o atacante, ao mesmo tempo em que ela é mais barata do que o valor da informação protegida.

Quando o valor do ativo que se está protegendo é tão alto que o dano causado ao mesmo é difícil de ser calculado, devemos assumir o valor da informação como altíssimo, imensurável. Um exemplo a se analisar seria um receituário de medicamentos para pacientes internados em um hospital. Este sistema de informação lida com dados que podem colocar em risco a vida humana caso a integridade dos dados seja corrompida, neste caso não temos como fazer uma análise quantitativa do impacto, pois a vida humana é tida como mais valiosa que qualquer ativo.

Mesmo não se tratando de um valor imensurável, temos ainda os ativos que são vitais para a empresa e aqueles que podem levar a implicações legais. Quando estamos lidando com a análise de valor destes bens, consideramos que o dano nos mesmos pode resultar em grande perda de credibilidade pela empresa e até mesmo no posterior encerramento de suas atividades.

Neste contexto, a segurança da informação é a proteção da informação em si, dos sistemas, da infra-estrutura e dos serviços que a suporta, contra acidentes, roubos, erros de manipulação, minimizando assim os impactos dos incidentes de segurança.

A identificação da real necessidade de proteção de cada ativo é baseada no conceito de **Risco**, que é apresentado neste capítulo. Uma vez identificados os maiores riscos às informações, serão implementadas medidas de segurança, cuja definição e classificação também fazem parte deste capítulo. A constante avaliação de risco e implementação de medidas de segurança fazem parte do ciclo de segurança, que fecha o conjunto de assuntos tratados neste módulo.



NOTÍCIAS PELO MUNDO

Especialistas em segurança informática reunidos em Kuala Lumpur, na Malásia, explicaram que problemas identificados em determinados softwares poderiam permitir controlar o telefone de forma remota, ler a agenda dos diretores ou escutar secretamente uma conversa. Advertiram que a última geração de telefones móveis é vulnerável a ataques de hackers, segundo informou o site de notícias da BBC.

Os participantes da conferência "Hack in the Box", realizada na capital da Malásia, foram testemunhas de uma demonstração dos defeitos de segurança encontrados no Java 2 Micro Edition ou J2ME, software desenvolvido em conjunto pela Sun Microsystems, Nokia, Sony Ericsson e Motorola.

A vulnerabilidade do software, que vem incluído em telefones "inteligentes" fabricados por essas empresas, está relacionada com a maneira usada pela linguagem Java para tentar evitar que o sistema operacional aceite ordens do exterior, ressaltou um porta-voz.

"A nova geração de telefones, na verdade, vem com um software muito mais poderoso dentro do sistema operacional", defendeu Dylan Andrew, o organizador do encontro. "Encontramos novos ataques que afetam essas novas plataformas, permitindo que o invasor, por exemplo, controle o telefone celular de forma remota, podendo até mesmo ler a agenda dos diretores ou escutar secretamente uma conversa", acrescentou.

No entanto, o diretor de segurança sem-fio da empresa McAfee, esclareceu que o risco, embora exista, ainda é mínimo.

Fonte: <http://www.laflecha.net/canales/seguridad/200410061/>

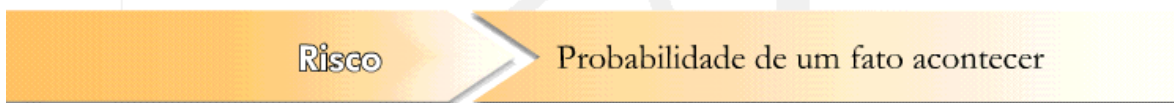
Notícias como essa são comuns no mundo de hoje. Todos os dias ficamos sabendo de possíveis riscos em diferentes dispositivos ou sistemas de gestão de informação. Para poder evitar esses riscos, é necessário conhecê-los bem, além de conhecer as medidas de segurança necessárias para minimizá-los.

4.2 OBJETIVOS



- ☐ Conhecer o conceito de risco e sua implicação na segurança das informações da empresa.
- ☐ Distinguir a diferença entre aplicar ou não medidas de segurança nos diferentes aspectos de nossa empresa.
- ☐ Compreender o que se conhece como ciclo de segurança, o que nos permitirá manter vigentes nossas ações nessa matéria.

O risco é uma equação que leva em conta os prejuízos para a gestão do negócio e qual a frequência para ocorrência das ameaças.



4.3 RISCOS

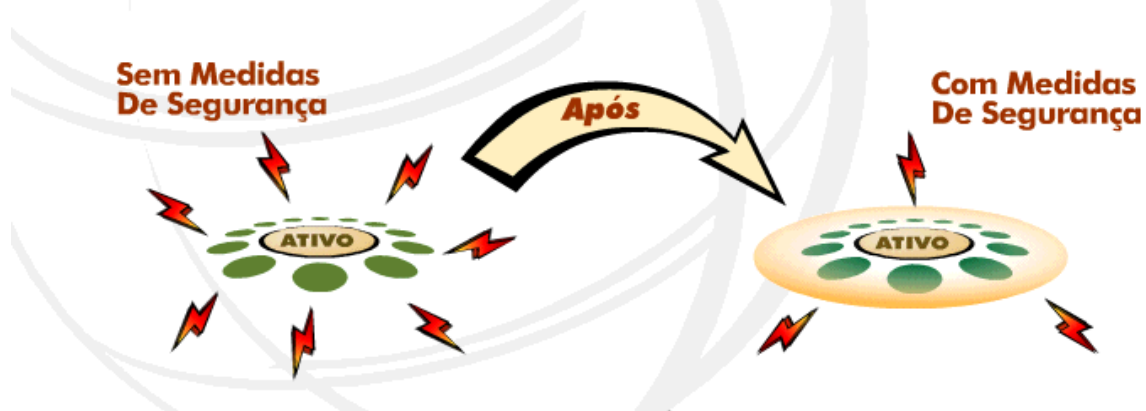


Conceito-chave

Risco é a probabilidade de que as ameaças explorem os pontos fracos, causando perdas ou danos aos ativos e impactos no negócio, ou seja, afetando: a confidencialidade, a integridade e a disponibilidade da informação.

Concluimos que a segurança é uma prática orientada para a eliminação das vulnerabilidades a fim de evitar ou reduzir a possibilidade de que as ameaças potenciais se concretizem no ambiente que se deseja proteger. O principal objetivo é garantir o êxito da comunicação segura, com informações disponíveis, íntegras e confidenciais, através de medidas de segurança que possam tornar o negócio de um indivíduo ou empresa factível com o menor risco possível.

As medidas de Segurança tem como função reduzir ao máximo o impacto das ameaças sobre os ativos.



4.4 MEDIDAS DE SEGURANÇA



Conceito-chave

As medidas de segurança são **ações orientadas para a eliminação ou redução de vulnerabilidades**, com o **objetivo de evitar que uma ameaça se concretize**. Essas medidas são **o primeiro passo para o aumento da segurança da informação** em um ambiente de tecnologia da informação e devem considerar a totalidade do processo.

Como existe uma variedade de tipos de pontos fracos que afetam a disponibilidade, a confidencialidade e a integridade das informações, é importante haver medidas de segurança específicas para lidar com cada caso.

Antes da definição das medidas de segurança que serão adotadas, deve-se conhecer o ambiente nos mínimos detalhes, buscando os pontos fracos existentes.



A partir desse conhecimento, tomam-se medidas ou realizam-se ações de segurança que podem ser do tipo:

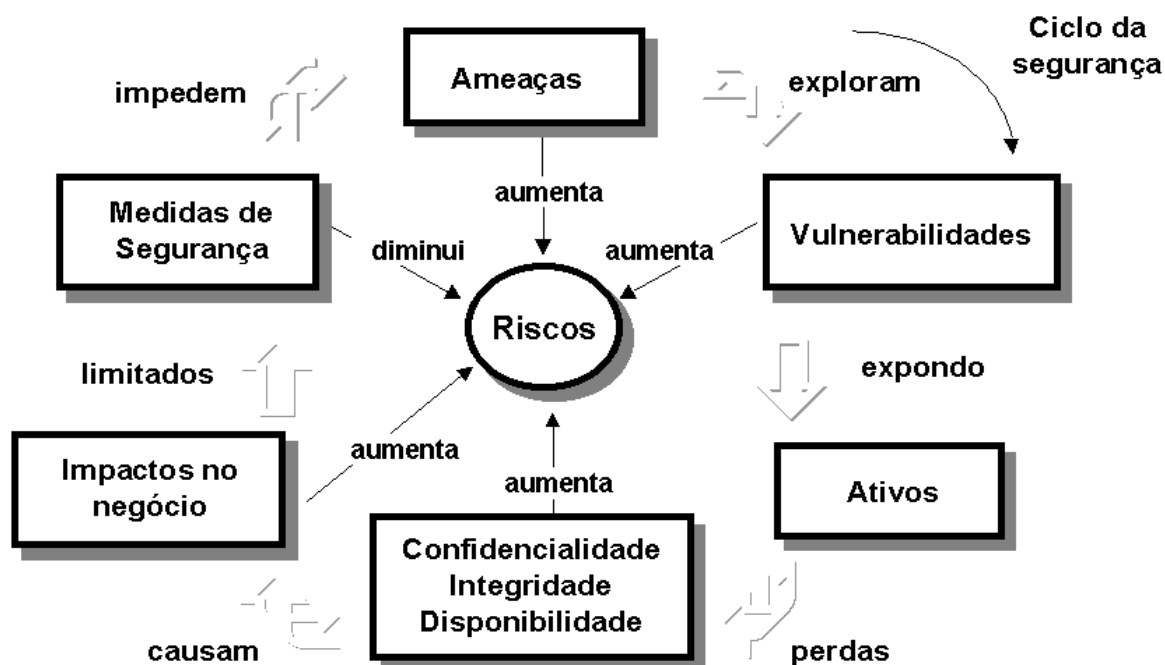
- ☐ **Preventivo:** buscando evitar o surgimento de novos pontos fracos e ameaças.
- ☐ **Perceptivo:** orientado para a revelação de atos que possam pôr em risco as informações.
- ☐ **Corretivo:** orientado para a correção dos problemas de segurança à medida que ocorrem.

As medidas de segurança são um conjunto de práticas que, quando integradas, constituem uma solução global e eficaz da segurança da informação. Entre as principais medidas, destacamos:

- ☐ Análise de riscos;
- ☐ Diretiva de segurança;
- ☐ Especificação de segurança;
- ☐ Administração de segurança.

A segurança da informação deve ser garantida de forma integral e completa, por isso é muito útil conhecer com um pouco mais de detalhes estas quatro medidas de segurança que permitem nos mover desde a análise de risco até a administração da segurança:

Análise de riscos	É uma medida que busca rastrear vulnerabilidades nos ativos que possam ser explorados por ameaças. A análise de riscos tem como resultado um grupo de recomendações para a correção dos ativos a fim de que possam ser protegidos.
Diretiva de segurança	É uma medida que busca estabelecer os padrões de segurança que devem ser seguidos por todos os envolvidos no uso e na manutenção dos ativos. É uma forma de administrar um conjunto de normas para guiar as pessoas na realização de seu trabalho. É o primeiro passo para aumentar a consciência da segurança das pessoas, pois está orientada para a formação de hábitos, por meio de manuais de instrução e procedimentos operacionais.
Especificações de segurança	São medidas que objetivam instruir a correta implementação de um novo ambiente tecnológico através do detalhe de seus elementos constituintes e a forma como os mesmos devem estar dispostos para atender aos princípios da segurança da informação.
Administração da segurança	São medidas integradas para produzir a gestão dos riscos de um ambiente. A administração da segurança envolve todas as medidas mencionadas anteriormente, a do tipo preventiva, perceptiva e corretiva, com base no ciclo da segurança apresentado a seguir.



4.5 CICLO DE SEGURANÇA

Agora que você já conhece todos os conceitos necessários para compreender o que é a segurança, apresentamos a seguir o ciclo da segurança da informação, com todos os seus conceitos básicos.

O ciclo de segurança inicia com a identificação das ameaças que as empresas enfrentam. A identificação das ameaças permitirá a visualização dos pontos fracos que podem ser explorados, expondo os ativos a riscos de segurança.

Essa exposição leva a uma perda de um ou mais princípios básicos da segurança da informação, causando impactos no negócio da empresa, aumentando ainda mais os riscos a que estão expostas as informações.

Para que o impacto dessas ameaças ao negócio sejam reduzidas, é necessário tomar medidas de segurança para impedir a ocorrência de pontos fracos.

Acima, concluímos a definição de segurança da informação com a ilustração do ciclo.

Como podemos ver no diagrama anterior: os riscos na segurança da empresa aumentam à medida que as ameaças conseguem explorar as vulnerabilidades e, portanto, provocar danos nos ativos. Esses danos podem fazer com que a confidencialidade, a integridade ou a disponibilidade da informação se percam, causando impactos no negócio da empresa.

As medidas de segurança permitem diminuir os riscos e, assim, fazer com que o ciclo seja de muito menor impacto para os ativos e, portanto, para a empresa.

Portanto, a segurança é ...

... uma atividade cujo propósito é:

- ☐ proteger os **ativos contra acessos não-autorizados**,
- ☐ **evitar alterações indevidas** que possam pôr em risco sua integridade
- ☐ maximizar a **disponibilidade** da informação

E é instrumentada por meio de **políticas e procedimentos de segurança** que permitem: a identificação e o controle de ameaças e pontos fracos, levando em consideração a preservação da **confidencialidade, integridade e disponibilidade** das informações.

4.6 LIÇÕES APRENDIDAS

- ☐ Identificamos como devemos visualizar os diferentes riscos aos quais nossa empresa está exposta, o que nos permitirá reduzi-los e aumentar a segurança dos ativos.
- ☐ Compreendemos os diferentes tipos de medidas de segurança que podemos tomar na empresa, sejam preventivas, perceptivas ou corretivas, aplicando-as e, assim, diminuindo os possíveis impactos ou danos resultados dos ataques.
- ☐ Conhecemos o ciclo de segurança, no qual se recorre às diferentes medidas para evitar a ocorrência de vulnerabilidades.



4.7 REFERÊNCIA BIBLIOGRÁFICA

¹ Novo Dicionário Aurélio – O Dicionário da Língua Portuguesa – edição de 1999.

² Timeline of the History of Information - Geoffrey Numberg

³ Chappman

⁴ Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security. Editado por W. H. Ware.

⁵ CSC-STD-001-83 - Library No. S225,711 - Department of Defense Trusted Computer System Evaluation Criteria - 15 August 1983.

⁶ An Introduction to Computer Security: The NIST Handbook – Special Publication 800-12.

⁷ <http://www.iso27001security.com/html/iso27000.html>.

⁸ Decreto No 3.505, de 13 de junho de 2.000 – Presidência da República – Casa Civil.

⁹ Segurança de Redes – Projeto e gerenciamento de redes seguras – Thomas A. Wadlow. Editora Campus, 2000.