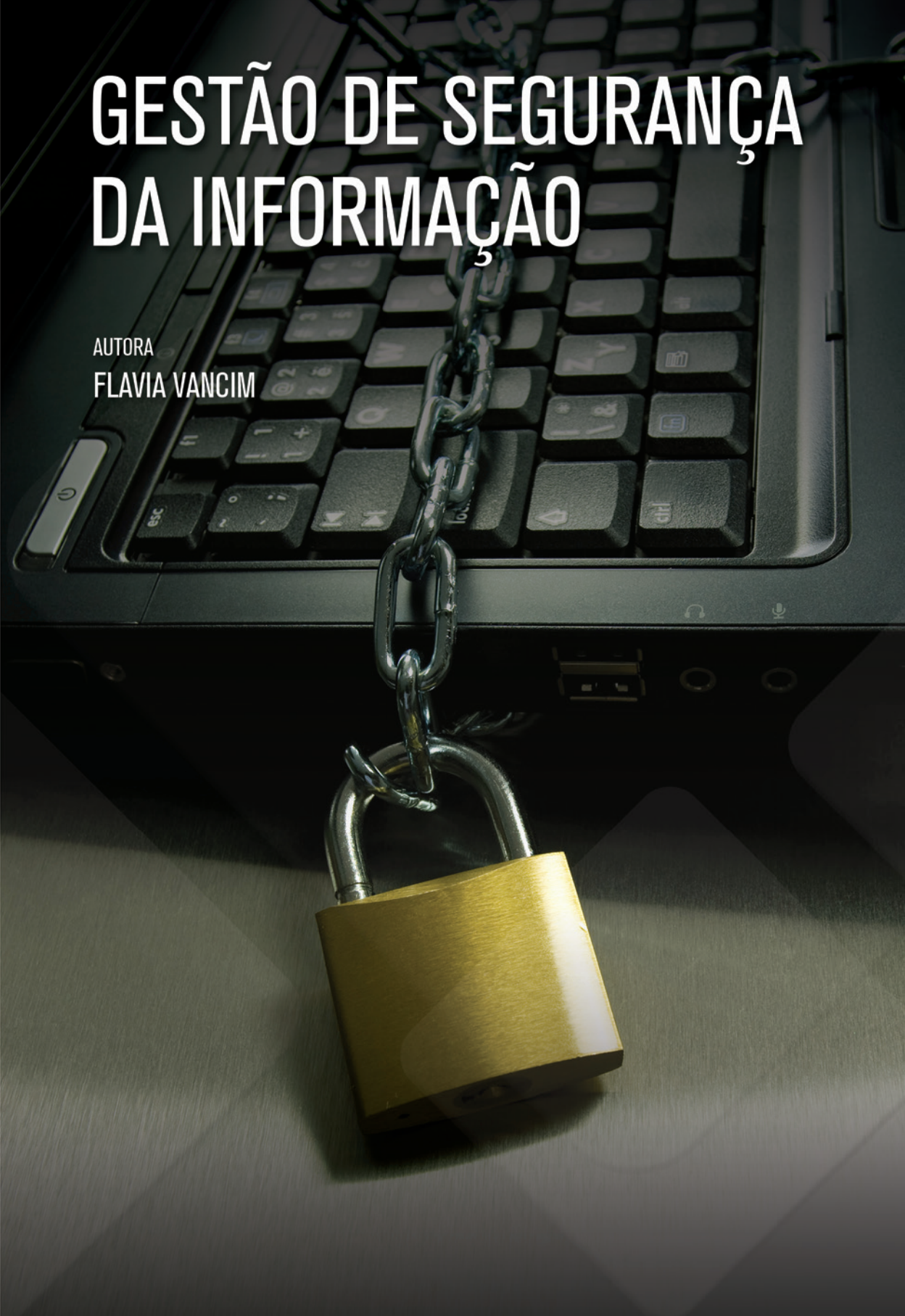
GESTÃO DE SEGURANÇA DA INFORMAÇÃO

AUTORA
FLAVIA VANCIM



GESTÃO DA SEGURANÇA DA INFORMAÇÃO

AUTORA
FLAVIA VANCIM

1ª EDIÇÃO
SESES
RIO DE JANEIRO 2016

Estácio

Conselho editorial REGIANE BURGER; ROBERTO PAES; GLADIS LINHARES; KAREN BORTOLOTI; HELCIMARA AFFONSO DE SOUZA

Autora do original FLAVIA VANCIM FRACHONE NEVES

Projeto editorial ROBERTO PAES

Coordenação de produção GLADIS LINHARES

Coordenação de produção EaD KAREN FERNANDA BORTOLOTI

Projeto gráfico PAULO VITOR BASTOS

Diagramação BFS MEDIA

Revisão linguística AMANDA CARLA DUARTE AGUIAR

Imagem de capa PETO ZVONAR | DREAMSTIME.COM

Dados Internacionais de Catalogação na Publicação (CIP)

V222G VANCIM, FLAVIA

Gestão de segurança da informação / Flavia Vancim

Rio de Janeiro : SESES, 2016.

152 P. : IL.

ISBN: 978-85-5548-184-0

1. Sistemas de informação. 2. Gestão organizacional. 3. Softwares. 4. Segurança da informação. I. SESES. II. Estácio.

CDD 005.82

Diretoria de Ensino — Fábrica de Conhecimento

Rua do Bispo, 83, bloco F, Campus João Uchôa

Rio Comprido — Rio de Janeiro — RJ — CEP 20261-063

Sumário

Prefácio

Prezados(as) alunos(as),

A maioria das empresas, independentemente do porte (pequeno, médio, grande), tem em seu cotidiano o uso da Tecnologia de Informação.

Mas,, afinal, o que é Tecnologia de Informação (T.I.)? A T.I. é uma estrutura organizada de hardware, software, banco de dados e redes de telecomunicações que permite às empresas manipular os dados, transformando-os em informações que agregam valor e/ou conhecimento aos processos de negócio. Além de trabalhar e fazer transações de negócios, a T.I. também possibilita aos usuários estudar, pesquisar, consumir, entreter, relacionar, expressar, entre outras possibilidades.

De fato, hoje não negociamos mais como há 20 anos. A cada dia surgem novas tecnologias em uma velocidade muito grande provocando grandes, mudanças e transformações na forma como as pessoas trabalham, consomem e interagem. Processos que antes eram executados e controlados por pessoas agora passam por algum meio tecnológico.

Crescentemente, as organizações passam a depender de sistemas informatizados. Seja numa simples troca de e-mail, seja em complexos sistemas de gestão, a tecnologia sempre permeia a troca de dados entre as empresas.

Diante de todo este contexto de mudanças, a velocidade com que essas tecnologias são modernizadas e difundidas, em especial as relacionadas ao uso da Internet e à comunicação móvel, tem atingido de forma distinta diferentes segmentos de população e de empresas, em países desenvolvidos e em desenvolvimento.

Dessa forma, a intensificação da transação e fluxo de dados, independentemente de tempo e espaço, além de terem alterado a forma como as pessoas passaram a interagir, mudou-se também o foco da preocupação. Não somente se deve garantir que a tecnologia funcione corretamente, mas principalmente que os dados nela trafegados sejam compartilhados e visualizados apenas com as pessoas devidas.

Ou seja, passou a ser necessário precaver-se não somente dos ataques físicos, mas também dos virtuais, a fim de se garantir que os dados sejam trafegados de forma segura e inviolável.

Nesta disciplina iremos trabalhar tópicos como a influência e o impacto da tecnologia no cotidiano das pessoas e das empresas e como lidar com ela de forma segura e confiável. Esses conhecimentos são de extrema importância, pois, além de conhecermos os desafios e a interferência da tecnologia das empresas, iremos apresentar métodos e técnicas para assegurar a gestão segura da informação.

Espero que desfrute da disciplina e que em breve possa colocar em prática os conhecimentos que aqui veremos.

Bons estudos!

1

Introdução à Segurança da Informação

Olá, pessoal. Neste primeiro capítulo iremos conhecer alguns conceitos introdutórios que nortearão nossos próximos passos. Iremos percorrer aspectos básicos da segurança das informações, e também conhecer todo o ciclo de vida das informações. Não obstante, e devido à constante confusão que há entre os conceitos de dados, informação e conhecimento, iremos distingui-los. Por fim, compreenderemos a necessidade de se gerenciar corretamente a segurança das informações que trafegam no ambiente corporativo. Preparados? Vamos juntos!

OBJETIVOS

Nossos objetivos serão:

- Compreender os conceitos básicos de informação;
- Distinguir os conceitos de dados, informações e conhecimento;
- Conhecer aspectos básicos da segurança da informação;
- Analisar as necessidades de segurança das informações no ambiente corporativo;
- Conhecer princípios da segurança da informação.

1.1 Compreendendo a Informação

A informação está intrinsecamente relacionada ao nosso dia a dia, seja pessoal ou profissional. Especificamente abordando o contexto organizacional, pode-se seguramente afirmar que a qualidade das informações, que fluem intermitentemente, impacta diretamente no processo de tomada de decisão dos gestores.

Mas o que é mesmo informação?

De acordo com o Dicionário Online de Português[1], a informação refere-se a:

> Reunião dos dados, sobre um assunto ou pessoa.
> O que se torna público através dos meios de comunicação ou por meio de publicidade. Ex.: o jornal divulgou a informação sobre o concurso.
> Esclarecimento sobre o funcionamento de algo. Ex.: informações sobre o aparelho.
> [...]
> Informática: Reunião dos dados que, colocados num computador, são processados, dando resultados para um determinado projeto.
> [...]
> Informação Genética: Conjunto dos dados que se referem aos caracteres hereditários.
> Ação ou efeito de informar ou de se informar.

No conceito supracitado, já notamos a correlação entre dados e informação. No entanto dedicaremos um item a esta explicação, tendo em vista a demasiada confusão que comumente as pessoas costumam fazer.

CONEXÃO

DICA DE VÍDEO: "O Poder da Informação" de Mário Persona: http://www.youtube.com/watch?v=HgIn7wwyY7w&feature=fvsr

Este video é o trecho de uma palestra de Mário Persona: palestrante, professor e consultor de estratégias de comunicação e marketing e autor de vários livros de negócios. Há mais de dez anos apresenta palestras, *workshops* e treinamentos de temas ligados a comunicação, marketing, vendas e clima organizacional.

1 Disponível em: http://www.dicio.com.br/informacao/. Acesso: 01/05/2015

Complementarmente a este conceito, expomos outra explicação publicada através do dicionário de Conceitos[2], conforme segue:

> A informação é um conjunto organizado de dados, que constitui uma mensagem sobre um determinado fenômeno ou evento. A informação permite resolver problemas e tomar decisões, tendo em conta que o seu uso racional é base do conhecimento.
> A informação é um fenômeno que confere significado ou sentido às coisas, já que através de códigos e de conjuntos de dados, forma os modelos do pensamento humano.
> [...]
> Os especialistas afirmam que existe uma relação indissolúvel entre a informação, os dados, o conhecimento, o pensamento e a linguagem.
> Ao longo da história, a forma de armazenamento e o acesso à informação foi variando. Na Idade Média, o principal patrimônio encontrava-se nas bibliotecas dos mosteiros. A partir da Idade Moderna, graças ao nascimento da imprensa, os livros começaram a ser fabricados em série e surgiram os jornais.
> Já no século XX, apareceram os meios de comunicação de massa (televisão, rádio) bem como as ferramentas digitais resultantes do desenvolvimento da Internet.

Conforme pudemos observar, além de complementar a primeira citação, esta ainda adiciona um novo conceito: o conhecimento.

Naturalmente, e muito comumente, as pessoas costumam se equivocar quanto aos conceitos de dados, informações e conhecimento.

Diante do exposto, e se nossa meta é esclarecer o conceito de informação para que possamos prosseguir no entendimento de segurança da informação, é imprescindível, antes, desmitificar toda esta confusão. Para tanto, o próximo subitem tratará desta distinção.

Cabe ressaltar, de acordo com Santos e Resende (2000 apud Neves et al, 2006), que a posse da informação reduz incertezas sobre algum estado ou evento. No entanto, é igualmente importante salientar que nem toda informação é crucial e/ou essencial a ponto de requerer cuidados especiais. Opostamente, pode haver uma determinada informação que pode vir a ser tão vital que o custo de manter sua integridade, por maior que seja, ainda será menor que o custo de não dispor dela adequadamente.

2 Disponível em: http://conceito.de/informacao. Acesso: 01/05/2015

Acompanhemos a citação abaixo, que explana a respeito da necessidade constante das organizações em obter informações. E tal demanda permanente pode vir a gerar uma ansiedade de informação.

> Os aspectos de constante transição da economia acarretam nas organizações, em geral, uma necessidade permanente de informação. Essa ansiedade de informação é o resultado da distância entre o que é compreendido e o que acha-se que deveria ser compreendido numa espécie de "buraco negro" existente entre dados e conhecimento. Isso ocorre quando a informação não nos sacia, ou seja, não é suficiente. Além disto, a ansiedade também é gerada quando tais situações ocorrem: não compreender a informação; sentir-se assoberbado pelo seu volume; não saber se uma certa informação existe; não saber onde encontrá-la, nem exatamente onde ela se situa. Ainda assim, esta ansiedade pode-se aumentar quando se tem consciência de que o acesso à informação é limitado não conseguindo, então, atender às necessidades dos clientes (NEVES, 2003).

Diante do panorama exposto pela citação acima, analisam-se, conforme ilustra Wurman (1995), alguns aspectos comportamentais das pessoas que apresentam um grau de ansiedade pela incerteza ou ausência de informações que podem ser notados. São eles:

- Falar compulsivamente que não consegue se manter atualizado com os acontecimentos;
- Sentir-se culpado com aquela pilha, cada vez maior, de periódicos e relatórios que se acumulam à sua espera;
- Descobrir que é incapaz de explicar algo que pensava ter entendido;
- Dedicar tempo e atenção a notícias que não têm quaisquer impactos culturais, econômicos ou científicos em suas vidas e seus negócios;
- Achar que os colegas profissionais estão entendendo tudo e você não;
- Ficar receoso ou encabulado de dizer "não sei".

Dessa forma, e de acordo com Neves (2003), somos muito atingidos pelas mídias de comunicação, pelos colegas de trabalho, por conversas etc. Com isto, as organizações, de modo geral, ficam cada vez mais preocupadas com suas aparentes incapacidades de tratar, compreender, manipular essa epidemia

de dados que toma conta de tudo. O próprio volume disponível de informação acaba tornando parte dela inutilizável, devido à incapacidade de utilizá-las adequadamente, bem como a forma como nos é transmitida.

De acordo com o exposto por Wadlow (2000), a informação pode ser classificada em níveis de prioridade dentro da organização, conforme segue:

INFORMAÇÃO PÚBLICA	Informação que pode vir ao público sem consequências prejudiciais ao funcionamento normal da empresa e cuja integridade não é vital;
INFORMAÇÃO INTERNA	Informação que deveria ter o livre acesso evitado, embora não haja consequências prejudiciais/sérias do acesso e uso não autorizado. A integridade deste tipo de informação é importante, porém não vital;
INFORMAÇÃO CONFIDENCIAL	Informação que é restrita aos limites da empresa e cuja divulgação ou perda pode acarretar em desequilíbrio operacional e, eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo;
INFORMAÇÃO SECRETA	Informação muito crítica para as atividades da empresa e cuja integridade deve ser preservada a qualquer custo. O acesso deve ser restrito, e a segurança deste tipo de informação é crucial/vital para a empresa.

1.1.1 Dados, Informação e Conhecimento

Vamos discutir um pouco esses conceitos e as diferenças entre eles?

A seguir, definições dadas pelo Professor Dr. Valdemar W. Setzer[3] referente a dados, informação e conhecimento:

3 Setzer, V. W.. Dado, Informação, Conhecimento e Competência. Disponível em: < http://www.ime.usp.br/~vwsetzer/dado-info.html>.

• Dados:

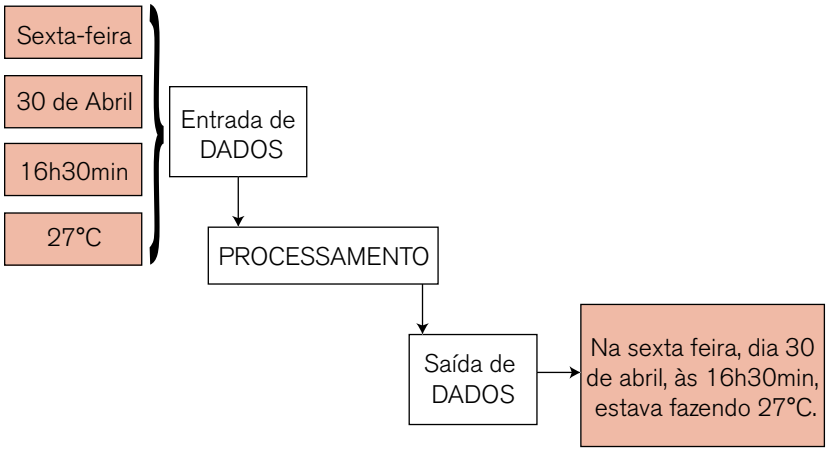
> [...] uma sequência de símbolos quantificados ou quantificáveis. Portanto, um texto é um dado. De fato, as letras são símbolos quantificados, já que o alfabeto, sendo um conjunto finito, pode por si só constituir uma base numérica (a base hexadecimal emprega tradicionalidade, além dos 10 dígitos decimais, as letras A a E). Também são dados fotos, figuras, sons gravados e animação, pois todos podem ser quantificados a ponto de se ter eventualmente dificuldade de distinguir a sua reprodução, a partir da representação quantificada, com o original. É muito importante notar-se que, mesmo se incompreensível para o leitor, qualquer texto constitui um dado ou uma seqüência de dados [...]

Ainda segundo o autor, um dado é uma entidade matemática sintática, ou seja, os dados podem ser descritos por estruturas de representação. Assim sendo, podemos dizer que o computador é capaz de armazenar dados. Estes dados podem ser quantificados, conectados entre si e manipulados pelo processamento de dados. Da mesma forma, pode-se definir dados como fatos brutos, ainda não organizados nem processados.

• Informação:

> Se a representação da informação for feita por meio de dados, como na frase sobre Paris, pode ser armazenada em um computador. Mas, atenção, o que é armazenado na máquina não é a informação, mas a sua representação em forma de dados. Essa representação pode ser transformada pela máquina, como na formatação de um texto, o que seria uma transformação sintática. A máquina não pode mudar o significado a partir deste, já que ele depende de uma pessoa que possui a informação. Obviamente, a máquina pode embaralhar os dados de modo que eles passem a ser ininteligíveis pela pessoa que os recebe, deixando de ser informação para essa pessoa. Além disso, é possível transformar a representação de uma informação de modo que mude de informação para quem a recebe (por exemplo, o computador pode mudar o nome da cidade de Paris para Londres). Houve mudança no significado para o receptor, mas no computador a alteração foi puramente sintática, uma manipulação matemática de dados. Assim, não é possível processar informação diretamente em um computador. Para isso é necessário reduzi-la a dados. No exemplo, "fascinante" teria que ser quantificado, usando-se por exemplo uma escala de zero a quatro. Mas então isso não seria mais informação.

Podemos agrupar dados isolados e torná-los consistentes ao se transformarem em informações. Por exemplo, se tivermos um conjunto de dados que descreva a temperatura do ambiente num local, horário e data, poderíamos ter a seguinte relação:



Assim, o conjunto de dados inicial foi organizado de maneira que "faça sentido" àqueles que o estiverem lendo. Isto os torna informação. No entanto, a representação no computador é feita baseada nos dados. Seguindo com o pensamento de Setzer:

- Conhecimento:

> "[...] abstração interior, pessoal, de algo que foi experimentado, vivenciado, por alguém. Continuando o exemplo, alguém tem algum conhecimento de Paris somente se a visitou[...]".

Dessa maneira, o conhecimento precisa ser descrito por informações.

A informação pode ser inserida em um computador por meio de uma representação em forma de dados (se bem que, estando na máquina, deixa de ser informação). Como o conhecimento não é sujeito a representações, não pode ser inserido em um computador. Assim, neste sentido, é absolutamente equivocado falar-se de uma "base de conhecimento" em um computador. O que se tem é, de fato, é uma tradicional "base (ou banco) de dados". Um nenê de alguns meses tem muito conhecimento (por exemplo, reconhece a mãe, sabe que chorando ganha comida, etc.). Mas não se pode dizer que ele tem informações, pois não associa conceitos. Do mesmo modo, nesta conceituação não se pode dizer que um animal tem informação, mas certamente tem muito conhecimento.

A informação associa-se à semântica, enquanto o conhecimento está associado à pragmática, ou seja, algo existente no mundo real.

CONEXÃO

Recomendamos ler o artigo do Prof. Dr. Valdemar W. Setzer na íntegra, através do link: http://www.ime.usp.br/~vwsetzer/dado-info.html

Para simplificar o entendimento sobre dados, informação e conhecimento, vamos expor alguns exemplos:

EXEMPLO

1. Fazer um bolo.

Os ingredientes de um bolo podem ser comparados aos **dados.**

A mistura destes ingredientes para transformá-los na massa do bolo que será assada e resultará no bolo é a **informação**.

Cada pessoa que provar/experimentar o bolo terá sua própria opinião/conceito – ou seja, esta vivência pode ser comparada ao **conhecimento.**

Figura 1.1 – Comparação de dados, informação e conhecimento.

2. Relatório Estatístico de Vendas do Supermercado "Vende Bem".

O Sistema de Informação Gerencial do Supermercado "Vende Bem", entre outras funções, vai armazenando os dados das vendas realizadas em seu banco de **dados**.

Os gestores podem necessitar analisar um relatório estatístico das vendas de um determinado produto em um dado período de tempo. Ou seja, dados serão agrupados e organizados, pelo Sistema de Informação Gerencial, para compor este relatório estatístico. Este, por sua vez, conterá, portanto, **informações**.

Cada gestor fará sua interpretação pessoal, baseando-se na sua experiência, vivência, *know-how*, e assim por diante. Ou seja, cada gestor interpretará um mesmo relatório à sua maneira, compondo desta forma seu **conhecimento**.

Figura 1.2 – Um sistema pode prover relatórios estatísticos extraídos de seu banco de dados, para ser analisado pelos gestores.

Por fim, vale explicitar, de acordo com Pereira et al (2012), que uma organização que possuir uma equipe responsável por mapear e monitorar os dados, informação e conhecimento que circulam em seu ambiente aumenta, consideravelmente, suas chances de se destacar diante das concorrentes.

1.2 Segurança da Informação

1.2.1 Segurança da Informação no Ambiente Corporativo

Todo tipo de complemento da tarefa dentro de uma corporação requer informação. A comunicação é requerida para assegurar que estas informações provêm para a pessoa responsável pela tarefa.

As informações trafegadas intermitentemente pela organização caracterizam-se por serem um dos seus ativos mais valiosos. Elas são fundamentais para todo o processo organizacional. Ou seja, as informações são primordiais para o sucesso das negociações. Acompanhemos a citação abaixo, que enfatiza e detalha tal afirmação.

> A informação é o elemento fundamental para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor, podendo levar a organização do sucesso ao fracasso, em função de impactos financeiros, operacionais ou de imagem, ocasionados por falhas, erros ou fraudes no uso da informação. O que diferencia o uso da informação entre as organizações é a necessidade de se manter disponível, mantendo a integridade e o rigor em relação ao sigilo que cada organização precisa para a sua informação (FONTES, 2011, p. 2).

Diante do exposto, podemos afirmar, em concordância com Lima (2013), que a informação passou a ser um recurso estratégico para as organizações, possibilitando a geração de conhecimento e apoiando o processo de tomada de decisões. Em virtude disto, o grau de proteção e preocupação com estas informações cresceu consideravelmente. Neste âmbito, medidas e cuidados de segurança devem ser tomados e sempre verificados.

Acompanhemos a próxima citação, que enfatiza a necessidade das organizações em investirem numa infraestrutura adequada de telecomunicação para viabilizar a troca de informações com parceiros de negócios e clientes.

> Para se criar um serviço com qualidade é necessário que a organização se dedique a conhecer seus clientes, seus problemas e expectativas. O cliente deve ser visto como patrimônio mais valioso que precisa ser cuidado e mantido, uma vez que, atualmente,

os consumidores têm mais acesso à informação e, consequentemente, são mais exigentes. Dessa forma, é fundamental que as organizações estejam bem preparadas para atender essas necessidades.
Para tanto, é essencial que as organizações tenham uma infraestrutura de telecomunicações, que permita a comunicação entre pessoas e recursos, sendo bem projetada e bem dimensionada. Isto é vital para a sobrevivência de uma organização (NEVES, 2003).

Adicionalmente, Laureano e Moraes (2005) abordam que dispor da informação correta, no momento adequado, significa tomar uma decisão assertiva. Neste contexto, a evolução das tecnologias de informação proporcionou mobilidade, inteligência nos negócios e real capacidade de gestão. Complementarmente, e de acordo com Bremer (2000), as tecnologias de informação e comunicação trazem consigo consequências extremamente relevantes no contexto empresarial e, uma relação muito forte, pode ser notada entre essas tecnologias e o avanço das parcerias entre as empresas.

O uso da Tecnologia da Informação se tornou uma necessidade indispensável para fins comerciais nos dias de hoje, não só para as grandes corporações, mas também para as microempresas. Apesar da alta disponibilidade, o uso de TI também traz consigo várias ameaças que podem passar por despercebidas pelos pequenos empreendedores, podendo colocar em grande risco a longevidade de seus negócios – considerando que muitas destas empresas possuem a TI como uma parte crítica de seu processo de produção (MENDES, 2013)

Informações técnicas, comerciais e financeiras, necessárias para o bom andamento dos negócios, trafegam pela rede que conecta a empresa a seus parceiros comerciais. Portanto, uma série de cuidados e medidas devem ser tomados, principalmente no que tange à proteção das informações que trafegam por esta rede. Ou seja, a tecnologia veio a impulsionar e otimizar cada dia mais o rápido acesso às informações organizacionais, sem barreiras de tempo ou espaço. Esta grande vantagem competitiva traz consigo também importantes preocupações acerca da segurança de todo este fluxo de dados armazenados, acessados, alterados, e assim por diante.

> Atualmente a maior parte das organizações trabalha com um sistema informatizado de modo que as informações fluam de maneira mais rápida, baseando boa parte de seu plano de negócio e suas decisões nessas informações (OLIVEIRA, 2001 apud ALVES e MOREIRA, 2012, p. 130).
> Porém, toda essa tecnologia traz algumas vulnerabilidades para a organização, obrigando-a a desenvolver uma política de segurança da informação para que essas informações possam ser manuseadas de maneira correta e segura. A política de segurança da informação tem o propósito de tratar essas informações desde a sua criação até o seu descarte, definindo regras para que as mesmas não sejam roubadas, alteradas ou perdidas (SÊMOLA, 2003 apud ALVES e MOREIRA, 2012, p. 130).

De acordo com Lima (2013), a informação é um ativo de significativa importância para qualquer organização, independentemente do seu porte e do seu segmento de mercado. Complementarmente, e conforme explicitam Laureano e Moraes (2005), a informação possui um valor para a organização e, portanto, necessita ser adequadamente protegida, por meio dos processos de Segurança da Informação, pois está sob constante risco.

> A segurança da informação deve existir para proteger os recursos de informação que são utilizados estratégica e operacionalmente para o funcionamento da organização, contra divulgação indevida, seja ela intencional ou não, alteração não autorizada, destruição não desejada, negação de serviço, fraudes financeiras, apropriação indevida de informações ou reputação da imagem da instituição. Essa proteção é feita através da implantação de controles de segurança definidos em políticas e procedimentos (LIMA, 2013, p. 14)

Após a leitura da citação supracitada, cabe-nos ressaltar que podemos seguramente afirmar, em concordância com Alves e Moreira (2012), que não há informação que esteja 100% segura, por mais arrojado que seja o aparato tecnológico de segurança. Pois novos riscos sempre poderão surgir. Diante deste contexto, é imprescindível que a organização direcione esforços para realizar um correto gerenciamento da segurança das informações.

> A segurança da informação, segundo Solms (2005), passou a ser parte integral para um bom gerenciamento da corporação. Embora esse fato sempre ser verdadeiro, foi apenas recentemente enfatizado, no bom gerenciamento da corporação. Elevando a "segurança da informação" para a "segurança dos negócios", haverá um foco extra nas necessidades de assegurar a existência prolongada da companhia, e integrar e envolver todos os presentes esforços, da mesma forma que a proteção é considerada (NEVES et al, 2006, p. 53).

1.2.2 Princípios da Segurança da Informação no Ambiente Corporativo

A segurança da informação no ambiente corporativo visa a estabelecer uma série de soluções técnicas para problemas não técnicos. A exemplo desta afirmação, e concordando com Moreira e Cordeiro (2002), pode-se despender muito tempo, dinheiro e esforço em segurança computacional, **mas nunca será resolvido o problema de perda de dados acidentais ou uma interrupção intencional de suas atividades.** Dadas as circunstâncias – "bugs" de software, acidentes, erros, mau tempo ou um invasor bem motivado e bem equipado –, qualquer computador pode ficar comprometido, submetido a desuso ou algo pior que isto.

> Antes de se estabelecer qual a melhor política de segurança, faz-se necessário analisar e planejar, qual a real necessidade da mesma, pois, dessa forma, implantações de mecanismos de segurança não serão adotados, inadequadamente (NEVES et al, 2006, p. 53).

Complementarmente a esta citação, e de acordo com Nakamura e Geus (2002 *apud* Neves et al, 2006), para melhorar a segurança de um sistema, deve-se prioritariamente considerar alguns aspectos, dentre os quais:

CONHECER OS POSSÍVEIS OPONENTES	identificando o que eles desejam fazer, e os perigos que podem vir a causar à organização;
CONTABILIZAR OS VALORES	uma vez que a implementação e o gerenciamento da política de segurança pode significar, além da necessidade de mais recursos pessoais, a necessidade de significativos recursos de software e de hardware. Os custos das medidas de segurança devem, portanto, ser compatíveis e proporcionais às necessidades da organização e às probabilidades de ocorrerem incidentes de segurança;
CONSIDERAR OS FATORES HUMANOS	uma vez que muitos procedimentos de segurança falham, porque as reações dos usuários a esses procedimentos não são considerados com seu devido valor;
CONHECER OS PONTOS FRACOS	pois todo sistema possui vulnerabilidades;
APLICAR A SEGURANÇA DE ACORDO COM OS NEGÓCIOS DA ORGANIZAÇÃO	a fim de definir uma estratégia de segurança que melhor se adapte às necessidades deles.

Fazendo este levantamento e análise, pode-se ter conhecimento do que se tenta proteger, contra quem e quanto tempo e custo pretende-se investir para obter a proteção adequada. Com isto, temos a base para a análise de risco (assunto a ser visto posteriormente nesta disciplina).

CONEXÃO

Dica de Vídeo: "Segurança da Informação – Bradesco"

LINK: https://www.youtube.com/watch?v=EsO5f3kS6Lw

Este vídeo é muito interessante e pertinente. Mostra como o comportamento dos colaboradores podem impactar diretamente na segurança das informações confidenciais.

Adicionalmente, ao mencionarmos a segurança da informação, e antes de cogitarmos a possibilidade de nos "munir" com aparatos tecnológicos, devemos prioritariamente fazer um levantamento e nos questionar/indagar:

- **O que** minha empresa quer proteger? (ou seja, tomar ciência do que se almeja proteger);
- **Por que** minha empresa quer proteger? (ou seja, descobrir a relevância de tais informações que se almeja proteger);
- Minha empresa quer proteger **de quê**? (ou seja, fazer um mapeamento/levantamento do que se deve monitorar para que as informações não sejam extraviadas/corrompidas);
- **Como** minha empresa deve proteger? (ou seja, determinar normas/regras de como, quando, onde, quem poderá ter acesso).

De acordo com Stallings (1999), Moreira e Cordeiro (2002), Kurose e Ross (2006 apud Alves e Moreira 2012) e Lima (2013), as informações devem cumprir os seguintes requisitos:

AUTENTICAÇÃO	irá definir que as partes envolvidas na comunicação sejam autenticadas, a fim de garantir que cada uma delas seja realmente quem diz ser;
CONFIDENCIALIDADE	refere-se a proteger a informação de ser lida ou copiada por qualquer um que não está explicitamente autorizado pelo proprietário da informação;

CONSISTÊNCIA	assegura que o sistema comporta-se como esperado pelos usuários autorizados. Se o software ou hardware repentinamente começa a se comportar de maneira radicalmente diferente daquele que se costuma comportar, especialmente após uma atualização ou a reparação de um erro, pode ocorrer um “desastre”;
DISPONIBILIDADE	irá definir que as informações devidas estarão disponíveis para seus respectivos usuários. Aqui cabe uma ressalva: para garantir esta disponibilidade da informação somente para o usuário devido, deve-se implementar controles de acesso, a fim de conter usuários não autorizados;
CONTROLE	que regula o acesso ao sistema. Se indivíduos (ou softwares) desconhecidos ou não autorizados são encontrados no sistema, eles podem ocasionar um grande problema. Deve-se preocupar como entraram, o que devem ter feito e que ou o que mais também acessou o sistema. Recuperar-se destes episódios pode requerer consideráveis tempo e gasto para reconstruir e reinstalar o sistema e ainda verificar se nada de importante foi mudado ou revelado – mesmo se nada aconteceu de fato;
AUDITORIA	tal como se preocupar com usuários não autorizados, os usuários autorizados às vezes cometem erros, ou até mesmo atos maliciosos. Nesses casos, deve-se determinar o que foi feito, por quem, e o que foi afeitado. A única maneira de se alcançar estes resultados é através de alguns registros incorrompíveis de atividade no sistema que indubitavelmente identifica os autores e ações envolvidas. Em algumas aplicações críticas, a trilha da auditoria pode se estender à autorização de operações que desfaçam ou ajudem a restaurar o sistema ao seu estado correto;

INTEGRIDADE	irá definir que a informação é originária de quem diz originar, de forma a impedir que alterações na mensagem original confundam as partes envolvidas na comunicação. E, mesmo que haja alguma alteração na mensagem original, que esta seja passível a ser detectada;
NÃO REPÚDIO	irá garantir que a informação enviada por quaisquer partes envolvidas na comunicação não seja negada pelo seu respetivo remetente (em outras palavras, irá garantir que quem enviou a informação não poderá negar sua transmissão);
EFETIVIDADE	a informação sendo entregue em tempo, de maneira correta, consistente e utilizável;
EFICIÊNCIA	entrega da informação através do mais produtivo e econômico uso dos recursos;
CONFORMIDADE OU LEGALIDADE	de acordo com leis, regulamentos, políticas internas e obrigações contratuais impostos externamente;
CONFIANÇA	profissionais de segurança geralmente não se referem a um sistema como sendo “seguro” ou “inseguro”. Em vez disto, é usada a palavra “confiável” para descrever o nível de confiança no qual o sistema computacional se comporta. Isto reconhece que a segurança absoluta nunca estará presente. Desenvolver confiança adequada em um sistema computacional requer um pensamento cauteloso e planejado.

Embora todos esses aspectos acima descritos sejam importantes, ressaltamos que cada organização irá atribuir-lhes diferentes níveis de importância, de acordo com suas respectivas demandas.

Adicionalmente, é importante ressaltar que alguns fatores acabam impactando diretamente e negativamente para que medidas de segurança adequadas sejam adotadas:

- Falta de informação sobre a importância da segurança das informações da empresa;
- Falta de recursos financeiros para investimento adequado;
- Ausência de uma política de segurança adequada;
- Não ter noção/conhecimento dos possíveis/prováveis prejuízos causados pela falta de segurança das informações.

Portanto, e conforme explicita Mendes (2013), os administradores precisam de procedimentos para conduzir uma avaliação periódica sobre segurança da informação, revisar os resultados e tomar as medidas necessárias, treinar e educar seus funcionários sobre o assunto.

Por fim, é importante salientar, em concordância com Laureano e Moraes (2005), que antigamente a atenção dada à segurança da informação estava focada apenas na tecnologia. Atualmente, notamos que o desafio vai além desta amplitude e engloba, também, a construção de uma relação de confiabilidade com os clientes e parceiros da empresa.

ATIVIDADES

01. De acordo com a classificação de prioridade das informações dentro das organizações, leia as sentenças abaixo e assinale a alternativa que as preenche correta e respectivamente.

I. _____ informação que pode vir ao público sem quaisquer consequências prejudiciais à empresa;

II. _____ informação que deveria ter o livre acesso evitado, porém não haverá consequências danosas provenientes do acesso não autorizado;

III. _____ informação que é restrita aos limites da empresa e, se divulgada livremente, acarretará eventuais perdas financeiras ou de confiabilidade;

IV. _____ informação muito crítica para as atividades da empresa e cujo acesso deve ser restrito. Além disso, a segurança é crucial para a empresa.

a) Informação Interna; Informação Pública; Informação Confidencial; Informação Secreta.
b) Informação Pública; Informação Interna; Informação Confidencial; Informação Secreta.
c) Informação Pública; Informação Confidencial; Informação Interna; Informação Secreta.
d) Informação Secreta; Informação Interna; Informação Confidencial; Informação Pública.
e) Informação Pública; Informação Secreta; Informação Interna; Informação Confidencial.

02. Sobre os conceitos de Dados, Informação e Conhecimento, leia as asserções e assinale a alternativa correta:

I. Pode-se afirmar que o computador armazena conhecimento;

II. Dados são fatos brutos, não lapidados;

III. A informação depende de algum tipo de relacionamento, avaliação ou interpretação dos dados;

IV. O conhecimento é uma abstração interior, pessoal, de algo que foi experimentado, vivenciado por alguém.

a) As asserções I e II estão corretas.
b) As asserções I, III e IV estão corretas.
c) As asserções II, III e IV estão corretas.
d) As asserções II e IV estão corretas.
e) As asserções I e III estão corretas.

03. Para melhorar a segurança de um sistema, deve-se primeiramente considerar alguns aspectos importantes. Sobre tais aspectos, assinale a alternativa incorreta.

a) Conhecer os possíveis oponentes.
b) Contabilizar os valores.
c) Considerar os fatores humanos.
d) Levantar a situação financeira da empresa.
e) Conhecer os pontos fracos.

04. As informações devem cumprir alguns requisitos. Diante dessa afirmação, assinale a alternativa incorreta sobre tais requisitos.

a) Autenticidade
b) Integridade
c) Não repúdio
d) Custo baixo
e) Disponibilidade

05. Para melhorar a segurança de um sistema, deve-se prioritariamente considerar alguns aspectos. Sobre este assunto, leia as asserções e assinale a alternativa correta.

I. Conhecer os possíveis oponentes;

II. Contabilizar os valores;

III. Considerar os fatores humanos;

IV. Conhecer os pontos fracos.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) Somente as asserções I, II e III estão corretas.
d) Somente as asserções II, III e IV estão corretas.
e) As asserções I, II, III e IV estão corretas.

06. Quando falamos em segurança da informação, antes de cogitarmos a possibilidade de nos munir com aparatos tecnológicos, devemos prioritariamente fazer um levantamento e nos questionar sobre alguns aspectos. Diante do exposto, assinale a alternativa incorreta.
a) O que minha empresa quer proteger?
b) Por que minha empresa quer proteger?
c) Qual o orçamento da proteção?
d) Minha empresa quer proteger de que?
e) Como minha empresa deve proteger?

REFLEXÃO

Este capítulo introdutório nos posicionou no assunto que norteará nossa disciplina.

Compreendemos a importância da Segurança das Informações que trafegam intermitentemente por toda a empresa. Apesar desta grande relevância, notamos a grande resistência que ainda existe nas empresas em assumir o quesito Segurança das Informações como sendo prioritário tanto quanto a lucratividade é vista.

LEITURA

Recomendamos a leitura do Estudo de Caso publicado por Mendes (2013) e intitulado: "Segurança da Informação em Microempresas – Estudo de Caso". Detalhes sobre esta pesquisa encontram-se no item Referências Bibliográficas deste capítulo.

Apresentaremos, subsequentemente, a síntese desta pesquisa:

O supracitado pesquisador realizou um estudo de caso, aplicando um questionário em **oito Microempresas** a fim de investigar de que forma elas trabalhavam com a questão de segurança dos dados no dia a dia. Tais empresas situam-se nos Estados de São Paulo e Paraná e atuam no setor da informática.

Diante deste contexto de área de atuação, o pesquisador subentendeu que os entrevistados possuíam boa noção dos problemas que abrangem a segurança no uso da Tecnologia.

Resultados obtidos:

▪ **Backup das Informações:** quando perguntados se realizam alguma forma de backup para com os seus dados digitais, a maioria dos entrevistados foi positiva quanto à resposta: 87% dos entrevistados realizam o backup.

▪ **Controle de Acesso:** no que tange a controlar o acesso às máquinas da empresa, primeiramente na questão de autenticação, os resultados obtidos foram bem dispersos, onde apenas 50% das empresas utilizam algum sistema de login para acesso aos computadores da empresa. E quanto à restrição de acesso ao computador principal da empresa, os resultados também não foram muito satisfatórios, sendo que metade das empresas questionadas permite que terceiros utilizem livremente suas máquinas. Outro grande fator de risco na área de TI são os dispositivos de armazenamento móveis. Como se tratam de ferramentas que costumam ser utilizadas com grande freqüência e em diversas máquinas, acabam facilmente sendo infectadas por diversos tipos de softwares maliciosos. Pelos resultados obtidos, 75% das empresas entrevistadas não restringem o uso dos dispositivos em suas máquinas principais.

▪ **Senhas:** no que tange a senhas, quando questionadas se usavam uma mesma senha para múltiplos serviços, 62% das empresas afirmaram que preferem não ter mais de uma senha para se lembrar, o que não é favorável à questão segurança, já que se um invasor acabar por descobrir a senha, ele poderá ter acesso a todo o conteúdo que a empresa acreditaria estar sendo mantido seguro.

▪ **Questões Financeiras:** questionadas sobre seus investimentos em softwares de antivírus/antispywares, interessante relevar que independente de qual foi a escolha de cada empresa, notou-se que a maioria (75%) preferiu utilizar softwares gratuitos para garantir a sua proteção. Quando questionados sobre o uso de firewall, a maioria foi positiva quanto ao uso do mesmo, no qual a maioria também optou pelos meios gratuitos de proteção, especialmente o firewall nativo do próprio sistema operacional. Câmeras de monitoramento e outros equipamentos que auxiliam no controle de acesso também colaboram na segurança das informações. Junto à pesquisa, todas as empresas abordadas concordam na total importância em equipamentos de monitoramento de acesso ao local. Porém, mesmo atuando no ramo de informática, tendo acesso mais fácil a estes produtos, o interesse em investir na segurança física não é de grande prioridade, onde apenas 50% responderam ter grande interesse em investir neste quesito, outros 38% possuem breve interesse e 12% restantes não possuem interesse de investimento.

Considerações finais da pesquisa realizada:

Através de sua pesquisa, Mendes (2013) concluiu que as empresas entrevistadas não priorizam a segurança de seus dados, apesar de atuarem todas no setor da Tecnologia e terem conhecimento sobre a importância de tal segurança. Ou seja, muitas vezes, mesmo cien-

tes da importância da segurança e reconhecedores de ferramentas e procedimentos que a proporcionem, constatou-se certo receio por parte dos entrevistados ao serem questionados sobre o uso de seus recursos para tratar da segurança de seus dados digitais. No entanto, e por se tratarem de Microempresas que atuam diretamente na área de TI, ainda possuem um nível de atitude favorável quanto à segurança, no qual as posicionam em uma situação mais vantajosa quanto às pequenas empresas de diversos outros ramos de atuação. Porém, a preocupação quanto à questão financeira reflete um modo de pensar compartilhado pela grande maioria dos microempresários de diversos ramos. Com este pensamento de sempre posicionar a lucratividade em primeiro plano, além do fato de que destinar capital para segurança não traz retorno algum, acabam não compreendendo a real importância da prevenção de um futuro prejuízo.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, L. C. M.; MOREIRA, J. **Gerenciamento da Política da Segurança da Informação.** Tecnologias, Infraestrutura e Software (TIS), v.1, nº 2, p. 130-137, set-dez, 2012.

BREMER, C. F. Redes de Cooperação. Revista: **Produtos e Serviços:** Fábrica do Futuro – entenda hoje como vai ser sua indústria amanhã, Edição Especial, p. 99-104, dezembro, 2000.

CASTILHO, J. O Ciclo de Vida da Informação. **Revista Saúde Business**, disponível em: http://saudebusiness.com/noticias/o-ciclo-de-vida-da-informacao/ , 7 de maio de 2013.

FONTES, E. L. G. **Políticas e Normas para a Segurança da Informação.** Editora Brasport, Rio de Janeiro, 2011.

LAUREANO, M. A. P.; MORAES, P. E. S. **Segurança como Estratégia de Gestão da Informação.** Revista Economia & Tecnologia, ISSN 1415-541X, Vol 8, Fascículo 3, p. 38-44, 2005

LIMA, F. J. **Estudo de Melhorias em Segurança de Informação.** Monografia de Pós Graduação (Especialização) em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, Universidade Tecnológica Federal do Paraná, Curitiba, 2013.

MENDES, B. **Segurança da Informação em Microempresas –** Estudo de Caso. Disponível em: http://www.profissionaisti.com.br/2013/07/seguranca-da-informacao-em-microempresas-estudo-de-caso/ , publicado em 18 de julho de 2013.

MOREIRA, S. E. M.; CORDEIRO, M. F. R. **Desenvolvimento de Procedimentos de Segurança e Implantação de Firewall no Laboratório de Bioinformática da Rede Genoma Centro-Oeste.** Monografia de Graduação do Curso de Ciências da Computação da Universidade de Brasilia (UNB), 2002.

MULLER, E. J. **O Ciclo de Vida da Informação.** Disponível em: http://www.ezequieljuliano.com.br/?p=27 , 11 de abril de 2014.

NEIVA, D. **Gestão Inteligente de Dados e o Ciclo de Vida da Informação.** Disponível em: http://www.baguete.com.br/artigos/893/daniel-neiva/16/09/2010/gestao-inteligente-de-dados-e-o-ciclo-de-vida-da-informacao , Publicado em 16 de setembro de 2010.

NEVES, F. V. F. **Formação de Redes de Cooperação entre Empresas:** Análise dos Modelos de Comunicação e Informação. Monografia de conclusão de curso superior em Análise de Sistemas, Universidade de Ribeirão Preto – UNAERP, 2003.

NEVES, F. V. F.; GUERRINI, F. M.; SILVA, E. C. C. **Cooperação entre empresas, qualidade, recursos humanos e ambiente:** reflexões nas organizações empresariais. Editora Ottoni, Araraquara, p. 44 – 70, 2006.

OLIVEIRA, W. J. **Segurança da Informação Técnica e Soluções**. Editora Federal, 7ª Edição, 2001.

PEREIRA, E. N.; HOTENCIO, G. O.; NASCIMENTO, K. P. D.; SILVA, E. F. **Inteligência Competitiva**: o tratamento dos dados, informação e conhecimento às unidades de informação. XV Encontro Regional de Estudantes de Biblioteconomia, Documentação, Ciência e Gestão da Informação (EREBD), de 15 a 21 de janeiro de 2012.

SEMOLA, M. **Gestão da Segurança da Informação:** uma visão executiva. Editora Elsevier, 7ª Edição, 2003.

WADLOW, T. **Segurança de Redes**. Editora Campus, Rio de Janeiro, 2000.

WURMAN, S. R. **Ansiedade de Informação** – como transformar informação em compreensão. Editora: Cultura Editores Associados, 5ª edição, 1995.

2

Vulnerabilidades de Segurança

Olá, pessoal. Neste segundo capítulo iremos conhecer o ciclo de vida que compõe a informação e também falaremos, enfaticamente, sobre as vulnerabilidades que abrangem a segurança das informações, definindo o conceito e apresentando tipos de vulnerabilidades. Preparados? Vamos juntos!

OBJETIVOS

Nossos objetivos serão:

- Compreender o ciclo de vida da informação;
- Compreender a definição de vulnerabilidade;
- Analisar os principais tipos de vulnerabilidades;
- Conhecer exemplos de ferramentas para a análise de vulnerabilidades de segurança;
- Conhecer mecanismos de segurança das informações.

2.1 O Ciclo de Vida da Informação

Nós já sabemos, através de explicações encontradas no capítulo anterior, que as informações são provenientes de um conjunto de dados que foram lapidados. O que não sabíamos até o presente momento é que a informação possui um ciclo de vida finito. E que, quando este ciclo percorre a etapa final, as informações ali envolvidas devem ser adequadamente descartadas. Vejamos a citação subsequente que enfatiza tal afirmação.

> Toda informação possui um ciclo de vida. Um dado é gerado, permanece disponível pelo tempo necessário, passa por atualizações e, depois, ao perder sua serventia, deve ser descartado adequadamente. [...]
> Há quem sofra com a possibilidade de uma informação sigilosa ser acessada e comprometer o futuro da organização. E esse medo tem sentido: qualquer vazamento, seja de um arquivo sobre o histórico de saúde de um paciente, seja de dados sobre as finanças da instituição, é potencialmente desastroso para a reputação de quem deveria zelar pela proteção da informação (CASTILHO, 2013)

Após a leitura, constatamos a importância o de descarte da informação ser feito cuidadosamente, para que pessoas não autorizadas não tenham acesso a conteúdos sigilosos/indevidos, uma vez que os sistemas informatizados encontrados nas empresas integram os departamentos e suas respectivas massas de dados, permitindo um fluxo de informações intermitente por toda a empresa.

> Estamos vivendo na era de "sobrecarga de informações". As companhias estão muito dependentes em sistemas de planejamento empresarial, como ERP (Planejamento de Recursos Empresariais), SCM (Gestão da Cadeia de Suprimento) e CRM (Gestão de Relacionamento com Cliente) para automatizar e administrar seus recursos. Estes sistemas geram e abrigam uma vasta quantidade de dados que são bem estruturadas em sua própria maneira. Independente destes dados estruturados, as empresas também armazenam volumes enormes de dados não estruturados na forma de e-mail, Messenger, documentos e imagens. As informações estruturadas e não estruturadas devem ser armazenadas e retidas dentro destes sistemas (NEIVA, 2010).

Entre os benefícios gerados pela implantação de um ERP, podemos destacar:

- Integração das diversas áreas da empresa, pois os processos implementados no sistema transpõem os limites departamentais e permitem aos colaboradores terem maior visibilidade das responsabilidades;
- Adoção de um único sistema em toda a empresa, diminuindo o retrabalho de tarefas e melhorando a comunicação interna com informações padronizadas;
- Gestão baseada em processos, permitindo à empresa crescer sem ter necessidade de mudar de sistema, como também a garantia de todos os requerimentos globais, regionais e locais do negócio;
- Maior controle e gerenciamento dos processos internos da empresa, gerando implicitamente melhor desempenho e maior competitividade, provendo agilidade nos negócios, pois as decisões tomadas são baseadas em informações seguras e em tempo real; e
- Utilização de soluções voltadas à inteligência de negócios como Business Intelligence - BI, e ao relacionamento com o cliente, Customer Relationship Management - CRM.

Fonte: http://www.informazione4.com.br/cms/opencms/desafio21/artigos/gestao/organizando/0016.html

Estamos afirmando que as informações têm um Ciclo de Vida e já ressaltamos a importância de se realizar o descarte adequado de tais informações. Mas e as demais fases?

Vamos conhecer este ciclo!

Existem quatro fases através das quais percorre o ciclo de vida da informação. Em todas estas fases, a informação fica exposta a ameaças e tem riscos de integridade.

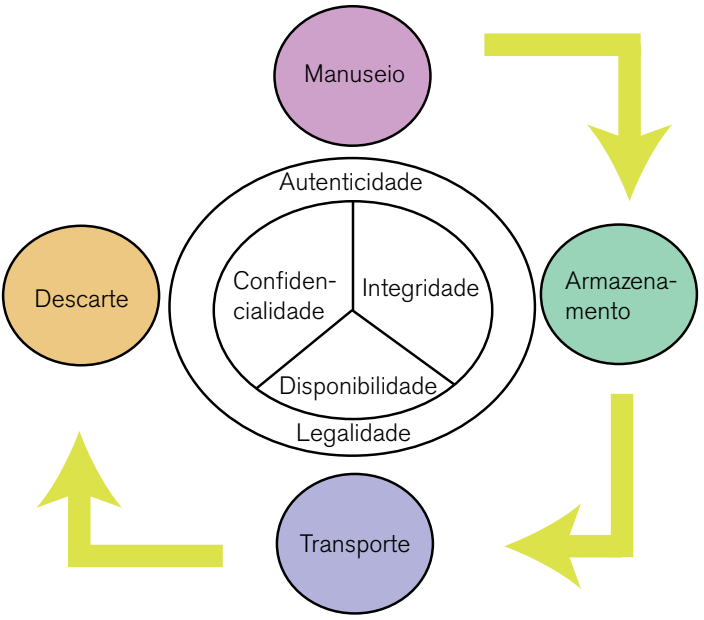


Figura 2.3 – Ciclo de Vida da Informação. Fonte: Adaptado de Muller (2014)

Vejamos a descrição sucinta de cada uma das fases:

MANUSEIO	é o momento em que a informação é criada e manipulada. Exemplos: digitar informações recém-geradas, utilizar uma senha de acesso para autenticação em um sistema, folhear papéis;
ARMAZENAMENTO	como o próprio nome já sugere, é o momento em que a informação é armazenada. E esta não se restringe ao armazenamento em banco de dados, mas, também, por exemplo, em uma anotação feita no papel e armazenada em arquivos físicos (estantes, prateleiras etc.);
TRANSPORTE	como também sugerido pelo nome, é o momento em que a informação é transportada, seja encaminhando-as através de correio eletrônico (e-mail), postagem convencional (Ex.: através do Correios), transmissão via fax, telefone etc.

DESCARTE	conforme deduzimos, o descarte ocorre no momento em que a informação não é mais útil. Desta forma, arquivos em papel são descartados em lixeiras, arquivos eletrônicos são apagados do banco de dados, CD's contendo informações sem serventia são descartados, e assim por diante.

Ao mencionarmos a etapa de descarte, é importante ressaltar que ela não pode ser realizada sem critérios. Descartar informações confidenciais, com valor legal, de qualquer forma, acarreta sérios impactos negativos.

Aliás, e em se tratando dos documentos com valor legal, deve-se atentar que o seu descarte deve obedecer aos prazos determinados em lei.

Outra ressalva diz respeito a documentos com valor histórico permanente, pois eles não poderão ser descartados. Um documento secreto, por exemplo, pode vir a ser considerado (a princípio) como sendo um documento de valor histórico permanente.

2.2 Vulnerabilidades de Segurança

A palavra vulnerabilidade nos faz logo pensar em fragilidade, certo? E a ideia é essa mesma!

Vulnerabilidades são os pontos fracos existentes nos ativos, que, quando explorados por ameaças, afetam a confiabilidade, a disponibilidade e a integridade das informações de uma organização (WADLOW, 2000, p. 12).

> As vulnerabilidades não seriam problema se não existissem as ameaças para explorá-las. As ameaças visam por meio das vulnerabilidades: explorar, danificar ou até mesmo roubar ativos das organizações. Com o passar dos tempos e à medida que a tecnologia progride, as formas de exposição ou vulnerabilidades irão crescer possibilitando assim o surgimento de novas ameaças (MOREIRA et al, 2008, p. 6)

Pontos fracos devem ser eliminados tão logo identificados. Neste aspecto, Nascimento (2013) afirma que, quando identificamos as vulnerabilidades, os riscos ficam mais bem dimensionados nos locais onde são expostos, facilitando, desta forma, a definição de medidas corretivas de segurança.

VULNERABILIDADE - Fragilidade de software, hardware ou procedimento que pode fornecer a um atacante a maneira para entrar em um computador ou rede e ganhar acesso às informações do ambiente.
AMEAÇA - Agente ou ação, espontâneo ou proposital, que aproveita das vulnerabilidades de um ambiente para conseguir seu intento.
RISCO – Calculado considerando o nível de impacto e a probabilidade de uma ameaça
ATAQUE – Incidência da ameaça sobre a vulnerabilidade.
EXPLOIT – Programa capaz de explorar uma vulnerabilidade.

Fonte: http://www1.univap.br/cccomp/Seminario/Palestra_Seguranca.pdf. Consultado em: 29/07/2015

2.2.1 Identificação de Vulnerabilidades

Após identificar e listar as ameaças, é possível diagnosticar quão vulnerável é, ou poderá tornar-se, o ambiente.

Vulnerabilidades são falhas ou fraquezas nos processos de segurança, nos projetos, no desenvolvimento ou nos controles internos de um sistema, os quais, se explorados, podem resultar em eventos não desejados. (STONEBURNER et al 2002, p. 15)

Métodos recomendados para a identificação de vulnerabilidades do sistema englobam o uso das fontes de vulnerabilidade, desempenho dos testes de segurança do sistema e desenvolvimento de uma lista de verificação de requisitos de segurança. Além disto, e de acordo com a ABNT (2008), outros métodos proativos englobam: testes e simulações, testes de invasão de sistemas, auditorias em códigos-fonte etc.

2.3 Principais tipos de Vulnerabilidades

De acordo com Modulo (2006) e Nascimento (2013), existem alguns tipos de vulnerabilidades (pontos fracos) que podem ser encontradas em uma organização no que tange ao contexto da segurança das informações, as quais:

VULNERABILIDADES NATURAIS	são aquelas decorrentes de fenômenos naturais, e que trazem riscos para equipamentos e informações. Exemplos: inundações, terremotos, maremotos, furacões etc.
VULNERABILIDADES FÍSICAS	são os ambientes que contêm pontos fracos em nível do espaço físico, comprometendo o armazenamento e gerenciamento correto das informações. Exemplos: instalações inadequadas para o trabalho, falta de extintores de incêndio, local desorganizado, pessoas não autorizadas transitando no local etc.
VULNERABILIDADES DE HARDWARE	são aquelas relacionadas aos equipamentos que apresentam defeitos de fabricação ou configuração inadequada, podendo permitir o ataque de vírus ou violações. Exemplos: a falta de atualizações dos programas e equipamentos não dimensionados corretamente;
VULNERABILIDADES DE SOFTWARE	são os pontos fracos existentes nos aplicativos de software, permitindo o acesso de indivíduos não autorizados. Por esta razão que os softwares são os preferidos dos elementos que buscam as ameaças. Exemplos: Aplicativos com configurações ou instalações inadequadas, programas de e-mail que permitem a execução de códigos maliciosos e falta de atualizações necessárias;
VULNERABILIDADES DE ARMAZENAMENTO	as informações são armazenadas em suportes físicos (disco rígido) ou magnéticos (CD, DVD, Cartão de memória, Pen drive etc). Suas utilizações inadequadas podem ocasionar uma vulnerabilidade, afetando, portanto, a integridade, a disponibilidade e a confidencialidade das informações. Consequentemente, isto pode danificar ou indisponibilizar os meios de armazenamento. Exemplos: defeito de fabricação de um meio de armazenamento, uso incorreto destes meios, prazo de validade e expiração ultrapassados;

VULNERABILIDADES DE COMUNICAÇÃO	são aquelas relacionadas com o tráfego de informações, os quais podem ser realizados através de fibra óptica, ondas de rádio, satélite ou cabos. Independentemente do meio escolhido, o sistema de comunicação escolhido deve ser seguro e garantir que as informações transmitidas alcancem o destino desejado sem intervenção alheia. Além disso, as informações trafegadas devem ser criptografadas, pois, caso haja alguma falha no processo, a informação não pode ser acessada por pessoas não autorizadas;
VULNERABILIDADES HUMANAS	são aquelas atitudes intencionais ou não que podem gerar vulnerabilidades às informações, como, por exemplo: uso de senha fraca, compartilhamento de credencial de acesso, falta de treinamentos para o usuário, a não consciência ou desconhecimento de segurança da informação e funcionários descontentes.

A vulnerabilidade de dados ocorre devido à interatividade com os clientes, fornecedores, parceiros de negócios, contatos pessoais etc., compartilhando informações, banco de dados, estratégias, tecnologias e enfim.

Nas operações *business-to-business*, apesar de uma empresa adotar um devido padrão de segurança com seus dados, por ser compartilhado, esses dados sigilosos poderão não estar seguros se a outra empresa que receber esses dados não adotar o mesmo padrão de segurança ou até mesmo ignorar a questão da segurança da informação, expondo, desta forma, informações importantes.

A dependência de empresas parceiras no *business-to-business* faz com que a segurança do negócio deve ser implementada em todos os perímetros da rede de negócios, ou seja: clientes, fornecedores e parceiros, devendo no mínimo utilizar o mesmo padrão de segurança internamente.

2.4 Ferramentas para análise de vulnerabilidades de segurança

As atuais medidas de segurança não garantem 100% de eficácia contra todos os possíveis ataques. A análise de risco, processo de avaliação das vulnerabilidades do sistema e das potenciais ameaças, é, portanto um componente essencial de qualquer programa de gerência de segurança da informação. O processo de análise identifica as prováveis conseqüências, ou riscos associados com as vulnerabilidades, e gera a base para estabelecimento de um programa de segurança que tenha um custo-benefício efetivo (MOREIRA et al, 2008).

Enfatizando a citação acima, devemos ter clareza de que nenhuma medida de segurança, por mais arrojada que seja, vá garantir/assegurar total proteção contra os ataques, pois a cada dia novos ataques podem surgir.

Dentro deste contexto, abordaremos alguns **tipos de *scanners*,** que, de acordo com Nakamura e Geus (2006), são programas de varredura utilizados para detectar possíveis vulnerabilidades em sistemas. Ou seja, são programas que procuram certas falhas de segurança que podem permitir ataques e até mesmo invasões.

Mesmo que você tenha apenas um único micro conectado à Internet, ele pode estar sujeito a ataques. Por esse motivo, é indispensável que você atualize com freqüência o antivírus e demais aplicativos, principalmente os que utilizam a conexão com a Internet, incluindo o próprio sistema operacional.

A partir do momento que você interliga os micros em rede e compartilha a conexão entre eles, os cuidados devem ser redobrados. Falhas nas configurações da rede ou mesmo desconhecimento por parte dos usuários podem tornar sua rede um prato cheio para os invasores. Os scanners servem justamente para checar as condições de segurança de um ou mais micros, de modo que você corrija eventuais falhas antes que alguém mal intencionado tenha chance de explorá-las, obtendo alguma vantagem ou causando prejuízo. Assim como os demais, estes programas também precisam ser atualizados com frequência, de modo a corrigir falhas descobertas mais recentemente.

Fonte: http://www.hardware.com.br/dicas/scanners-porta.html. Publicado em: 19 de fevereiro de 2008. Consultado em: 29/07/2015

Através destes *scanners*, de acordo com Nakamura e Geus (2006), é possível evitar desperdício de esforço com medidas de prevenção a ataques, uma vez que, quando uma vulnerabilidade é encontrada, deve ser medido seu grau de risco para a organização e então tratada para que uma ameaça não venha a explorá-la.

Neste contexto, há vários exemplos de aplicações que executam a análise de vulnerabilidades de uma rede ou *host*. Na sequência, detalharemos três tipos: o nmap, o languard e o nessus.

- NMAP

O Nmap é uma das ferramentas relacionadas à segurança e gerenciamento de redes mais difundidas no ambiente Linux. Ela foi inicialmente criada com o objetivo de detectar portas abertas em um destino, mas também pode ser utilizada para a localização de dispositivos em uma rede, ou para a verificação de alguns itens básicos de segurança, como portas abertas em um host (servidor ou estação), verificação de regras de firewall e testes de sistemas IDS (Intrusion Detection Systems), ou até mesmo detectar qual sistema operacional ou que tipo de equipamento se trata um determinado host. O scanner de vulnerabilidade Nmap é muito utilizado na auditoria dos firewalls, que são estruturas de hardware e software que isolam a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e outros não. Ele é um pacote muito utilizado e por isso está disponível em todas as principais distribuições. Pode ser instalado usando o yast (SuSE), yum (Fedora), urpmi (Mandriva), ou outro gerenciador de pacotes disponível (KUROSE e ROSS, 2007).

- Languard

O languard é um software que registra os eventos e pesquisa vulnerabilidades de segurança em uma rede. Entre os benefícios da utilização dessa ferramenta em uma rede estão: a detecção e controle de falhas de segurança, como falhas de patches (atualização de segurança) e para cada vulnerabilidade encontrada, apresenta uma solução de segurança ou service packs (pacote de atualização de segurança), contas não utilizadas, identificação de portas abertas e permite varrer um ou mais IP's.

Permite agendar scanners periódicos e comparar com execuções anteriores, permitindo ainda, configurar o tipo de vulnerabilidade a ser pesquisada (ausência de patches, erros de configurações, dentre outros) e exportar resultados em XML. Ele detecta uma grande quantidade de vulnerabilidades que estiverem em um sistema operacional, uma aplicação, banco de dados, etc, seja ele Windows, Linux, Solaris, Mac OS ou um roteador (GFI NETWORK SECURITY, 2008 apud MOREIRA et al, 2008, p. 9).

- NESSUS

O Nessus tem exatamente a função de encontrar "brechas" na máquina local, na rede ou em uma rede de computadores. Ele é dividido em “Nessusd” (servidor) e “nessus” (cliente), ambos com versões para sistemas operacionais Linux e Windows. Possui arquitetura cliente/servidor e baseada em plug-in . Cada plug-in é utilizado em uma vulnerabilidade de segurança que é enquadrada por órgãos competentes destinados a lançarem boletins de segurança a respeito de falhas em sistemas de informação (SANTOS, 2005 apud MOREIRA et al, 2008, p. 10).
O Nessus pode ser utilizado para descobrir worms e backdoors instalados em estações de trabalho e servidores. A ferramenta tem atualização freqüente e suas funcionalidades incluem relatórios completos, scanning de um grupo de hosts e buscas de vulnerabilidades em tempo real. O Nessus é software que tem o objetivo de fazer verificação remota e segura de vulnerabilidades nos hosts de uma rede (OLIVEIRA et al, 2002 apud MOREIRA et al, 2008, p. 10).

2.5 Mecanismos de segurança das informações

2.5.1 A Criptografia de Dados

A Criptografia é o estudo de princípios e técnicas através dos quais se torna possível transformar informações em sua forma original para outra forma irreconhecível/ilegível, a fim de que possa apenas ser reconhecida/lida por seu destinatário devido. Ou seja, é a ciência e a arte de escrever mensagens em forma cifrada ou em código.

A Criptografia é parte de um campo de estudos que trata das comunicações secretas e sigilosas, que tem por finalidade, dentre outros fatores explicitados por Neves (2003):

SIGILO	somente os usuários autorizados terão acesso a informação;
INTEGRIDADE	garantia oferecida ao usuário de que a informação correta e original não foi alterada, nem acidentalmente ou intencionalmente;
AUTENTICAÇÃO DO USUÁRIO	processo que permite ao sistema verificar se a pessoa que está se comunicando é de fato quem alega ser;
AUTENTICAÇÃO DE REMETENTE	processo que permite ao usuário verificar se a mensagem recebida foi de fato enviada pelo remetente informado;
AUTENTICAÇÃO DO DESTINATÁRIO	consiste em se obter uma prova de que a mensagem enviada foi mesmo recebida pelo destinatário devido;
AUTENTICAÇÃO DE ATUALIDADE	consiste em provar que a mensagem é atual, não se tratando de uma mensagem antiga que está sendo reenviada.

CONEXÃO

Dica de filme de ação que fala sobre supercomputadores e criptografia: "A SENHA" (*Swordfish*).

Basicamente, o que define a segurança de uma criptografia computacional é a quantidade de bits aplicados a ela. Por exemplo, uma chave de 8 bits gera apenas 256 combinações diferentes, pois este é o resultado de 2 elevado a 8. Isto prova que a criptografia de 8 bits não é de fato segura, pois qualquer um

que contar com tempo suficiente é capaz de resolvê-la. Imagine agora quantas combinações diferentes existem para uma chave de 128 bits. Para quebrar uma chave destas no método da tentativa e erro, seria necessária uma década e centenas de milhares de computadores. (fonte: http://www.tecmundo.com.br/seguranca/1334-o-que-e-criptografia-.htm, consultado em 04/04/13)

> Os computadores "entendem" impulsos elétricos, positivos ou negativos, que são representados por 1 ou 0. A cada impulso elétrico damos o nome de bit (BInary digiT). Um conjunto de 8 bits reunidos como uma única unidade forma um byte.
> Nos computadores, representar 256 números binários é suficiente para que possamos lidar a contento com estas máquinas. Assim, os bytes possuem 8 bits. É só fazer os cálculos: como um bit representa dois tipos de valores (1 ou 0) e um byte representa 8 bits, basta fazer 2 (do bit) elevado a 8 (do byte) que é igual a 256.
> Os bytes representam todas as letras (maiúsculas e minúsculas), sinais de pontuação, acentos, caracteres especiais e até informações que não podemos ver, mas que servem para comandar o computador e que podem inclusive ser enviados pelo teclado ou por outro dispositivo de entrada de dados e instruções. (Escrito por Emerson Alecrim, extraído de: http://www.infowester.com/bit.php, consultado em 04/04/2013)

De acordo com Stallings (2007), há duas maneiras básicas de se criptografar mensagens: através de códigos ou através de cifras.

2.5.2 Criptografia Através de Código

A criptografia através de código procura esconder o conteúdo da mensagem através, obviamente, de códigos preestabelecidos entre as partes envolvidas na troca de mensagens.

Imagine o exemplo em que, em uma guerra, um batalhão tem duas opções de ação contra o inimigo: atacar pelo lado esquerdo do inimigo ou simplesmente não atacar. A decisão depende da avaliação de um general posicionado em um local estratégico e distante da posição de ataque deste batalhão. É definido entre as partes (general e batalhão) que, se for enviada uma mensagem com a palavra "beriu", o exército deverá atacar pela esquerda; mas, se for enviada uma mensagem com a palavra "ragenci", não deve haver ataque. Com isso, mesmo que a mensagem caia em mãos inimigas, nada terá significado coerente.

O problema deste tipo de solução é que, com o uso constante dos códigos, em algum momento eles serão facilmente decifrados. Outro problema é que só é possível o envio de mensagens predefinidas (combinadas previamente). Por exemplo: não há como o general mandar seu exército atacar pela direita, pois nenhuma mensagem para este tipo de ação foi preestabelecida.

2.5.3 Criptografia Através de Cifra

O outro método usado para criptografar mensagens é a cifra, técnica na qual o conteúdo da mensagem é cifrado através da mistura e/ou substituição das letras da mensagem original. A mensagem é decifrada fazendo-se o processo inverso ao ciframento. Os principais tipos de cifras, conforme explicitado por Singh (2002) e Stallings (2007), são:

2.5.3.1 Cifra de Transposição "Cerca-de-ferrovia":

Uma mensagem é separada letra sim, letra não em duas linhas (que lembram os trilhos de uma ferrovia), como no exemplo:

A mensagem:

"O QUE VOCE LE HOJE E OURO AMANHA"

Muda para:

O U V C L H J E U O M N A
Q E O E E O E O R A A H

Após, coloca a segunda linha logo em sequência da primeira (variações de quantidade de linhas e como uni-las é possível aqui). Então, a mensagem cifrada fica:

O U V C L H J E U O M N A Q E O E E O E O R A A H

2.5.3.2 Cifra de deslocamento (ou substituição monoalfabética) de Cézar (Júlio Cézar):

Assim como visto já anteriormente, cada letra de uma mensagem é simplesmente substituída por outra que dista desta três posições para a direita. Exemplo, o A seria substituído pelo D, o F pelo J, e assim por diante. Considera-se que o alfabeto seja circular, i.e., depois do Z, vem o A novamente.

A mensagem:

O	Q	U	E	V	O	C	E	L	E	H	O	J	E	E	O	U	R	O	A	M	A	N	H	A

Muda para:

R	T	Y	H	W	R	F	H	N	H	K	R	M	H	H	R	Y	U	R	D	P	D	Q	K	D

Princípio de Kerckhoff: "A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave".

A cifra de substituição pode usar um alfabeto arranjado de qualquer maneira entra as 403.291.461.126.605.635.584.000.000 possíveis. Um truque é pegar uma frase-chave (transformando-a de modo a remover espaços e letras repetidas) e a partir dela colocar as letras do alfabeto que faltam.

Se a frase é, por exemplo, o nome "Jose Diogo da Silva", ficaria

JOSEDIGALVXYWZBCFHKMNPQRT

E a substituição ficaria:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	W	Z
J	O	S	E	D	I	G	A	L	V	X	Y	W	Z	B	C	F	H	J	K	M	N	P	Q	R	T

A falha das substituições monoalfabéticas acabam sendo quebradas por análise de frequência de letras.

2.5.3.3 Cifra de Substituição Polialfabética

O diplomata francês Blaise de Vigenère (Séc. XVI) bolou o sistema de cifras de substituição polialfabética (publicado em 1586) que durou quase 3 séculos indecifrável.

Neste sistema, usa-se a frase original em letras minúsculas, como, por exemplo: "oquevocelehojeeouroamanha".

Neste caso, deve-se tirar todos os espaços e pontuação (eles enfraquecem o código)

Escolhe-se uma palavra chave (do código), por exemplo REBECA

Esta palavra chave é repetida sob a frase original quantas vezes for necessária, como no exemplo abaixo:

o	q	u	e	v	o	c	e	l	e	h	o	j	e	e	o	u	r	o	a	m	a	n	h	a
R	E	B	E	C	A	R	E	B	E	C	A	R	E	B	E	C	A	R	E	B	E	C	A	R

Substitui-se cada letra da frase original pela correspondente da linha que começa com a letra do código abaixo dela. Deste modo, o "o" primeiro fica (da linha do R) "F". A mensagem fica:

o	q	u	e	v	o	c	e	l	e	h	o	j	e	e	o	u	r	o	a	m	a	n	h	a
R	E	B	E	C	A	R	E	B	E	C	A	R	E	B	E	C	A	R	E	B	E	C	A	R
F	U	V	I	X	O	T	I	J	I	J	O	A	I	F	S	W	R	F	E	N	E	P	H	R

Ou seja, a mensagem ficaria: FUVIXOTIJIJOAIFSWRFENEPHR

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2.5.3.4 Cifra de Substituição de Polígramos

Utiliza um grupo de caracteres em vez de um único caractere individual para a substituição da mensagem. Este método consiste em uma escrita que se baseia em um conjunto de símbolos cujo significado é conhecido por poucos, permitindo com isto que se criem textos que serão incompreensíveis aos que não saibam o padrão de conversão necessário para a sua leitura.

2.5.3.5 Cifra de substituição por deslocamento

Ao contrário da cifra de César, não usa um valor fixo para a substituição de todas as letras. Cada letra tem um valor associado para a rotação através de um critério. Por exemplo, cifrar a palavra "CARRO" utilizando o critério de rotação "023" seria substituir "C" pela letra que está 0 (zero) posições à frente no alfabeto, o "A" pela letra que está 2 (duas) posições à frente, e assim por diante, repetindo-se o critério se necessário.

A principal vantagem das cifras em relação aos códigos é a não limitação das possíveis mensagens a serem enviadas, além de ser tornarem mais difíceis de serem decifradas. As cifras são implementadas através de algoritmos associados a chaves, longas sequências de números e/ou letras que determinarão o formato do texto cifrado. (Disponível em: http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm. Acesso em: 04/04/13)

Um algoritmo nada mais é do que uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa. Ele não responde a pergunta "o que fazer?", mas sim "como fazer". Em termos mais técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa.
Embora você não perceba, utiliza algoritmos de forma intuitiva e automática diariamente quando executa tarefas comuns. Como estas atividades são simples e dispensam ficar pensando nas instruções necessárias para fazê-las, o algoritmo presente nelas acaba passando despercebido. (Fonte: http://www.tecmundo.com.br/programacao/2082-o-que-e-algoritmo-.htm, consultado em 04/04/13)

CONEXÃO

Dica de filme biográfico que fala sobre criptografia: "UMA MENTE BRILHANTE" (A Beautiful Mind).

2.6 Chave Criptográfica

Uma chave criptográfica é um valor secreto que modifica um algoritmo de encriptação. A fechadura da porta da frente da sua casa tem uma série de pinos. Cada um desses pinos possui múltiplas posições possíveis. É como quando alguém coloca a chave na fechadura. Ou seja, cada um dos pinos é movido para uma posição específica. Se as posições ditadas pela chave são as de que a fechadura precisa para ser aberta, ela abre; caso contrário, não (Fonte: http://portalwebrs.com.br/gerenc5ad6r/upload_arquivos/Apostila%20Informatica%20Instrumental%20I.pdf, p. 25, consultado em 24/04/2013)

2.7 Aspectos relevantes da Criptografia

A criptografia é essencial para a troca de informações através da internet, mas mesmo com tanta segurança, ela jamais será capaz de garantir absoluta integridade do conteúdo. Sempre vão existir pessoas capazes de desenvolver técnicas para quebrar estas chaves, por este motivo é que novas técnicas são criadas a cada dia e as existentes aperfeiçoadas (Fonte: http://olhardigital.uol.com.br/negocios/central_de_videos/o-que-e-criptografia, consultado em 26/04/2013)

Todos nós utilizamos a criptografia e, às vezes, sem nos darmos conta de que a estamos utilizando. Diante disto, é importante ressaltar alguns aspectos sobre as desvantagens da utilização da criptografia, uma vez que não há como previnir que um intruso:

- Apague todos os seus dados, estando eles criptografados ou não;
- Modifique o programa para modificar a chave. Deste modo, o receptor não conseguirá decriptografar com sua chave original;
- Acesse o seu arquivo antes de ele ser criptografado.

As técnicas de criptografia oferecem seis tipos de serviços básicos, sem os quais não é possível realizar o comércio eletrônico seguro através da Internet, são eles:

1. Disponibilidade: garante que uma informação estará disponível para acesso no momento desejado;

2. Integridade: garante que o conteúdo da mensagem não seja alterado;;

3. Controle de Acesso: garante que o conteúdo da mensagem somente será acessado por pessoas autorizadas;

4. Autenticidade da origem: garante a identidade de quem está enviado a mensagem;

5. Não repudiação: previne que alguém negue o envio/recebimento de uma mensagem;

6. Privacidade (confidencialidade ou sigilo): impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem, garantindo que apenas a origem e o destino tenham conhecimento (Fonte: http://www.training.com.br/lpmaia/pub_seg_cripto.htm, consultado em 26/04/2013)

Levando-se em consideração, a título de exemplo, uma compra realizada através da Internet, podemos detectar a demanda por todos estes serviços nas etapas do processo de compra virtual.

Ainda sobre as transações realizadas através da Internet, apesar de terem "ganhado o gosto do público", alguns clientes ainda se sentem inseguros e desconfortáveis/com medo de realizarem compras *online*, temendo pela privacidade de seus dados.

Na criptografia assimétrica inserida no processo de assinatura digital, é utilizado primeiro a chave privada, pelo emissor da assinatura, o qual estará executando o algoritmo de ciframento, mas com o objetivo de assinar o documento, e não cifrá-lo. Posteriormente, qualquer usuário que deseje verificar a autenticidade da assinatura digital em questão, irá processar o algoritmo de deciframento, mas com o objetivo de verificar a assinatura digital, e não de decifrar o documento.

Portanto, a criptografia assimétrica permite a utilização das chaves nos dois sentidos (RIBEIRO et al 2010, p. 88)

A assinatura e a certificação digital serão subsequentemente detalhadas.

2.8 Assinatura Digital

De acordo com o portal eletrônico da Justiça Federal, http://www.jf.jus.br/cjf, a Assinatura Digital é uma tecnologia que permite dar garantia de integridade e autenticidade a arquivos eletrônicos. É um conjunto de operações criptográficas aplicadas a um determinado arquivo, tendo como resultado o que se convencionou chamar de assinatura digital.

A Assinatura Digital permite comprovar:

1. Que a mensagem ou arquivo não foi alterado; e
2. Que foi assinado pela entidade ou pessoa que possui a chave criptográfica (chave privada) utilizada na assinatura.

A Assinatura digital proporciona, eletronicamente, o não repúdio e a autenticação dos dados.

Além de estar relacionada a uma entidade emissora, uma assinatura digital se relaciona à transação em questão, sendo única para cada transação realizada pelo emissor e tendo sempre um prazo de validade determinado.
Para possibilitar a utilização de assinaturas digitais em transações comerciais e governamentais, foi criada e aperfeiçoada ao longo do tempo, uma Infraestrutura de Chaves Públicas (ICP), envolvendo padronizações, normas, procedimentos, orientações e leis. Envolvem ainda órgãos como Autoridades Registradoras (AR), Autoridades Certificadoras (AC) e outros. A Certisign, maior empresa brasileira em tecnologia com foco exclusivo nas soluções que utilizam Certificação Digital, explica aos usuários, entre outros detalhes, que não há necessidade de se processar a assinatura digital da mensagem completa. Para tornar o custo de tempo de processamento da assinatura digital eficiente, ela é gerada a partir do valor de hash da mensagem.
A certificação digital certifica a autenticidade da assinatura digital combinando aspectos tecnológicos e jurídicos. Ela vem sendo utilizada no Brasil para atribuir valor legal a documentos eletrônicos e para garantir sua eficácia probatória.

Os ambientes de infraestruturas de chaves públicas precisam estar sob critérios de segurança rigorosos, desde a Autoridade Certificadora até o usuário do certificado digital.
Nesta visão, uma infraestrutura de chave pública é uma combinação de tecnologia e processos que vinculam a identidade do titular da chave privada sua respectiva chave pública, utilizando a tecnologia assimétrica de criptografia (RIBEIRO et al 2010, p. 85).

Em síntese, a assinatura digital envolve dois processos: o resumo (hash) e a encriptação deste resumo (hash). Ou seja, primeiramente é feito um resumo da mensagem através de algoritmos. A isto dá-se o nome de hash, cujas características são:

- Deve ser impossível encontrar a mensagem original a partir do hash da mensagem;
- O hash deve parecer aleatório, mesmo que o algoritmo seja conhecido. Uma função de hash é dita forte se a mudança de um bit na mensagem original resultar em um novo hash totalmente diferente;
- Deve ser impossível encontrar duas mensagens diferentes que levam a um mesmo hash.

Aqui cabe uma ressalva: se as mensagens possíveis são infinitas, mas o tamanho do hash é fixo, é impossível impedir que mensagens diferentes levem a um mesmo hash. De fato, isto ocorre. Quando se encontram mensagens diferentes com hashs iguais, é dito que foi encontrada uma colisão de hashes. Um algoritmo onde isso foi obtido deve ser abandonado.

- As funções de hash estão em constante evolução para evitar que colisões sejam obtidas. Cabe destacar porém que a colisão mais simples de encontrar é uma aleatória, ou seja, obter colisões com duas mensagens geradas aleatoriamente, sem significado real. Quando isto ocorre os profissionais de criptografia já ficam atentos, porém para comprometer de maneira imediata a assinatura digital seria necessário obter uma mensagem adulterada que tenha o mesmo hash de uma mensagem original fixa, o que é teoricamente impossível de ocorrer com os algoritmos existentes hoje. Desta forma, garante-se a integridade da assinatura (Fonte: http://www.oficinadanet.com.br/artigo/430/assinatura_digital, consultado em 29/04/2013)

Um hash é uma sequência de bits geradas por um algoritmo, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F). É a transformação de uma grande quantidade de informações em uma pequena quantidade. Essa sequência busca identificar um arquivo ou informação unicamente. Por exemplo, uma mensagem de correio eletrônico, uma senha, uma chave criptográfica ou mesmo um arquivo. É um método para transformar dados de tal forma que o resultado seja (quase) exclusivo. Além disso, funções usadas em criptografia garantem que não é possível a partir de um valor de hash retornar à informação original.
Como a sequência do hash é limitada, muitas vezes não passando de 512 bits, existem colisões (sequências iguais para dados diferentes). Quanto maior for a dificuldade de se criarem colisões intencionais, melhor é o algoritmo.

Fonte: adaptado de http://www.nfp.fazenda.sp.gov.br/inf_tecnicas.shtm. Consultado em: 24/04/2013

Gerado o hash, deve ser feita a criptografia do mesmo (com chave pública). O autor/emissor usa sua chave privada para assinar a mensagem e armazenar o resumo criptografado junto à mensagem original (não criptografada).

Após, um novo resumo é gerado, a partir da mensagem armazenada, a fim de verificar a autenticidade do documento. Este novo resumo é analisado e comparado à assinatura digital. No entanto, e para que seja possível fazer isto, é necessário descriptografar a assinatura, obtendo o resumo (hash) original.

A história da Assinatura Digital:
Em 1976, Whitfield Diffie (5/6/1944, matemático e criptográfico) e Martin Hellman (2/10/1945, criptográfico) descreveram primeiramente a noção de um esquema de assinatura digital, sem saber exatamente a dimensão que representaria aquilo.
Apenas mais tarde, Ronald Rivest, Adi Shamir, e Len Adleman (sendo os dois primeiros criptógrafos e o ultimo cientista de computadores além de biólogo molecular) inventaram o algoritmo RSA (que deriva das inicias de seus respectivos nomes) que poderia ser usado para assinaturas digitais primitivas.
O primeiro pacote de software amplamente comercializado a oferecer a assinatura digital foi o Lotus Notes 1.0 (sistema cliente-servidor de trabalho colaborativo e e-mail, concebido pela Lotus Software – do IBM Software Group), em 1989, que usava o algoritmo RSA.

Desde então, já havia sido notado que este esquema básico não era muito seguro. Como prevenção, aplicava-se primeiro uma função de criptografia hash para a mensagem e após o algoritmo RSA ao resultado.
Outros esquemas de assinatura digital foram logo desenvolvidos depois do RSA, o mais antigo sendo as assinaturas de Lamport, de Merkle (também conhecidas como árvores de Hash) e as de Rabin.
Em 1984, Shafi Goldwasser, Silvio Micali, e Ronald Rivest tornaram-se os primeiros a rigorosamente definir os requerimentos de segurança de esquemas de assinatura digital. Eles descreveram uma hierarquia de modelos de ataque para esquemas de assinatura, e também apresentaram o esquema de assinatura GMR, o primeiro que podia se prevenir até mesmo de uma forja existencial contra um ataque de mensagem escolhida.

Disponível em: http://pt.wikipedia.org/wiki/Assinatura_digital. Acesso em 24/04/2013

2.9 Certificação Digital

Garantir a segurança com a proteção das informações dos sistemas corporativos deve ser a preocupação constante de uma empresa, visando a assegurar que estas não sejam acessadas por terceiros não autorizados ou corrompidas por estarem suscetíveis às ações de vírus provenientes do sistema interno de mensagens ou pela internet, que podem resultar em prejuízos devastadores para a organização. Assim como as empresas, pessoas comuns também prezam pelo sigilo de suas informações pessoais e das armazenadas em seu computador. Segundo o CERT (Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil), foram comunicados cerca de 300.000 ataques à segurança da informação, de janeiro a junho de 2009, e boa parte destes incidentes está ligada a ações de cibercriminosos para capturar dados de internautas, como números de cartão de crédito, senhas bancárias e de informações trocadas através de redes sociais, seja verbalmente ou por escrito em salas de bate-papo e outras redes.

A Internet e o mundo digital nos proporcionam acesso ilimitado a qualquer tipo de informação, trazendo facilidades na comunicação entre pessoas e instituições. Em contraste, ainda há margem para a insegurança, pois, por exemplo, como garantir que quem está realizando uma compra virtual é realmente quem afirma ser? Ou seja, o anonimato nas transações virtuais gera probabilidade de risco de segurança das informações que estão sendo acessadas.

> Com o crescimento da demanda em segurança de transações comerciais que ocorrem por intermédio de redes eletrônicas, públicas ou privadas, a certificação digital desponta como tecnologia que fornece confiabilidade e segurança para usuários e que, com outrastecnologias, é utilizada como instrumento para estabelecer um adequado fluxo de informações e regulamentações na comunicação entre empresas e sociedade.
>
> A Certificação Digital foi criada justamente para solucionar preocupações relacionadas à segurança e proteção na Internet. Com o objetivo de combater a fraude e os crimes digitais, inclusive o pishing (roubo da identidade), os certificados garantem a identificação do autor de uma transação, mensagem, documento, e asseguram que nenhuma informação foi alterada, garantindo a sua integridade (RIBEIRO et al 2010, p. 83).

Mais detalhadamente, a Certsign expõe que a Certificação Digital proporciona:

> - Controle de acesso a aplicativos e assinatura eletrônica de documentos, através de identificação e de comprovação segura da identidade em questão;
> - Garantia de autenticidade do documento ou mensagem;
> - Validade jurídica dos documentos assinados impossibilitando o repúdio à autoria e ainda; e
> - Possibilidade de sigilo e privacidade fazendo com que apenas o servidor ou destinatário de uma mensagem interprete corretamente a informação (Fonte: http://www.certisign.com.br/certificacaodigital, consultado em 01/03/2012)

A Certificação Digital garante a autenticidade das informações trafegadas na rede virtual. Algumas de suas aplicações envolvem as transações na utilização de: NF-e, e-CPF e e-CNPJ; no IRPF (Imposto de Renda de Pessoa Física), IRPJ (Imposto de Renda de Pessoa Jurídica) etc. Nestes casos, é utilizada a ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira).

O Certificado Digital é uma credencial que identifica uma entidade, seja ela empresa, pessoa física, máquina, aplicação ou site na web. Um documento eletrônico seguro permite ao usuário se comunicar e efetuar transações na internet de forma mais rápida, sigilosa e com validade jurídica.
Os Certificados Digitais são compostos por um par de chaves (Chave Pública e Privada) e a assinatura de uma terceira parte confiável – a Autoridade Certificadora – AC. As Autoridades Certificadoras emitem, suspendem, renovam ou revogam certificados, vinculando pares de chaves criptográficas ao respectivo titular. Essas entidades devem ser supervisionadas e submeter-se à regulamentação e fiscalização de organismos técnicos (Fonte: http://hotsite.certisign.com.br/conectividadesocial/certificado-digital.html, consultado em 29/04/2013)

Para que a certificação digital garanta integridade, autenticidade, confidencialidade e não repúdio das informações assinadas, por meio eletrônico, é necessário que uma terceira parte ou uma estrutura de mediação ateste e emita os certificados necessários. No Brasil, essa infraestrutura governamental é a Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sendo ela que estabelece o sistema de certificação digital governamental que se relaciona com as empresas (Government to Business- G2B) e com o cidadão (Governmemt to Citizen - G2C).

O processo da Assinatura e Certificação Digital
A função hash realiza o mapeamento de uma sequencia de bits (todo arquivo digital é uma sequencia de bits) de tamanho arbitrário para uma seqüência de bits de tamanho fixo, menor. O resultado é chamado de hash do arquivo. Os algoritmos da função hash foram desenvolvidos de tal forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que, a partir do hash, seja impossível reproduzir a sequência que o originou.

O signatário de um documento (quem assina o documento) ao aplicar a função hash está gerando uma espécie de "impressão digital" do conteúdo do documento. Permitindo verificar sua integridade.
O hash é então criptografado com a chave privada do signatário.
Ao criptografar o hash com sua chave privada o signatário estará juntando a sua própria "impressão digital", isto é, ele gerou o hash para garantir a integridade do documento e o critpgrafa com a chave privada, para gar\ntir a autoria, ou autenticidade do documento.
Nesse momento o "pacote" é composto de: original + assinatura digital (hash criptografado).
Para completar o "pacote", finalmente, o certificado digital do signatário é agregado.
Agregar o certificado ao pacote, "autentica a assinatura", uma vez que o certificado permite verificar a identidade do signatário.
O certificado permite a imediata verificação da assinatura digital.
Primeiramente analisamos o certificado para verificar a identidade do autor da assinatura. (lembrando que o certificado digital é assinado por uma AUTORIDADE CERTIFICADORA, que identificou o titular do certificado)
Utilizamos a chave pública que ele contém para descriptografar o hash, que havia sido criptografado com a chave privada do signatário.
Se for possível realizar essa operação está comprovada a autenticidade (autoria) do arquivo.
O proprio certificado digital é um arquivo assinado digitalmente, por uma Autoridade Certificadora, que é denominada como o 3º elemento de confiança, isto é um elemento externo em quem os envolvidos no processo (signatário e destinatário da mensagem ou arquivo) confiam.

Fonte: http://www.jf.jus.br/cjf/tecnologia-da-informacao/identidade-digital/o-que-e-assinatura-digital. Consultado em 24/04/2013).

2.10 O processo da assinatura e certificação digital

Uma ICP (Infraestrutura de Chave Pública) tem a finalidade de regulamentar, com efeito jurídico/valor legal, a certificação das assinaturas digitais.

A ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) foi instituída pela Medida Provisória 2.200-2, de 24 de agosto de 2001, que cria o Comitê Gestor da ICP-Brasil, a Autoridade Certificadora Raiz Brasileira e define as demais entidades que compõem sua estrutura. A partir dessa Medida Provisória, foram elaborados os regulamentos que regem as atividades das entidades integrantes da Infraestrutura de Chaves Públicas Brasileira: Resoluções do Comitê Gestor da ICP-Brasil, as Instruções Normativas e outros documentos (Fonte: http://www.praticacertificacao.com.br/site/content/institucional/icpbrasil.php, consultado em 29/04/2013)

A ICP-Brasil é controlada pelo Instituto Nacional de Tecnologia da Informação, o ITI que é a autoridade certificadora raiz (primeira autoridade da cadeia de certificação brasileira – AC Raiz), uma autarquia federal vinculada à casa Civil da Presidência da República que tem como função credenciar as Autoridades Certificadoras (ACs) e as Autoridades Registradoras (ARs) por meio de supervisão e auditorias. A ICP-Brasil é responsável pelo conjunto de técnicas, práticas e procedimentos a serem implementados pelas organizações, com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chaves públicas

Fonte: Ribeiro et al (2010)

CONEXÃO

Assista ao vídeo institucional apresentando a estrutura do Instituto de Tecnologia da Informação pela Certificação Digital no Brasil: http://www.youtube.com/watch?v=4c0vaDrkIDU&feature=channel_page.

ATIVIDADES

01. Sobre o Ciclo de Vida da Informação, leia as asserções e assinale a alternativa correta.

I. O descarte ocorre no momento em que a informação não é mais útil;

II. Documentos com valor histórico permanente podem ser descartados quando se julgar que deles não são mais úteis;

III. Documentos com valor legal podem ser descartados, porém obedecendo aos prazos determinados em lei.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) As asserções I e III estão corretas.
d) As asserções II e III estão corretas.
e) Somente a asserção III está correta.

02. Sobre os tipos de vulnerabilidades, leia as asserções e assinale a alternativa correta.

I. Vulnerabilidades Naturais são, por exemplo: pessoas não autorizadas transitando no local;

II. Vulnerabilidades de Hardware englobam, por exemplo: a falta de atualizações dos programas e equipamentos não dimensionados corretamente;

III. Vulnerabilidades de Software englobam, por exemplo: aplicativos com configurações ou instalações inadequadas.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) Somente a asserção III está correta.
d) As asserções I e II estão corretas.
e) As asserções II e III estão corretas.

REFLEXÃO

Este foi um capítulo um tanto complexo.

Compreendemos o Ciclo de Vida da Informação e exploramos as vulnerabilidades acerca da segurança das informações organizacionais. Sobre este aspecto aprofundamos mais ainda abordando mecanismos de segurança. Ou seja, vimos todo o processo de crifagem/codificação de uma mensagem, importância e aplicação. Além disto, aprendemos a diferenciar e detectar a aplicação da assinatura e certificação digital.

LEITURA

Após todo aprendizado tido no decorrer deste capítulo, você deve estar se questionando quem é o órgão regulamentador dos certificados e assinaturas digitais. Pois bem, vamos conhecer mais sobre este assunto subsequentemente.

A Medida Provisória nº 2.200-1, de 27 de julho de 2001, reeditada pela MPv nº 2.200-2 de 2001, institui a Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil e dá outras providências. Quanto ao Comitê Gestor da ICP Brasil, a referida Medida Provisória institui:

> [...]
> Art. 5o Compete ao Comitê Gestor da ICP-Brasil:
> I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;
> II - estabelecer a política, os critérios e as normas técnicas para licenciamento das AC (Autoridade Certificadora), das AR (Autoridade de Registro) e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;
> III - estabelecer a política de certificação e as regras operacionais da AC Raiz;
> IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;
> V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;
> VI - aprovar políticas de certificados e regras operacionais, licenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;
> VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e
> VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.
> [...]
>
> (Fonte: http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-1.htm, consultado em 29/04/2013)

O decreto 3.872 de 18/07/2001 estabelece as competências e composição do CG-ICP.

Pelas leis brasileiras em vigor, toda AC deve utilizar-se de chave RSA de comprimento de no mínimo 2048 bits, devendo este valor ser revisto periodicamente, de acordo com as novas definições publicadas pelo CG ICP-Brasil (Comitê Gestor da ICP-Brasil).

A fim de garantir a segurança da infraestrutura de chaves públicas, há a necessidade de cuidados na distribuição dos pares de chaves (pública e privada), evitando assim ataques como o ataque MITM (Man-In-The-Middle / Ataque por Homem ao Meio). Neste tipo de ataque, o invasor interage entre duas partes que estejam se comunicando, sem que nenhuma das partes perceba o que está ocorrendo.

Suponha que um adversário obtenha um par de chaves (pública/privada) para utilizar no ataque e que, de alguma forma, ele consiga trocar a chave pública de A pela sua. O adversário passa a monitorar a linha de comunicação. Quando um criptograma for enviado para A, o adversário intercepta o canal tendo acesso ao criptograma e não deixa que ele chegue ao destinatário A. O adversário decifra o criptograma, altera a mensagem conforme sua conveniência e a envia para A com a chave pública correta de A, de forma que A consiga abrir a mensagem. Da mesma forma, quando A enviar uma assinatura digital, o adversário intercepta a mensagem enviada e a substitui por outra que ele cria conforme sua conveniência e divulga como se fosse assinada por A. Para evitar esse tipo de ataque, as ACs operam como uma terceira parte confiável, certificando a validade do par de chaves no momento da sua criação. Outra necessidade técnica para a segurança em assinaturas digitais é a utilização de algum esquema de codificação, que processe algum tipo de codificação na mensagem que será assinada, tornando-a pseudoaleatória e evitando, assim, possíveis ataques por mensagem escolhida (PEREIRA, 2009, p. 79)

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTIN, A. L. **Comércio Eletrônico:** seus aspectos de segurança e privacidade. Revista de Administração, versão 38, nº 2, p. 49-61, 1998.

CASTILHO, J. **O Ciclo de Vida da Informação**. Revista Saúde Business, disponível em: http://saudebusiness.com/noticias/o-ciclo-de-vida-da-informacao/ , 7 de maio de 2013.

CERT. **Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil.** URL: <http://www.cert.br/>. Acessado em 01/03/2012.

CERTISIGN. Site institucional. **Certificação digital.** URL: <http://www.certisign.com.br/certificacaodigital>. Acessado em 01/03/2012.

ICP-Brasil. **Infraestrutura de chaves públicas brasileira.** URL: <http://www.icpbrasil.gov.br/>. Acessado em 01/03/2012.

ITI. Instituto Nacional de Tecnologia da Informação. **Autoridade certificadora brasileira raiz.** URL: <http://www.iti.gov.br/twiki/bin/view/ITI/Apresentacao>. Acessado em 01/03/2012.

KUROSE, J. F.; ROSS, K. W. Redes de Computadores e a Internet (Uma abordagem top-down). São Paulo: Pearson, 2007.

NAKAMURA, T. E.; GEUS, L. P. **Segurança de Redes em Ambientes Cooperativos.** São Paulo, Berkeley, 2002.

MÓDULO. **Curso Básico de Segurança da Informação** (Academia Latino-Americana de Segurança da Informação). Módulo Security, 2006.

MOREIRA, J. R. H.; TEIXEIRA, C. S.; TAVARES, C. C.; VERBENA, M. F.; QUINTAO, P. L. **Scanners de Vulnerabilidades Aplicados a Ambientes Organizacionais.** Revista Eletrônica da Faculdade Metodista, nº 5, ISSN 19810377, jul/dez, 2008.

MULLER, E. J. **O Ciclo de Vida da Informação.** Disponível em: http://www.ezequieljuliano.com.br/?p=27 , 11 de abril de 2014.

NAKAMURA, E. T.; GEUS, L. P. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Novatec, 2007.

NASCIMENTO, N. J. **Ameaças e Vulnerabilidades da Informação.** Como Precaver. Disponível em: http://www.portaleducacao.com.br/educacao/artigos/48819/ameacas-e-vulnerabilidades-da-informacao-como-precaver , Publicado em 5 de julho de 2013.

NEIVA, D. **Gestão Inteligente de Dados e o Ciclo de Vida da Informação.** Disponível em: http://www.baguete.com.br/artigos/893/daniel-neiva/16/09/2010/gestao-inteligente-de-dados-e-o-ciclo-de-vida-da-informacao , Publicado em 16 de setembro de 2010.

PEREIRA, S. R. **O sistema criptográfico de chaves públicas RSA.** Dissertação apresentada à Universidade Católica de Santos, UNISANTOS. 2008.

SANTOS, B. R. **Detecção de Intrusos Utilizando o Snort.** Computação da Universidade Federal de Lavras, Graduação Latu Sensu em Administração de Rede Linux, 2005.

SILVA, L. G. C.; SILVA, P. C.; BATISTA, E. M.; HOMOLKA, H. O.; AQUINO, I. J. S.; LIMA, M. F. **Certificação digital: conceitos e aplicações, modelos brasileiro e australiano.** 1. ed. São Paulo: Editora Ciência Moderna, 2008.

STALLINGS, W. **Criptografia e segurança de redes. 4ª edição** Ed. Prentice Hall, 2007.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. Risk Management Guide for Information Technology Systems. Gaithersburg: **NIST - National Institute of Standards and Technology.** Disponível em: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, julho, 2002.

VOLPI, M. M. **Assinatura digital: aspectos técnicos, práticos e legais.** Rio de Janeiro: Axcel Books do Brasil, 2001.

WADLOW, Thomas A. **Segurança de redes:** projeto e gerenciamento de redes seguras. Tradução: Fábio Freitas da Silva. Rio de Janeiro: Campus, 2000.

3

Ameaças e Ataques à Segurança das Informações

Olá, pessoal. Neste terceiro capítulo conheceremos a distinção entre ameaças e ataques à segurança da informação. Da mesma forma, fazeremos um detalhamento de ambos, de forma a conhecer alguns aspectos muito importantes. Isto as faz necessário porque é muito comum haver a confusão entre estes dois conceitos, como se fossem sinônimos.

Além disso, é importante ressaltar que muitas organizações acabam se equivocando em estabelecer políticas de segurança das informações (tanto dos dados armazenados localmente no servidor da organização quanto daqueles trafegados através da Internet). Ou seja, notamos que muitas organizações estabelecem políticas de segurança sem conhecer detalhadamente as ameaças e os ataques (internos e externos).

Então vamos juntos!

OBJETIVOS

Nossos objetivos serão:

- Conhecer o conceito de ameaças;
- Conhecer os principais tipos de ameaças;
- Conhecer o conceito de ataques;
- Conhecer os principais tipos de ataques.

3.1 Introdução

O uso de sistemas de informações e redes mudou de maneira drástica com o advento da internet. Atualmente, infraestruturas críticas são suportas sobre a internet como o gerenciamento de energia, sistemas de transporte, coordenação de finanças etc. Isso influencia diretamente a maneira como as companhias realizam negócios, como os governos disponibilizam seus serviços aos cidadãos e como as pessoas trocam informações e se comunicam. Tudo isto influi na natureza da informação trocada.

A quantidade de dispositivos com conexões "always on" (sempre conectados) também aumentou significativamente. Assim, houve um aumento da interconectividade, e os sistemas de informações e redes tendem a ficar expostos cada vez mais a um maior número de ameaças e vulnerabilidades.

As questões relativas à segurança de informações não se aplicam apenas a sistemas informatizados. No entanto, a informatização trouxe novas questões a serem discutidas. Se voltássemos cerca de um século (ou um pouco mais) no tempo e verificássemos como era a segurança de sistemas bancários, perceberíamos que você precisaria invadir fisicamente um banco para roubá-lo. Hoje, isto não é necessário. Atacantes do mundo todo podem tentar burlar a segurança em sistemas bancários, pois estes sistemas estão conectados à internet.

É necessário discutir questões novas sobre segurança e formar uma "cultura de segurança".

Os armários e as fechaduras para arquivos confidenciais hoje são digitais.

A informação é um ativo que, como qualquer outro relevante para o negócio, possui valor para a organização e necessita ser adequadamente protegido. Além disso, as dependências dos sistemas de informação e serviços, as tendências e evoluções tecnológicas da computação, as interconexões de redes públicas e privadas e o compartilhamento de recursos expõem as organizações às mais variadas fontes de ameaças: fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo, inundação, blackouts, códigos maliciosos, hackers, entre outras.

Para grande parte das organizações, a informação e a tecnologia associada representam ativos valiosos. As organizações bem-sucedidas utilizam a tecnologia da informação para dirigem e agregarem valores aos seus negócios. Estas empresas, em virtude de atenderem regulamentações e da dependência de seus processos com a da tecnologia da informação, reconhecem a necessidade de gerir os riscos associados.

> A segurança da informação protege a informação contra ameaças no intuito de garantir a continuidade, minimizar os danos e maximizar os investimentos e oportunidades do negócio. A segurança da informação é obtida pela utilização de controles: políticas, práticas, procedimento, estruturas organizacionais e infraestruturas de hardware e software. É caracterizada pela preservação da confidencialidade, integridade e disponibilidade da informação, e visa preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização (GONÇALVES, 2008, p. 11).

Ou seja, quando nos referimos ao tema "segurança da informação", é imprescindível também abordar a gestão/análise de riscos, ameaças e ataques, uma vez que novas situações estarão sempre surgindo para vulnerabilizar a segurança. Especificamente abordando a Gestão de Riscos, trataremos de tal assunto no próximo capítulo.

Existem três fontes principais, conforme explicitado pelas normas da ABNT (2008), para que uma organização identifique seus requisitos de segurança:

• A primeira é o conjunto de princípios, objetivos e necessidades para o processamento da informação que uma organização tem de desenvolver para apoiar suas operações;

• A segunda é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm de atender;

• As duas anteriores são utilizadas como referências para desenvolver a principal fonte de requisitos de segurança, que é derivada da avaliação de riscos, processo responsável por identificar as ameaças aos ativos, as vulnerabilidades com suas respectivas probabilidades de ocorrência e os impactos ao negócio.

Ou seja, entende-se a necessidade e importância de estabelecer políticas de segurança das informações trafegadas na rede. No entanto, deve-se primeiro detectar, analisar e "atacar" os riscos e ameaças organizacionais, a fim de se estabelecer uma política de segurança coerente e eficaz.

O que é segurança da informação?
A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.
A informação pode existir em muitas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Fonte: http://artigos.netsaber.com.br/resumo_artigo_16364/artigo_sobre_seguran%C3%87a_da_informa%C3%87%C3%83o>. Acessado em 06/07/2015

3.2 Ameaças à Segurança das Informações

De acordo com Shirey (2000), uma **ameaça** é potencial para a violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.

Ameaça: palavra, ato, gesto pelos quais se exprime a vontade que se tem de fazer mal a alguém, sinal, manifestação que leva a acreditar na possibilidade de ocorrer alguma coisa.
Sinônimos de Ameaça: advertência, bravata, cominação, intimação e prenúncio.

Fonte: Dicionário Online Português

Ameaças organizacionais são **situações externas**, pertencentes ao tempo atual ou futuras que, se não eliminadas, minimizadas ou evitadas pela empresa, podem (ou poderão) **afetá-la negativamente.**

No Livro "A Arte da Guerra", o autor Zun Tsu afirma: "Se conhecemos o inimigo (ambiente externo) e a nós mesmos (ambiente interno), não precisamos temer o resultado de uma centena de combates. Se nos conhecemos, mas não ao inimigo, para cada vitória sofreremos uma derrota. Se não nos conhecemos nem ao inimigo, sucumbiremos em todas as batalhas."

De acordo com dados publicados pelo CNASI – Congresso de Segurança da Informação, Auditoria e Governança TIC – (2013), as ameaças à segurança de uma organização estão relacionadas com a perda de uma (ou mais) das suas três características principais:

- Perda da Integridade: que acontece quando certa informação fica exposta ao manuseio de uma pessoa não autorizada, que acaba por efetuar alterações não aprovadas e sem o controle, provado ou corporativo do proprietário da informação;
- Perda de confidencialidade: ocorre quando há uma quebra de sigilo de uma determinada informação, como a senha de um usuário ou administrador, por exemplo, que permite que informações restritas, que deveriam estar acessíveis apenas para um determinado grupo de usuários, fiquem expostas;
- Perda de disponibilidade: que acontece quando a informação deixa de estar acessível, justamente, por quem necessita dela. É o caso que ocorre com a perda de comunicação com um sistema importante para a empresa, que pode acontecer com a queda de um servidor, de uma aplicação crítica de negócio, que pode apresentar uma falha, devido a um erro causado por motivo interno ou externo ao equipamento (CNASI, 2013).

No que tange às ameaças a rede de computadores ou sistemas, ainda de acordo com o CNASI (2013), estas podem vir através de agentes maliciosos, tais como os crakers. A fonte de motivação para este tipo de quebra de código pode ser oriunda de diversos fatores, a exemplo: notoriedade, vingança, dinheiro etc.

Importante fazermos uma "pausa" antes de continuarmos a detalhar o assunto, pois é comum encontramos os termos hackers e crakers (dentro outros). Vejamos a explicação no *box* a seguir.

"Hacker" e "cracker" podem ser palavras parecidas, mas possuem significados bastante opostos no mundo da tecnologia. De uma forma geral, hackers são **indivíduos que elaboram e modificam softwares e hardwares de computadores,** seja desenvolvendo funcionalidades novas ou adaptando as antigas. Já **cracker** é o termo usado para designar **quem pratica a quebra** (ou cracking) **de um sistema de segurança.**

Na prática, os dois termos servem para conotar pessoas que têm habilidades com computadores, porém cada um dos "grupos" usa essas habilidades de formas bem diferentes. Os **hackers utilizam todo o seu conhecimento para melhorar softwares de forma legal e nunca invadem um sistema com o intuito de causar danos.** No entanto, **os crackers têm como prática a quebra da segurança de um software e usam seu conhecimento de forma ilegal, portanto são vistos como criminosos.**

As denominações foram criadas para que leigos, e especialmente a mídia, não confundissem os dois grupos. Apesar de os termos serem mundialmente conhecidos, chamar alguns de “bons” e outros de “maus” não agrada a todos. Há quem acredite que tanto o hacker quanto o cracker são habilidosos e podem fazer as mesmas coisas.

Os termos mais corretos são os usados dentro da ética hacker: “White Hat” (Chapéu Branco), “Black Hat” (Chapéu Preto) e “Gray Hat” (Chapéu Cinza). Os hackers "Chapéu Branco" são pessoas interessadas em segurança e, na maioria das vezes, usam suas habilidades a favor das empresas, sendo 100% éticos em suas ações. São eles que ocupam os cargos de analista de sistema, especialista em TI ou outros empregos na área de informática.

Já os hackers "Chapéu Preto" são criminosos e, normalmente, especializados em invasões maliciosas de sites. Os hackers "Chapéu Cinza" têm as intenções de um Chapéu Branco, mas suas ações são eticamente questionáveis.

Apesar dessa contradição dentro do próprio cenário de profissionais da segurança, ainda muitos programadores aceitam os termos hacker e cracker como definições corretas. Diversos Fóruns sobre programação, blogs de tecnologia, sites como Wikipedia e até dicionários conceituam os hackers como profissionais do bem e crackers como criminosos.

Disponível em: http://olhardigital.uol.com.br/noticia/qual-a-diferenca-entrehacker-e-cracker/38024>. Acesso em: 03/10/2013

3.3 Principais Tipos de Ameaças

Existem vários tipos de ameaças à segurança das informações nas organizações. Neste item iremos conhecer algumas delas.

3.3.1 Códigos Maliciosos (Malware)

Códigos maliciosos (*malware*), de acordo com dados divulgados pelo Comitê Gestor da Internet no Brasil – CGI.br (2012), são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

> O termo "***malware***" é proveniente do inglês "***malicious software***" ("*software* malicioso mal-intencionado"); é um *software* destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Ele pode aparecer na forma de código executável, scripts de conteúdo ativo, e outros *softwares*."*Malware*" é um termo geral utilizado para se referir a uma variedade de formas de *software* hostil ou intruso.
>
> Fonte: https://pt.wikipedia.org/wiki/Malware

Dentre as diversas formas que estas ações danosas e atividades maliciosas podem ocorrer, ainda de acordo com o CGI.br (2012), temos:

- Explorar vulnerabilidades já existentes nos programas instalados;
- Autoexecutar mídias, tais como um pen drive, infectadas;
- Acessar páginas virtuais suspeitas através de navegadores vulneráveis;
- Sofrer ação direta de atacantes que realizam um ataque inserindo arquivos com códigos maliciosos no computador;
- Executar arquivos infectados anexados a, por exemplo, mensagens eletrônicas.

Após instalados no computador, estes códigos maliciosos passam a ter acesso ao dados ali armazenados, podendo executar ações como se fossem o usuário.

Mas o que motiva isto acontecer? Dentre diversos outros fatores, um atacante elabora e alastra códigos maliciosos para:

- Obter vantagens financeiras;
- Obter informações confidenciais para realizar, por exemplo, chantagem;
- Autopromoção;
- Vandalismo.

A seguir, iremos conhecer os principais tipos de códigos maliciosos.

3.3.1.1 Vírus

Vírus são programas elaborados especificamente para alterar nocivamente softwares instalados em um computador.

> Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que se possa tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que seu computador seja infectado é preciso que um programa já infectado seja executado. CGI.br (2012, p. 24)

Para facilitar o entendimento, vamos fazer um comparativo com o vírus (doença) que nos acomete. Estes vírus multiplicam-se, mas precisam de um hospedeiro. Eles aguardam o momento certo para efetuar o ataque escondem-se para não serem prontamente exterminados. De acerta forma, assim também ocorre com os vírus de computadores.

Antigamente, o principal meio de propagação dos vírus era através dos disquetes. Com o passar o tempo, e o desuso destes, começaram a surgir novos meios de propagação, como por exemplo do envio de e-mails e também pelo uso de ***pen drives*** infectados.

> Este pequeno dispositivo é um acessório prático e fácil de usar, compatível com praticamente qualquer sistema.
> Tecnicamente o pendrive é um dispositivo portátil de armazenamento com memória flash, acessível através da porta USB. Sua capacidade varia de modelo para modelo, mas os pendrives mais atuais já passam dos gigabytes de memória. Por ser pequeno e ter uma grande capacidade, ele já marcou a morte dos velhos e saudosos disquetes de 3,5 polegadas.

Os CDs até tentaram substituir os discos flexíveis, mas sua portabilidade e praticidade não é maior que a dos pendrives. Não há hoje nenhuma mídia portátil tão rápida na gravação e leitura dos dados, como é com os pendrives, o que os tornou populares muito rapidamente.

? CURIOSIDADE

O termo "pendrive", apesar de ser em inglês, não é utilizado nessa língua. Os países falantes da língua inglesa utilizam o termo "USB Flash Drive". Pendrive pode ter sido o nome escolhido por alguns países pelo fato de os primeiros dispositivos portáteis com memória flash terem sido criados com aparência que lembrava uma caneta ("pen" em inglês). Outra possibilidade é a de que estes acessórios são tão pequenos que podem ser considerados até mesmo mais práticos de carregar que uma caneta comum.

Disponível em: adaptado de: http://www.tecmundo.com.br/pendrive/844-o-que-e-pen-drive-.htm>. Acesso em: 30/08/2008. Adaptado.

Existem diferentes tipos de vírus:

• Os que ficam ocultos infectando arquivos armazenados no disco rígido do computador, além de também executarem atividades sem que o usuário tome conhecimento;

• Os que ficam inativos por um período e, após, executam uma série de atividades sem que o usuário tome conhecimento;

• Ou então, aqueles que ficam inativos por um período e acionam sua atividade em datas específicas.

Conforme publicado pelo CGI.br (2012, p. 24), alguns dos tipos de vírus mais comuns são:

VÍRUS PROPAGADO ATRAVÉS DO E-MAIL	recebido como um arquivo anexado ao e-mail cujo conteúdo induz o usuário a executá-lo. Ao fazer isto, o vírus infecta arquivos e programas e replica cópias de si mesmo para os contatos de e-mails armazenados no computador infectado;

VÍRUS DE SCRIPT	escrito em linguagem como VBScript e JavaScript por exemplo, e recebido ao acessar uma página Web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML;
VÍRUS DE MACRO	tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem, como, por exemplo, os que compõem o Microsoft Office (Word, Excel, Power Point etc.);
VÍRUS DE SMARTPHONE	se propaga de celular a celular por meio da tecnologia Bluetooth ou de mensagens multimídia. Esta infecção ocorre quando um usuário permite o recebimento do arquivo infectado e o executa em seu celular. Após infectar o aparelho, o vírus pode destruir, sobrescrever arquivos, remover contatos, drenar a carga de bateria, se propagar a outros celulares etc.

3.3.1.2 Worm

Worm pode ser confundido com o vírus, pois ele é também capaz de se propagar automaticamente pelas redes, emitindo cópias de si mesmo para outros computadores. Entretanto, o que o diferencia de um vírus, de acordo com o CGI.br (2012), é que o Worm executa diretamente suas cópias ou explora automaticamente as vulnerabilidades existentes em programas instalados em computadores.

Em função de consumirem muitos recursos, os Worm acabam afetando o desempenho de uma rede e, consequentemente, os computadores a ela ligados.

O processo de propagação e infecção de um Worm ocorre da seguinte forma, de acordo com o CGI.br (2012, p. 25):

1. Identificação dos computadores alvos: após infectar um computador, o Worm tenta se propagar e continuar o processo de infecção. Para tanto, necessita identificar os computadores alvos para os quais tentará se copiar, o que pode ser feito da seguinte forma:

- Efetuar varredura na rede e identificar computadores ativos;
- Aguardar que outros computadores contatem o computador infectado;
- Utilizar listas, predefinidas ou obtidas na Internet, contendo a identificação dos alvos;
- Utilizar informações contidas no computador infectado, como arquivos de configuração e listas de endereços de e-mail.

2. Envio das cópias: após identificar os alvos, o Worm efetua cópias de si mesmo e tenta enviá-las para estes computadores, por uma ou mais das seguintes formas:

- Como parte da exploração de vulnerabilidades existentes em programas instalados no computador alvo;
- Anexadas a e-mail;
- Via canais de IRC (Internet Relay Chat);
- Via programas de troca compartilhadas em redes locais ou do tipo P2P (Peer to Peer).

3. Ativação das cópias: após realizado o envio da cópia, o Worm necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:

- Imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas que estão sendo executados no computador alvo no momento do recebimento da cópia;
- Diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu computador;
- Pela realização de uma ação específica do usuário à qual o Worm está condicionado, como, por exemplo, a inserção de uma mídia removível.

4. Reinício do processo: após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o computador que antes era o alvo agora passa a ser também o computador originador dos ataques.

3.3.1.3 Bot e Botnets

O Bot é um programa (software) que permite que o computador infectado seja controlado remotamente por um operador, sem que isto seja percebido. Este tipo de controle pode ser feito, por exemplo, via IRC (*Internet Relay Chat*).

> O **IRC** (***Internet Relay Chat***) é um protocolo utilizado na Internet como troca de arquivos e de informações.
> O modo de comunicação e canais do IRC é a conversação de um canal, no qual os usuários enviam mensagens ao servidor que as reenvia a todos do mesmo canal.
> O IRC pode ser utilizado para execução de Botnets, onde o usuário lança o chamado Spam a milhares de computadores.
>
> Disponível em: http://www.infoescola.com/internet/internet-relay-chat-irc/

O processo de infecção e propagação de um bot é semelhante ao do Worm (ou seja propagação automática).

Ao se comunicar, de acordo com o CGI.br (2012), o invasor pode enviar instruções para que ações maliciosas sejam executadas, como, por exemplo, desferir ataques, furtar dados do computador infectado, enviar spam, etc.

Ao computador infectado por um bot, dá-se o nome de **zumbi,** em função de ele poder ser controlado remotamente, sem que isto seja percebido.

Já o termo **Botnet** é utilizado para descrever uma rede composta por milhares de computadores zumbis. Nesta rede, ações maliciosas são executadas pelos bots, dentre as quais:

- Negação de serviços;
- Propagação de outros códigos maliciosos;
- Coleta de informações dos computadores da rede;
- Envio de spam.

A seguir, o CGI.br (2012, p. 26) descreve o funcionamento básico de uma botnet:

> **1.** Um atacante propaga um tipo específico de bot na esperança de infectar e conseguir a maior quantidade possível de zumbis;
> **2.** Os zumbis ficam à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;

3. Quando o controlador deseja que uma ação seja realizada, ele envia aos zumbis comandos a serem executados, usando, por exemplo, redes do tipo P2P ou servidores centralizados;

4. Os zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlados;

5. Quando a ação se encerra, os zumbis voltam a ficar à espera dos próximos comandos a serem executados.

3.3.1.4 - Spyware

Spyware, de acordo com o CGI.br (2012), é um programa cuja finalidade é monitorar as atividades de um determinado sistema e enviar as informações coletadas para terceiros.

Ainda de acordo com o CGI.br (2012), o *Spyware* tem uso malicioso quando executa ações que comprometem a privacidade do usuário e a segurança do computador, como, por exemplo: monitorar e capturar informações de navegação do usuário, login e senhas.

Alguns exemplos de tipos de programas *spywares* são:

KEYLOGGER	captura e armazena teclas digitadas pelo usuário;
SCREENLOGGER	armazena a tela apresentada pelo monitor de vídeo e a respectiva posição do cursor nela (muito usado para capturar posições do cursor em sites de Internet Banking);
ADWARE	projetado para apresentar propagandas (com fins legítimos ou maliciosos).

3.3.1.5 Cavalo de Troia (*Trojan*)

Cavalo de Troia ou Trojan é um programa que executa funções maliciosas. Geralmente ele vem "dentro" de outros programas que o usuário precisa executar em seu computador para que funcionem (a exemplo: cartões virtuais, jogos etc). Além disso, podem ser instalados no computador sem o consentimento de seu dono por atacantes invasores.

De acordo com classificação divulgada pelo CGI.br (2012, p. 29), há diferentes tipos de trojans:

TROJAN DOWNLOADER	Instala outros códigos maliciosos, obtidos de sites na Internet;
TROJAN DROPPER	Instala outros códigos maliciosos, embutidos no próprio código do trojan;
TROJAN BACKDOOR	Inclui backdoors, possibilitando o acesso remoto do atacante ao computador;
TROJAN DOS	Instala ferramentas de negação de serviço e as utiliza para desferir ataques;
TROJAN DESTRUTIVO	Altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação;
TROJAN CLIKER	Redireciona a navegação do usuário para sites específicos com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas;
TROJAN PROXY	Instala um servidor de Proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam;
TROJAN SPY	Instala programas spywares e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante;

TROJAN BANKER	Coleta dados bancários do usuário, através da instalação de programas spywares que são ativados quando sites de Internet Banking são acessados. É similar ao trojan spy, mas com objetivos mais específicos.

Ou seja, os Trojans, independentemente o tipo, são de forma geral programas maliciosos que executam ações não autorizadas pelo dono do computador, as quais podem englobar: modificação, cópia, eliminação, bloqueio de dados e interferência no desempenho dos computadores.

Diferentemente dos outros tipos de malwares, os trojans não têm a capacidade de se autorreproduzir.

3.4 Ataques à Segurança das Informações

Até o presente momento, abordamos as ameaças à segurança das informações. Vamos a partir de agora aprofundar um pouco mais o assunto e tratar dos aspectos relacionados aos ataques.

No entanto, para darmos prosseguimento, vamos fazer uma breve distinção entre ameaças e ataques, de acordo com Shirey (2000):

AMEAÇA	é potencial para a violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade;
ATAQUE	derivado de uma ameaça inteligente, uma tentativa de burlar os serviços de segurança e violar as políticas de segurança de um sistema usando um método ou técnica com eficiência e eficácia consideráveis.

LEITURA

Agora que definimos, embora sucintamente, o conceito de ataque a segurança da informação, vamos acompanhar juntos a leitura de trechos de um artigo cujo título é: "Segurança da Informação: Internet sobre maior ataque da história", publicado em 28 de março de 2013 (o artigo na íntegra está disponível através do link: http://www.marcosassi.com.br/seguranca-da-informacao-internet-sofre-maior-ataque-da-historia)

*A **internet** ficou lenta por causa de um massivo ataque de negação de serviço a servidores em diversos países. Segundo o noticiário britânico BBC, o ataque afetou serviços populares, como a Netflix.*

A BBC diz que o problema começou com uma briga entre o Spamhaus, grupo europeu de combate ao spam, e a Cyberbunker, empresa holandesa de serviços de data center. O Spamhaus incluiu servidores da Cyberbunker numa lista de emissores de spam. A lista é usada pelos programas antispam para filtrar os e-mails.

O grupo diz que a empresa está por trás dos ataques, que teriam sido lançados em retaliação ao bloqueio. No site da Cyberbunker, há uma nota acusando a Spamhaus de incluir a empresa na lista de bloqueio indevidamente.

*A técnica usada pelos **criminosos** é a de negação de serviço. Para realizar um ataque desse tipo, primeiro um grande número de computadores são infectados com um programa maligno que permite controlá-los a distância. Depois, esses computadores zumbis são usados para inundar os servidores-alvo com solicitações de dados.*

A sobrecarga acaba impedindo o funcionamento dos servidores e da rede à qual estão ligados. Em geral, um ataque desse tipo envia algumas dezenas de gigabytes por segundo ao servidor-alvo, o que é suficiente para derrubá-lo. Mas, no caso do Spamhaus, o fluxo chega a 300 gigabytes por segundo, volume capaz de congestionar a internet.

Os ataques vêm sendo realizados em seguidas ondas. O alvo principal são os 80 servidores de DNS do Spamhaus espalhados por diversos países. Esse tipo de servidor traduz endereços como abril.com.br para um código numérico conhecido como endereço IP. Isso é necessário para que cada pacote de dados encontre seu destino."

Após a leitura do texto e, independentemente dos reais culpados do ataque, pudemos ter um pequeno exemplo de ataque que burlou o sistema de segurança da empresa Spamhaus de forma eficiente e eficaz.

3.5 Principais Tipos de Ataques

Os ataques são divididos entre Passivos e Ativos:

1. Ataques Passivos
   - Bisbilhotar ou monitorar transmissões.
     - Obter informações que estão sendo transmitidas.
     - Conversa telefônica, mensagem de e-mail, arquivo transferido, podem ter informações importantes ou confidenciais.

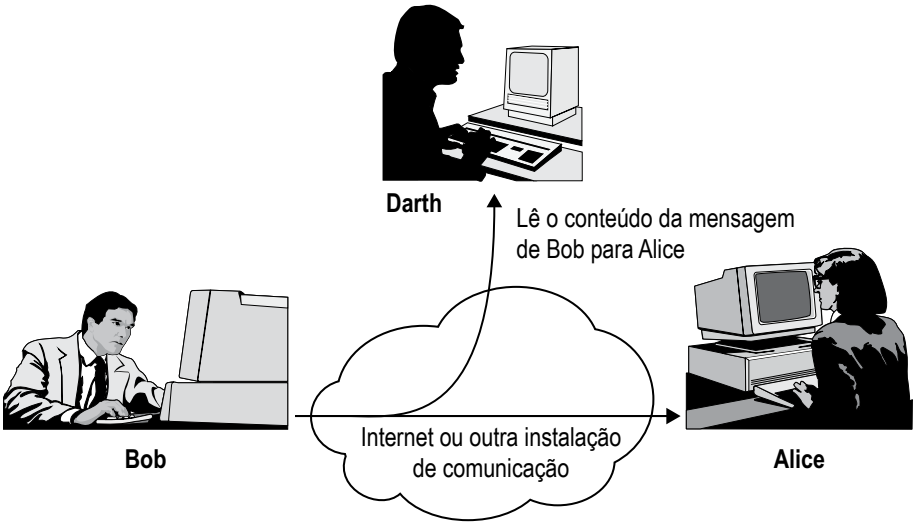


Figura 3.4 – Monitoramento de transmissões. Fonte: (STALLINGS, 2008).

   - Análise de Tráfego
     - Mais sutil.
     - Se for possível disfarçar o conteúdo das mensagens, mesmo que esta seja captada, não seria possível extrair as informações "de cara".

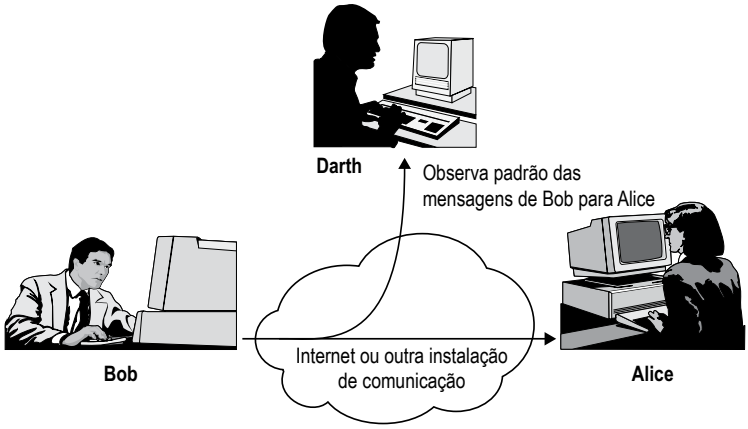


Figura 3.5 – Análise de tráfego. Fonte: (STALLINGS, 2008).

- Medida de segurança: impedir que alguém descubra o conteúdo destas.
    - Técnica mais comum é a criptografia.
    - O "intruso" poderia olhar o padrão dessas mensagens.
    - Também poderia determinar o local e a identidade dos hospedeiros da comunicação.
    - O "intruso" poderia observar a frequência e tamanho das mensagens trocadas.
    - Descobrir a "natureza" da comunicação.
- Ataques passivos são difíceis de detectar.
    - Não há alteração nos dados.
    - O tráfego de mensagens ocorre num padrão aparentemente normal.
    - Nem emissor nem receptor estão cientes de que um terceiro leu as mensagens ou observou o padrão de tráfego.
    - É viável impedir este tipo de ataque.
    - Foco na prevenção, e não na detecção.

2. Ataques ativos

- Envolvem modificação no fluxo de dados ou criação de um fluxo falso (4 tipos).
    - Disfarce
    - Entidade finge ser outra.

- Inclui uma das outras formas de ataque ativo (normalmente).

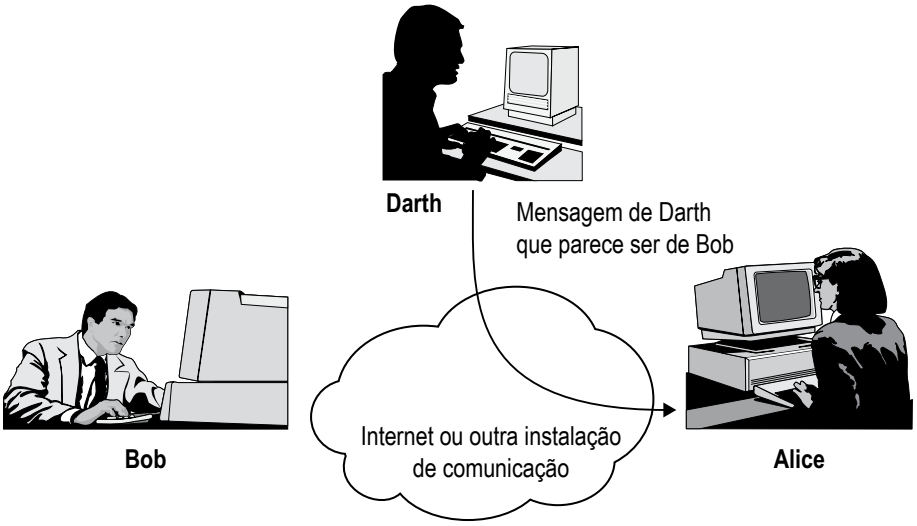


Figura 3.6 – Ataques ativos. Fonte: (STALLINGS, 2008).

- Repetição

Captura passiva de uma unidade de dados e subsequente transmissão para produzir um efeito não autorizado.

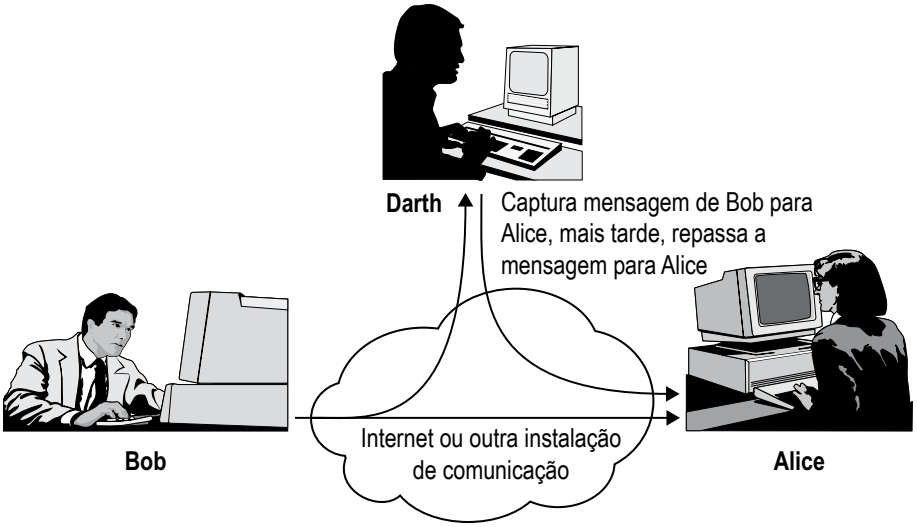


Figura 3.7 – Ataques por repetição. Fonte: (STALLINGS, 2008).

- Modificação de Mensagens

Alguma parte de uma mensagem legítima foi alterada.

Mensagens foram adiadas ou reordenadas para produzir um efeito não autorizado.

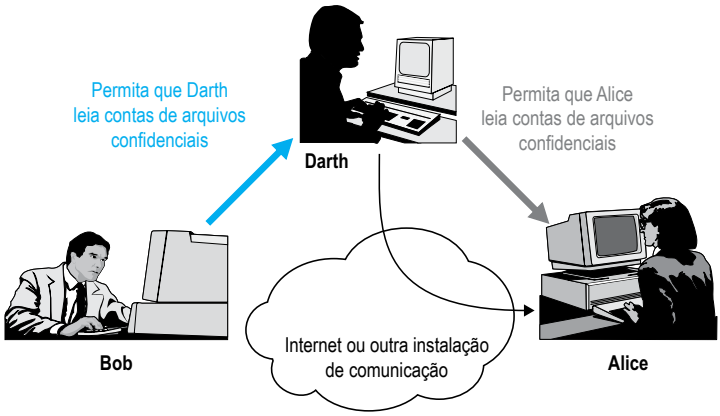


Figura 3.8 – Modificação de mensagens. Fonte: Adaptado de (STALLINGS, 2008).

- Negação de serviço

Impede ou inibe o uso ou gerenciamento normal das instalações de comunicação.

Ataque pode ter um alvo específico.

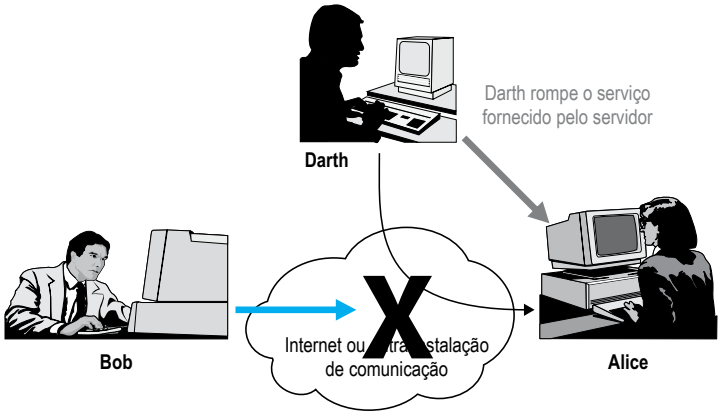


Figura 3.9 – Negação de serviço. Fonte: Adaptado de (STALLINGS, 2008).

- Medidas de segurança
  - Devido à grande quantidade de vulnerabilidades, é muito difícil de impedir ataques ativos.
  - Foco é na detecção de ataques ativos e recuperação de interrupções ou atrasos.

- Detecção pode ter efeito intimidador
  - Características opostas dos ataques passivos.
  - Ajuda na prevenção.
  - Agora que já sabemos mais sobre os ataques a sistemas computacionais, vamos ler um texto sobre o assunto e depois continuaremos falando mais sobre segurança.

Leia o texto abaixo extraído de (O´BRIEN, 2004)

Visa: estratégias para o controle da segurança global

Um dos maiores sistemas financeiros do mundo, a Visa Internacional, Inc., está escondido num inexpressivo edifício próximo de Washington, D.C. A Visa se empenha em manter sigilo em relação ao endereço em que se encontra. Seu nome não está indicado no prédio em que se localiza e é terminantemente proibido a qualquer repórter revelar o endereço da empresa. O centro de dados secreto é uma fortaleza de concreto à prova de terremotos e fogo, com portas que pesam mais de 2.200 quilos e um porão cheio de equipamentos de recuperação, possuindo janelas falsas para torná-lo semelhante a qualquer um das centenas de edifícios comerciais existentes na região. Isso pode ser considerado paranoia? Não quando você considera os riscos. Cinco minutos para uma parada de manutenção no sistema de processamento mundial da Visa, chamado de VisaNet, bloquearia US$ 55 milhões em transações de pagamentos, segundo cálculos da Foster City, uma empresa estabelecida na Califórnia.

"Não há algo como 99,9% de confiabilidade; esta deve ser de 100%", diz Richard L. Knight, vice-presidente sênior para operações na Inovant, Inc., subsidiária da Visa que opera seus centros de dados. "Algo menos que 100% e eu estarei procurando um novo emprego." Em 12 anos, a companhia esteve 98 minutos parada para manutenção. A Visa trava uma batalha contra as falhas e defeitos em duas ímpias frentes: sua instalação física de processamento é

protegida por diversas camadas de repetição e de cópias; e o departamento de TI da companhia criou software de teste para os equipamentos. Há mais de l bilhão de cartões especiais de pagamento Visa em todo o mundo, movimentando US$2 trilhões anuais em transações para 23 milhões de comerciantes e caixas automáticos e 21 mil membros de instituições financeiras da Visa. "Operamos a maior máquina de pagamentos do mundo", diz Sara Garrison, vice-presidente sênior para desenvolvimento de sistemas da Visa, na Califórnia."Durante o tempo que se leva para tomar um cafezinho, movimentamos o equivalente a todo o movimento de todos os mercados de valores do mundo durante 24 horas. Nossa velocidade cresce de 20 a 30% a cada ano, dobrando a cada três anos."

A Visa tem quatro centros principais de processamento para controlar tal carga, mas a instalação de Washington é a maior, passando por ali a metade das transações de pagamento de todo o mundo. Apesar de dividir o movimento com um outro centro em San Mateo, na Califórnia, caso ocorra algum problema, tem capacidade de receber instantaneamente todas as transações.

Realmente, tudo na infraestrutura de processamento da Visa — desde todos os centros de dados até os computadores, processadores individuais e chaves de comunicações — tem uma cópia. Até mesmo as cópias possuem uma cópia. Por exemplo, o centro de Washington tem em revezamento quatro unidades de suprimento contínuo de energia (apenas três são necessários) dirigidas pelo serviço local e apoiadas por um grupo de baterias e quatro geradores de força movidos a diesel de l megawatt. Os 100 mil litros de diesel armazenados no local são suficientes para abastecer o centro durante uma semana. As unidades de suprimento contínuo de energia protegem o centro de possíveis flutuações de energia. A instalação tem capacidade de refrigeração suficiente para fornecer ar-condicionado a 300 casas.

Calcula-se que os oito mainframes da IBM no centro de dados de Washington possam processar 3.000 MIPS (milhões de instruções por segundo). Juntos, no mundo todo, um poder de processamento de 7.000 MTPS pode realizar 10.000 autorizações de pagamentos de transações por segundo. A rede da Visa, uma das maiores redes particulares do mundo, possui cerca de 14,5 milhões de quilômetros de fios de cobre e de fibra ótica, e cada cliente Visa tem duas rotas na empresa por meio de canais comerciais.

O centro de processamento da área de Washington da Visa abriga 50 milhões de linhas de código em cerca de 300 aplicativos. Suas principais funções compreendem:

SISTEMA DE AUTORIZAÇÃO	esse sistema on-line com base em mainframes IBM movimenta um pedido de cartão de pagamento partindo do proprietário do cartão, passando pelo comerciante, indo ao banco, seguindo para o emissor do cartão e retornando ao comerciante;
SISTEMA DE PAGAMENTO E COMPENSAÇÃO	esse sistema conjunto de mainframes funciona toda noite e liquida as contas entre comerciantes, bancos de comerciantes e emissores do cartão;
SISTEMA DE DESCOBERTA DE FRAUDES	esse sistema on-line atua em servidores da Sun Microsystems e usa redes nervosas e algoritmos de reconhecimento de padrões para procurar fraudes em cada operação de pagamento;
DATAWAREHOUSE	essa imensa instalação de armazenamento é composta de 18 silos da StorageTechnology Corp. e uma biblioteca de fitas com 250.000 volumes que conservam durante sete anos os valores dos históricos das transações. Há um crescimento de 250TB de dados a cada mês.

Embora todas essas cópias e proteções contribuam para as superconfiáveis operações da Visa, elas são apenas parte da história. A cada verão, bem antes do momento de pico da época de processamento, a Visa realiza um teste completo de tensão, no valor de US$ l bilhão, no Centro de Escalabilidade e Desempenho da IBM, em Gaithersburg, Maryland, onde a IBM possui um poder de processamento de 14.000 MIPS. Os testes poupam meses de análises de pré-requisitos, planejamento e testes nas próprias instalações da Visa.

"Também temos falhas naquele ponto", diz MikeWolfson, vice-presidente sênior de engenharia na Inovant. "Assim, embora estejamos processando 5.000 mensagens por segundo, paramos um controlador de armazenamento e nos asseguramos de que o sistema não perde o ritmo." Esse tipo de teste completo

de volume — que a Visa não tem capacidade de realizar internamente — tem sido muito válido. "Por exemplo, vários aplicativos que rodavam perfeitamente na produção com cargas de pico, falharam quando a carga de teste foi aumentada para se ajustar a volumes projetados para a estação de férias seguinte" diz Wolfson.

ATIVIDADES

01. Existem três fontes principais para que uma organização identifique seus requisitos de segurança. Sobre esta afirmação, leia as asserções e assinale a alternativa correta.

I. A primeira fonte é um conjunto de princípios, objetivos e necessidades para o processamento da informação;

II. A segunda fonte é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais;

III. As duas primeiras fontes são utilizadas como referências para desenvolver a principal fonte de requisitos de segurança, que é derivada da avaliação de riscos.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) Somente a asserção III está correta.
d) As asserções I e II estão corretas.
e) As asserções I, II e III estão corretas.

02. As ameaças à segurança de uma organização estão sempre relacionadas com a perda de uma ou mais das seguintes características, as quais:

I. Perda de integridade.
II. Perda de confidencialidade.
III. Perda de performance.

a) Está correta somente a asserção I.
b) Está correta somente a asserção II.
c) Está correta somente a asserção III.
d) Estão corretas somente as asserções I e II.
e) Estão corretas somente as asserções II e III.

03. Sobre os tipos de vírus, leia as asserções e assinale a alternativa que preenche corretamente e respectivamente as sentenças abaixo:

I. _____ recebido como um arquivo anexado ao e-mail cujo conteúdo induz o usuário a executá-lo;

II. _____ escrito em linguagem como VBScript e JavaScript, por exemplo, e recebido ao acessar uma página Web ou por e-mail, como um arquivo anexo ou como parte do p´roprio e-mail escrito em formato HTML;

III. _____ tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem;

IV. _____ se propaga de celular a celular por meio da tecnologia Bluetooth ou de mensagens multimídia.

a) Vírus de script; Vírus propagado através de e-mail; Vírus de macro; Vírus de Smartphone.
b) Vírus propagado através de e-mail; Vírus de script; Vírus de macro; Vírus de Smartphone.
c) Vírus propagado através de e-mail; Vírus de macro; Vírus de script; Vírus de Smartphone.
d) Vírus de Smartphone; Vírus propagado através de e-mail; Vírus de script; Vírus de macro.
e) Vírus de Smartphone; Vírus de script; Vírus de macro; Vírus propagado através de e-mail.

REFLEXÃO

Neste capítulo conhecemos as diferenças entre ameaças e ataques à segurança das informações.

Detalhadamente conhecemos cada um destes conceitos e seus diferentes tipos.

O importante a enfatizarmos é que a organização deve trabalhar permanentemente de forma preventiva e não corretiva (quando os ataques já tiverem sido concretizados).

Falamos “permanentemente” porque, a cada dia, novos tipos de ameaças podem surgir, e a organização deve estar preparada para lidar com isso.

LEITURA

Recomendamos a leitura da reportagem: “Malware de Android simula desligar o aparelho para espionar os seus dados”, publicada no site: http://www.tecmundo.com.br/malware/75333-malware-android-simula-desligar-aparelho-espionar-dados.htm , em 21 de fevereiro de 2015.

Acompanhemo-na subsequentemente:

A AVG descobriu um novo malware para Android. Batizado de PowerOffHijack, ele explora uma vulnerabilidade se aproveitando do momento em que o usuário desliga o aparelho para espionar informações do dispositivo.

Ao ser instalado, o vírus exige permissões root para efetuar alterações no sistema. Quando o smartphone está prestes a ser desativado, o PowerOffHijack simula o processo de desligar o dispositivo, mostrando a animação característica e apagando a tela, porém faz com que o sistema continue funcionando.

O malware então aproveita o momento para obter suas fotos, efetuar ligações, enviar mensagens e acessar qualquer dado que esteja guardado no aparelho sem notificar o usuário. Um verdadeiro pesadelo para qualquer pessoa preocupada com segurança e privacidade.

Focos de infecção

Segundo a AVG, o PowerOffHijack atingiu mais de 10 mil dispositivos, a maioria na China, onde o aplicativo apareceu inicialmente através das app stores locais. O malware pode afetar dispositivos com Android 4.4 ou anterior.

Os antivírus mais recentes da AVG conseguem detectar a infecção, mas a recomendação da empresa é que os usuários retirem a bateria do smartphone quando quiserem ter certeza de que o aparelho está desligado.

Porém, a dica principal é sempre ficar de olho no que instala, especialmente em lojas de aplicativos não oficiais.

Conforme pudemos acompanhar através da leitura supracitada, devemos sempre estar atentos à procedência dos aplicativos instalados em nossos smartphones (e outros aparelhos eletrônicos como: tablets, notebooks, ipads etc.).

No entanto, devemos também estar cientes de que, embora haja antivírus, a cada dia novos vírus irão surgir e, até que se atualize um antivírus para que ele passe a detectar e sanar o problema, muitos danos podem ser causados.

A medida mais segura, portanto, sempre será a prevenção, que, neste caso, implica em averiguar a procedência do aplicativo e/ou arquivo antes de baixá-lo e instalá-lo.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. ABNT NBR ISO/EIC 27005:2008 : **Tecnologia da Informação:** Técnicas de Segurança: Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008.

CGI.br (Comitê Gestor da Internet no Brasil). **Cartilha de Segurança para Internet.** ISBN: 978-85-60062-54-6, versão 4.0, 2ª Edição, São Paulo, 2012.

CNASI (Congresso de Segurança da Informação, Auditoria e Governança TIC). **Ameaças à Segurança da Informação de uma Corporação.** Publicado em: http://www.cnasi.com.br/ameacas-a-seguranca-da-informacao-de-uma-corporacao/, 28 de novembro de 2013.

GONÇALVES, A. J. **Metodologias de Gerenciamento de Riscos em Sistemas de Tecnologia da Informação e Comunicação –** abordagem prática para conscientização e implantação nas organizações. Trabalho de Conclusão de Curso de Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores, Universidade Federal do Rio Grande do Sul, dezembro, 2008.

SHIREY, R. **Internet Security Glossary.** Networking Working Group. Disponível em: http://www.ietf.org/rfc/rfc2828.txt , acessado em 06/07/2015, publicado em 2000.

4

Gestão de Riscos em Segurança da Informação

Olá, pessoal. Agora que já falamos sobre as vulnerabilidades, ameaças e ataques à segurança das informações organizacionais, neste terceiro capítulo iremos falar sobre os riscos.

Vale enfatizar, já nesta apresentação de capítulo, que devemos estar cientes de que, por mais que a gestão de riscos seja feita de forma correta, estes podem ser minimizados, mas nunca extintos.

Vamos conhecer mais sobre este assunto? Vamos juntos!

OBJETIVOS

Nossos objetivos serão:

- Conhecer o conceito de Risco Organizacional;
- Conhecer a Gestão de Riscos;
- Conhecer as Etapas da Gestão de Riscos;
- Conhecer medidas de segurança para riscos organizacionais.

4.1 Introdução

Os termos risco e ameaças organizacionais são situações externas, pertencentes ao tempo atual ou futuras, que, se não eliminadas, minimizadas ou evitadas pela empresa, podem (ou poderão) afetá-la negativamente.

No Livro "A Arte da Guerra", o autor Zun Tsu coloca: "Se conhecemos o inimigo (ambiente externo) e a nós mesmos (ambiente interno), não precisamos temer o resultado de uma centena de combates. Se nos conhecemos, mas não ao inimigo, para cada vitória sofreremos uma derrota. Se não nos conhecemos nem ao inimigo, sucumbiremos em todas as batalhas."

> Ameaça: palavra, ato, gesto pelos quais se exprime a vontade que se tem de fazer mal a alguém, sinal, manifestação que leva a acreditar na possibilidade de ocorrer alguma coisa.
> Sinônimos de Ameaça: advertência, bravata, cominação, intimação e prenúncio.
> Fonte: Dicionário Online Português

Já o termo risco, segundo o Guia de Orientação para Gerenciamento de Riscos Corporativos, é proveniente da palavra *risicu ou riscu*, em latim, que significa ousar (*to dare* em inglês). De acordo com La Rocque (2007), costuma-se entender risco como a possibilidade de "algo não dar certo", mas seu conceito atual envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às "perdas" como aos "ganhos", com relação ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organizações.

O risco é inevitável. Por exemplo, quando:

- Investidores compram ações;
- Cirurgiões realizam operações;
- Engenheiros projetam pontes;
- Empresários abrem seus negócios;
- Políticos concorrem a cargos eletivos etc.

Ou seja, administrar os riscos – que sempre irão existir – torna-se estratégico e, além disto, pode vir a se transformar em oportunidades. Portanto, deve-se transcender o "medo aos riscos" para "saber lidar de forma estratégica com os riscos".

Na área de tecnologia da informação e comunicação, risco é considerado como o impacto negativo motivado pela exploração de uma vulnerabilidade, considerando a possibilidade e o impacto da sua ocorrência. O processo para identificar, mensurar e planejar passos para reduzir um determinado risco a níveis aceitáveis pela organização é definido como Gerenciamento de Riscos (STONEBURNER, 2002 apud GONÇALVES, 2008, p. 15)

Risco é o efeito da incerteza nos objetivos.

- Um efeito é um desvio em relação ao esperado: positivo e/ou negativo;
- Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar-se em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo);
- O risco é muitas vezes caracterizado pela referência aos eventos potenciais e às consequências, ou uma combinação destes;
- O risco é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade de ocorrência associada;
- A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, conhecimento, sua consequência ou probabilidade.

Fonte: norma ISO 31000

Sob a óptica do Planejamento Estratégico, a sobrevivência e o sucesso da empresa dependem da sua sintonia com o ambiente.

A dependência da empresa em relação ao seu ambiente torna vital um esforço permanente de monitoramento dos ambientes externo e interno.

Mas estarão as empresas realmente preocupadas em analisar o ambiente? Sobre este assunto, que tal vermos juntos algumas análises importantes?

No livro “A Administração em Tempos Turbulentos”, o autor Peter Drucker afirma:

- "Em épocas turbulentas as empresas não podem pressupor que o amanhã será sempre uma extensão do presente. Pelo contrário, devem administrar visando mudanças que representem oportunidades e ameaças.";
- "Uma era de turbulência é também uma era de grandes oportunidades para aqueles que compreenderem, aceitarem e explorarem as novas realidades. Os tomadores de decisões devem e enfrentar face a face a realidade e resistirem àquilo que todos nós já conhecemos, a tentação das certezas do passado - certezas que estão prestes a se tomar as superstições do futuro.";
- "Mudanças são oportunidades. Podem ser vistas como ameaças por muitos executivos – mas todas precisam ser exploradas como uma oportunidade - para fazer algo de diferente, algo de novo e, acima de tudo, para fazer algo melhor, algo mais produtivo e lucrativo." (Disponível em: http://www.strategia.com.br/Estrategia/estrategia_corpo_capitulos_analise_ambiente.htm. Acesso em: 20/03/2013)

Ou seja, de acordo com o exposto, quando falamos em riscos e ameaças organizacionais, é imprescindível conhecer e analisar continuamente o ambiente organizacional (tanto interno quanto externo), pois as mudanças ocorrem e os gestores devem estar preparados para lidar com elas, a fim de manterem seus negócios competitivos no mercado.

4.2 Contexto dos Riscos

Atualmente, praticamente em todas as organizações, a segurança da informação é tida como uma área crítica, tendo em vista, todas as ameaças internas e externas a confiabilidade das informações organizacionais.
Uma gestão de Riscos com eficácia é proposta, com a principal finalidade de se identificar tais ameaças que rondam a confiabilidade das informações e possíveis impactos, em caso de materialização dos riscos, além de prover uma orientação no que diz respeito à melhor estratégia de medidas a serem tomadas.

Para tanto, é altamente recomendado que seja realizada uma analise de riscos orientada aos ativos de informação, com o propósito de determinar quais desses podem afetar a entrega de um produto ou serviço, em caso de violação de sua integridade, disponibilidade e/ou confidencialidade, podendo vir a causar danos, muitas vezes irreparáveis, à organização (fonte: http://www.tiespecialistas.com.br/2011/12/seguranca-a-importancia-da-gestao-de-riscos-orientada-a-ativos-de-informacao/#.UVoJvKLFXTp, consultado em 20/03/2013)

Não é possível, portanto, implantar o Gerenciamento de Riscos sem uma concisa definição dos requisitos do negócio. O ciclo de vida do negócio, tendo em vista os aspectos de tecnologia, depende de um bom entendimento do processo de Gerenciamento de Riscos do Negócio. O estágio de "análise de requisitos e definição de estratégias" é responsável por definir como a organização reagirá a uma interrupção do negócio ou desastre e os custos associados. Esse estágio tem processos de avaliação de risco e análise de impacto no negócio, comuns do ciclo contínuo de gerenciamento de riscos.

Portanto, o gerenciamento de riscos é um processo que tem como objetivo dar subsídios à organização para realizar sua missão institucional, de forma a:

- Possibilitar a segurança efetiva dos sistemas de Tecnologias de Informação e Comunicação, responsáveis pelo processamento, armazenagem e transmissão de dados;
- Criar uma base sólida para as tomadas de decisão, principalmente no que se relaciona com execução coerente do orçamento e no investimento em tecnologias necessárias para minimizar riscos de impacto ou potencial impacto para o negócio; e
- Permitir aos gestores equilibrarem seus custos de proteção e desempenho dos sistemas de informação vitais para o negócio.

Um fato importante é que o processo de gerenciamento de risco não deve ser considerado apenas na área de tecnologia da informação e comunicação, mas, sim, em todas as outras unidades de negócio.

CONEXÃO

Assista ao vídeo sobre Gestão de Riscos e Incertezas Organizacionais: http://www.youtube.com/watch?v=XOdH6ZUqvPo.

Risco: probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para a organização;
Vulnerabilidade: falha ou fraqueza de procedimento, design, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema;
Ameaça: possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente ou propositalmente uma vulnerabilidade específica.

Fonte: http://sseguranca.blogspot.com.br/2009/07/risco-vulnerabilidade-ameaca-e-impacto.html. Publicado em: janeiro de 2011. Acessado em: 29/07/2015

4.3 A Gestão de Riscos

A gestão de riscos, de acordo com o PMBOK (2008), consiste em processos sistemáticos de identificação, análise e avaliação dos riscos e no estabelecimento de respostas adequadas a eles.

Em função do monitoramento contínuo do ambiente organizacional externo e interno, a gestão de riscos pode detectar oportunidades e determinar como aproveitá-las. Portanto, o foco é minimizar o impacto de potenciais eventos negativos e obter plena vantagem de oportunidades com vistas a melhoramentos.

O risco tem duas dimensões: a probabilidade de sua ocorrência e o impacto sobre o projeto. Portanto, é necessáriocompreender dimensões para que se possa administrar o risco.

Importante ressaltar que dificilmente as chances de um risco podem ser eliminadas totalmente sem que o projeto seja reformulado.

Os processos que envolvem a gestão de riscos, de acordo com o PMBOK, (2008) são:

• Planejar o gerenciamento dos riscos: deve ser realizado na concepção do projeto e ser concluído nas fases iniciais do planejamento do projeto.

O processo de planejamento do gerenciamento dos riscos define como conduzir as atividades de gerenciamento dos riscos do projeto. O planejamento cuidadoso e explícito aumenta a probabilidade de sucesso para os outros cinco processos subsequentes. Este processo é importante para garantir que o grau, o tipo e a visibilidade do gerenciamento dos riscos sejam proporcionais tanto aos riscos como à importância do projeto para a organização (PMBOK, 2008, p. 228).

• Identificar os riscos: determina os riscos que podem afetar o projeto, bem como documenta suas características. Identificar os riscos, conforme expõe PMBOK (2008), é um processo iterativo porque novos riscos podem surgir ou se tornar conhecidos somente o ciclo de vida do projeto. O formato das declarações de riscos devem ser consistentes para garantir a capacidade de comparar o efeito relativo de um evento de risco com outros no projeto;

• Realizar a análise qualitativa dos riscos: de acordo com Kerzner (2004), Vargas (2005) e PMBOK (2008), prioriza os riscos para análise ou ação adicional através da avaliação e combinação de sua probabilidade de ocorrência e impacto. Neste aspecto, as organizações podem aumentar o desempenho do projeto concentrando-se nos riscos de alta prioridade. A realização da análise qualitativa de riscos é um meio rápido e econômico de estabelecer as prioridades do processo de Planejar as Respostas aos Riscos e Define a Base para a realização da análise quantitativa dos riscos, se necessária (PMBOK, 2008);

• Realizar a análise quantitativa dos riscos: analisa numericamente os efeitos dos riscos identificados nos objetivos gerais do projeto. Esta análise é realizada nos riscos que foram priorizados pela análise anterior (qualitativa). Este processo, confirme o PMBOK (2008), geralmente segue o da análise qualitativa de riscos e deve ser repetido depois de Planejar as respostas aos riscos e também como parte do processo de monitorar e controlar os riscos, para determinar se o risco geral do projeto diminuiu satisfatoriamente;

• Planejar as respostas aos riscos: de acordo com Valeriano (2001) e PMBOK (2008), desenvolve opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos do projeto. Além disto, é designada uma pessoa para ser responsável por cada resposta ao risco que foi acordada/financiada.

As respostas planejadas, de acordo com o PMBOK (2008), devem ser adequadas à relevância (prioridade) do risco, ter eficácia de custos para atender ao desafio, ser realistas dentro do contexto do projeto, acordadas por todas as partes envolvidas e ter um responsável designado;

• Monitorar e controlar os riscos: implementa planos de respostas a riscos, acompanha os riscos identificados, monitora os riscos residuais, identifica novos riscos e avalia a eficácia do processo de riscos durante todo o projeto. Este processo utiliza técnicas que requerem o uso das informações de desempenho geradas durante a execução do projeto. O responsável pela resposta ao risco informa ao gerente de projetos sobre a eficácia do plano, os efeitos imprevistos e qualquer correção para tratar o risco de forma adequada. O processo de monitorar e controlar os riscos também engloba, conforme expõem Vargas (2005) e PMBOK (2008), a atualização dos ativos de processos organizacionais, incluindo os bancos de dados de lições aprendidas e os modelos de gerenciamento dos riscos do projeto, para benefício de futuros projetos.

4.4 Análise/Avaliação dos Riscos

De acordo com Stoneburner et al (2002), a primeira etapa é avaliar/dimensionar os riscos, de forma a determinar a extensão das (potenciais) ameaças e riscos a elas associados. A resultante desta análise viabilizará a mitigação de riscos a fim de identificar meios para controlar e/ou minimizar os riscos.

Stoneburner et al (2002) propuseram alguns passos sequenciais para avaliar os riscos, os quais:

1. Caracterização do ambiente;
2. Identificação de ameaças;
3. Identificação de vulnerabilidades;
4. Análise de controles;
5. Determinação de probabilidades;
6. Análise de impacto;
7. Definição dos riscos;
8. Recomendações de controle; e
9. Documentação dos resultados.

O gerenciamento de riscos é subordinado a um adequado planejamento de avaliação de riscos. Falhas no alinhamento, escopo ou na obtenção da aceitação da avaliação reduz a eficácia das próximas fases. Por ser onerosa, a fase de avaliação de riscos reclama por investimentos significativos de recursos e tempo e depende da participação ativa do interessado (DILLARD, 2004 apud GONÇALVES, 2008, p. 22).
O risco é calculado em função da probabilidade de uma vulnerabilidade ser explorada por uma ameaça e o resultado do impacto na organização caso este evento ocorra. Para que se possam determinar as possibilidades de ocorrência de um evento adverso, as ameaças devem ser analisadas em conjunto com as potenciais vulnerabilidades e os controles já existentes. O nível do impacto é definido pela sua influência no negócio e por sua vez no valor do bem atingido (STONEBURNER et al, 2002 apud GONÇALVES, 2008, p. 22).

4.4.1 Caracterização do Ambiente

Caracterizar o ambiente apoia a identificação dos limites operacionais, computacionais, de informação etc.

Inventariar os ativos, conhecer seus respectivos valores e importância ao negócio assegura proteção de forma efetiva, pois os níveis de cuidado serão proporcionais a estes parâmetros, além de serem pré-requisitos fundamentais para o gerenciamento de risco. Exemplos de ativos associados a sistemas, de acordo com as normas ABNT (2005), são:

- Informação: bancos dados, arquivos, documentação de sistemas, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de contingência, procedimentos de recuperação, informações armazenadas;
- Softwares: aplicativos, sistemas, ferramentas de desenvolvimento, e utilitários;

- Hardware: equipamentos computacionais (processadores, monitores, notebooks, discos rígidos, impressoras, storages, autoloaders, nobreaks), ativos de rede (roteadores, switches), equipamentos de apoio (geradores, condicionadores de ar, iluminação);
- Serviços: contratos de apoio ou suporte, contratos de níveis de serviço, fornecimento de energia elétrica. (GONÇALVES, 2008, p. 22)

Este levantamento de informações (caracterização do ambiente) pode ser feito através de formulários, questionários, entrevistas com pessoas-chave, análise de documentos históricos, entre outros.

4.4.2 Identificação das Ameaças

Antes de falarmos em identificação das ameaças, é importante sabermos distingui-las. De acordo com Stoneburner et al (2002), elas podem ter origem:

- Natural (enchentes, terremotos, tornados, deslizamento de terra, tempestades de raios etc.);
- Humana (atos dolosos, negligentes, imperitos ou imprudentes de uso de programas maliciosos, de acesso a dados sigilosos, de mau uso dos sistemas, etc.) ou
- Ambiental (falta de energia, poluição, substâncias químicas, etc.).

Quando não há vulnerabilidades associadas, a fonte de ameaça não apresenta riscos (GONÇALVES, 2008, p. 23)

É aconselhável manter e atualizar continuamente um histórico (lista) das ocorrências de incidentes de segurança na organização. Isto auxiliará, entre outros aspectos, a formular as lições aprendidas.

CONEXÃO

Assista ao vídeo sobre as ameaças que podem invadir seu computador: http://www.youtube.com/watch?v=xpC2_kx3H50.

4.4.3 Identificação de Vulnerabilidades

Após identificar e listar as ameaças, é possível diagnosticar quão vulnerável é, ou poderá tornar-se, o ambiente.

Vulnerabilidades são falhas ou fraquezas nos processos de segurança, nos projetos, no desenvolvimento ou nos controles internos de um sistema, os quais, se explorados, podem resultar em eventos não desejados. (STONEBURNER et al 2002, p. 15)

Métodos recomendados para a identificação de vulnerabilidades do sistema englobam o uso das fontes de vulnerabilidade, desempenho dos testes de segurança do sistema e desenvolvimento de uma lista de verificação de requisitos de segurança. Além disto, e de acordo com a ABNT (2008), outros métodos proativos englobam: testes e simulações, testes de invasão de sistemas, auditorias em códigos-fonte etc.

4.4.4 Análise de Controles

> Este passo tem como objetivo, segundo as normas da ABNT (2008), avaliar os controles existentes ou planejados para minimizar ou eliminar chances de uma ameaça explorar determinada vulnerabilidade. Para que se evitem custos e retrabalhos, é conveniente que os controles existentes sejam identificados e avaliados quanto sua a eficácia. Controles existentes podem ser considerados ineficazes, insuficientes ou não justificáveis, devendo estes serem avaliados quanto a sua substituição ou manutenção no ambiente (GONÇALVES, 2008, p. 25)

De acordo com as normas da ABNT (2008), informações de controles podem ser obtidas por meio de:

1. Análise de documentos dos processos de gestão de segurança da informação, juntamente com seus respectivos responsáveis, além dos responsáveis pelas instalações, segurança predial ou usuários;

2. Averiguação da efetividade de funcionamento dos controles utilizados.

O produto da análise de controle é uma lista dos utilizados para reduzir a probabilidade de uma ameaça explorar uma vulnerabilidade ou de reduzir o dano causado por um evento não desejado.

4.4.5 Análise de Probabilidades

A produção de um índice que indique as chances de uma vulnerabilidade ser explorada deriva da capacidade e do estímulo das fontes de ameaças, da natureza da vulnerabilidade e da existência e da efetividade de controles existentes. Probabilidades são ditas altas quando a fonte de ameaça está altamente estimulada, é capaz de exercer a ameaça e não existem controles preventivos, ou se existem não são efetivos. Probabilidades são ditas médias quando a fonte de ameaça está motivada, é capaz de exercer a ameaça, mas os controles utilizados são efetivos, ou seja, não permitem o sucesso da fonte de ameaça. E por fim, probabilidades são ditas baixas quando as fontes de ameaças carecem de motivação e os controles são efetivos na prevenção da exploração da vulnerabilidade (STONEBURNER et al, 2002, p. 21).

Para uma análise e definição lapidada das vulnerabilidades, conforme normas da ABNT (2008), sugere-se considerar, entre outros aspectos: experiências passadas; estatísticas históricas de ocorrência de ameaças; motivações e ferramentas disponíveis para realizar atos intencionais; fatores climáticos e geográficos; prováveis situações que poderiam causar erros humanos e análise de quão efetivo são os controles atuais.

4.4.6 Análise de Impacto

O próximo passo importante na medição do nível de risco é determinar o impacto e o valor do sistema ou importância para uma organização. Antes de iniciar a análise de impacto, é necessário obter as seguintes informações:

- Missão do sistema (por exemplo, os processos realizados pelo sistema de TI);
- Criticidade do sistema de dados (por exemplo o valor ou importância do sistema para a organização);
- Sensibilidade dos dados do sistema (STONEBURNER et al, 2002, p. 21).

Ou seja, analisar o impacto visa a determinar o resultado do impacto no negócio caso uma determinada ameaça obtiver sucesso.

> Na ausência informações detalhas a respeito da criticidade dos ativos, a avaliação do impacto nos negócios pode ser realizada tendo como fundamento os requisitos de segurança atuais e as definições de nível de impacto dos responsáveis pelos ativos. O impacto adverso de um evento pode ser descrito como a perda e/ou degradação da integridade, disponibilidade ou confidencialidade da informação. Impactos tangíveis podem ser mensurados quantitativamente utilizando-se uma unidade de medida conhecida, como: perda de desempenhos, custos de manutenção ou tempo gasto para corrigir problema. Outros, de difícil mensuração, podem ser definidos qualitativamente como alto, médio ou baixo impacto, classificados conforme grandeza dos custos pela perda dos ativos ou recursos, significância do dano em relação à missão ou reputação da empresa, ou prejuízos a vida humana.
> Portanto, as abordagens quantitativa e qualitativa apresentam benefícios e inconveniências que precisam ser consideradas na avaliação de riscos. A organização deve optar pelo uso individual ou por combinação de ambas, conforme seus requisitos e níveis de exigência (GONÇALVES, 2008, p. 27)

4.4.7 Definição dos Riscos

A definição dos riscos, de acordo com definições de Stoneburner et al (2002) apud Gonçalves (2008), pode ser explicitada por meio de uma junção de três argumentos:

1. A possibilidade de exploração de uma vulnerabilidade;
2. O impacto ao negócio devido à ocorrência de um evento adverso; e
3. Pela efetividade do controles de segurança utilizados para reduzir ou eliminar riscos.

A seguir, vemos uma tabela que exemplifica os parâmetros de probabilidade de incidente e no impacto ao negócio, de acordo com as normas ABNT (2008). Observando o quadro, nota-se a escala crescente desde 0 até 8, em que respectivamente o número menor (zero) corresponde a “muito baixo” e o número maior (oito) corresponde a “muito alto”.

	PROBABILIDADE DO CENÁRIO DE INCIDENTE	MUITO BAIXA (MUITO IMPROVÁVEL)	BAIXA (IMPROVÁVEL)	MÉDIA (POSSÍVEL)	ALTA (PROVÁVEL)	MUITO ALTA (FREQUENTE)
IMPACTO NO NEGÓCIO	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

Tabela 4.1 – Classificação de Riscos. Fonte: Adaptado de ABNT (2008).

Tendo definido os riscos, conforme quadro supracitado, pode-se classificá-los e priorizá-los conforme seus respectivos níveis de relevância para a organização.

4.4.8 Recomendações de Controle

Durante este processo, pode-se mitigar ou eliminar os riscos identificados. A meta das recomendações de controle é reduzir o nível de risco para o sistema informatizado e seus dados a um nível aceitável.

Neste contexto os seguintes fatores devem ser considerados em recomendações de controle e soluções alternativas para minimizar ou eliminar riscos identificados:

- Efetividade de opções recomendadas (exemplo: compatibilidade de sistema);
- Legislação e regulamentação;
- Política organizacional;
- Impacto operacional;
- Segurança e confiabilidade.

As recomendações de controle são o resultado do processo de avaliação do risco e contribuem para o processo de mitigação de risco, durante o qual os controles de segurança técnica e procedural recomendados são avaliados, priorizados e implementados.

O processo de identificação de controles pode ser desafiador, especialmente se os envolvidos possuírem vivência limitada no assunto. Duas abordagens podem ser empregadas: a primeira consiste em um debate informal, enquanto a segunda fundamenta-se na organização e classificação de controles. A equipe de gerenciamento de riscos de segurança deve usar uma combinação dessas duas abordagens.

Na abordagem através de debate informal, os controles podem ser identificados depois de respondidas perguntas como:

- Que medidas a organização poderia tomar para resistir ou prevenir a ocorrência de riscos?
- O que a organização poderia fazer para recuperar-se de um evento adverso?
- Que medidas a organização pode tomar para detectar a ocorrência de riscos?
- Como o controle pode ser auditado e monitorado para garantir sua efetividade?
- Existem outras ações que podem ser tomadas para gerenciar o risco?

O segundo método de recomendação de controles sustenta-se na classificação do controle em organizacional, operacional e tecnológico, e ainda em subdivisões como prevenção, detecção/recuperação e gerenciamento de riscos. Os controles organizacionais definem como os colaboradores de uma organização devem executar suas tarefas. Os controles operacionais normatizam a utilização dos recursos de tecnologia da informação e comunicação, e incluem também as proteções ambientais e físicas. Enquanto que controles tecnológicos compreendem o planejamento arquitetônico, engenharia, hardwares, softwares e firmwares, ou seja, os componentes tecnológicos usados para construir os sistemas de informação da organização (DILLARD, 2004 apud GONÇALVES, 2008, p. 29)

A resultante deste processo servirá como base de entrada para o processo de mitigação de risco.

4.4.9 Documentação dos Resultados

Os resultados encontrados devem ser documentados e armazenados historicamente, a fim de se construir uma base de conhecimento de lições aprendidas. Além disto, tais dados coletados apoiarão, também, a tomada de decisão gerencial no que tange à elaboração de novas políticas, alterações/correções em procedimentos etc.

O relatório de avaliação de riscos não possui a características de apontar erros, mas sim de sistematizar de maneira analítica os riscos inerentes ao negócio, justificando investimentos e reduzindo potenciais perdas ou danos. Seu conteúdo demonstra as ameaças e vulnerabilidades, a medida dos riscos identificados, e fornece recomendações de controle que podem ser implantados pelo processo de mitigação de riscos (STONEBURNER et al, 2002, apud GONÇALVES, 2008, p. 32).

4.5 Mitigação (Diminuição) dos Riscos

A mitigação de riscos envolve priorizar, analisar, avaliar e implementar os controles apropriados e recomendados pelo processo de avaliação de riscos.

Devido ao fato de que a eliminação total de riscos é impraticável e/ou quase impossível, é de responsabilidade do gerente de negócio e gestores utilizarem a abordagem de menor custo e implementar os controles mais adequados para diminuir o risco a um nível aceitável, com mínimo impacto negativo sobre os recursos e metas organizacionais.

Por muito tempo, programadores e analistas de sistemas de software dirigiram sua atenção somente em entender o problema do cliente e sair programando, sem nenhuma preocupação com riscos envolvidos no decorrer do desenvolvimento e inerentes a qualquer natureza de projetos. Com advento da nova visão em tecnologia da informação, surgiu uma modalidade diferenciada de profissionais (gerente de negócios ou de projetos de TI) que não atentam somente o produto final, mas o planejamento de todo processo para atingimento das metas do projeto, inclusive na entrega de deliverables ou produtos intermediários a cada momento susceptíveis a riscos (http://www.techoje.com.br/site/techoje/categoria/detalhe_artigo/55, consultado em 20/03/2013)

De acordo com Stoneburner et al (2002), a mitigação dos riscos pode ser atingida através das seguintes opções:

• Suposição de riscos: aceitar o risco potencial e continuar operacionalizando o sistema informatizado ou implementar controles para diminuir o risco para um nível aceitável;

• Prevenção de riscos: evitar o risco, eliminando sua causa de risco e/ou consequência (por exemplo, abrir mão de certas funções do sistema ou desligar o sistema quando os riscos são identificados);

• Limitação de riscos: limitar o risco implementando controles que minimizam o impacto negativo de uma ameaça influenciar uma vulnerabilidade (por exemplo, o uso de controles de apoio, prevenção etc);

• Planejamento de riscos: gerenciar riscos através do desenvolvimento de um planejamento de mitigação de riscos que prioriza, implementa e mantém controles;

• Pesquisa e Reconhecimento: para diminuir o risco de perda, reconhecendo a vulnerabilidade ou falha e pesquisar controles para corrigir a vulnerabilidade;

• Transferência de risco: transferir o risco usando outras opções para compensar a perda, como, por exemplo, a compra de seguros.

As metas e a missão de uma organização devem ser consideradas na seleção de quaisquer opções de mitigação de risco. Pode não ser prático para resolver todos os riscos identificados, assim deve ser dada prioridade à ameaça e respectiva vulnerabilidade impactada significativamente.

4.5.1 Análise e Melhoria Contínua

A tecnologia da informação e comunicação é atualizada/melhorada/reinventada constantemente a fim de acompanhar as necessidades, tendências e comportamento dos consumidores (sejam eles domésticos, empresariais etc). As melhorias devem, portanto, ser realizadas de forma rigorosamente contínua.

A reavaliação periódica do ambiente através dos processos avaliação de riscos é o primeiro passo para se começar um novo ciclo. A equipe de gestão de riscos de segurança deve reutilizar e atualizar as listas de ativos, vulnerabilidades, controles e outras propriedades intelectuais desenvolvidas durante o projeto inicial de gerenciamento de riscos.
A equipe pode determinar onde se concentrar, reunindo informações atuais, precisas e relevantes sobre as alterações que afetam os sistemas de informações da organização. Os eventos internos que exigem uma apuração mais cuidadosa incluem a instalação de novos hardwares e softwares nos computadores; novos aplicativos desenvolvidos internamente; reorganizações corporativas; aquisições e fusões corporativas; bem

como liquidações de partes da organização. Também é recomendável revisar a lista de riscos existente para determinar se houve alterações. Além disso, examinar os registros de auditoria de segurança pode trazer idéias sobre outras áreas a investigar (DILLARD, 2004 apud GONÇALVES, 2008, p. 36)

Importante ressaltar que também se deve verificar continuamente se os critérios estabelecidos para mensurar o risco permanecem coerentes com as metas organizacionais, umas vez que estas últimas podem mudar conforme tendências e oportunidades de negócios.

Contudo, e conforme veremos no próximo item, o êxito na gestão de riscos dependerá diretamente do envolvimento, comprometimento e participação ativa de todos os envolvidos (direção, alta gerência e outros stakeholders) e comprometimento da alta gerência (assim como de todos os envolvidos).

4.5.2 Abordagem Reativa e Proativa

Quando ocorre determinado incidente de segurança, muitos profissionais tendem a agir para conter a situação, descobrir as causas e reparar os danos no menor tempo possível. Tal abordagem é dita reativa, ou seja, depende de um estímulo causado por um incidente para que ações sejam tomadas.

As respostas a incidentes são taticamente eficazes, principalmente se executada com rigor para se descobrir as causas raiz. Como resultado, incidentes de segurança recentes podem auxiliar na prevenção de incidentes futuros.

A abordagem proativa de gerenciamento de riscos de segurança almeja a redução da probabilidade de um incidente com a utilização de planos de controles. Ao contrário da abordagem reativa, a abordagem proativa não espera pelo surgimento de um incidente.

Em hipótese alguma, as organizações devem abandonar seus processos de respostas a incidentes, pois a abordagem proativa diminui a chance, mas não evitam que determinados incidentes possam ocorrer. Recomenda-se que as organizações utilizem as duas abordagens, aprimorando-as ao longo do tempo (DILLARD, 2004 apud GONÇALVES, 2008, p. 17).

Cabe ressaltar que a abordagem reativa acarreta, ao longo do tempo, maior custo do que a abordagem proativa. Isto se dá pelo fato de que o retrabalho e o desperdício (de tempo, recursos humanos, técnicos e de infraestrutura) acarretam severas perdas e prejuízos para a organização. Evitar que um problema ocorra, através de políticas de gestão de riscos adequadas, minimiza e/ou extingue a probabilidade de um problema futuro ocorrer.

4.6 Fundamentos de Sucesso da Gestão de Riscos

A fim de se lograr êxito com a política de gestão de riscos na organização, não basta apenas um excelente planejamento de ações e metas, mas também alguns fatores do contexto que engloba tal gestão:

- Total apoio e patrocínio da alta direção;
- Envolvimento, participação ativa e maturidade dos stakeholders (interessados);
- Comunicação ativa e assertiva;
- Alinhamento/gestão de conflitos da equipe;
- Visão sistêmica da gestão de riscos (compreender que uma parte afeta e pode ser afetada pelo todo);
- Liderança e liberdade de atuação da equipe de gestão de riscos, a fim de conseguirem realizar mudanças caso seja necessário e atingir às metas estabelecidas.

ATIVIDADES

01. "O crescente acirramento da concorrência e a necessidade de ganhar competitividade têm obrigado as empresas e instituições a buscarem estabelecer mais parcerias entre si. [...]

O Programa Cultura da Cooperação, criado há 15 anos, já foi aplicado em centenas de grupos de empreendedores de segmentos variados atendidos pelo Sebrae Minas, em projetos de desenvolvimento local, regional e territorial. O aprendizado da cooperação e os resultados, geralmente, são percebidos no médio e longo prazos.

O objetivo do programa é colaborar no desenvolvimento de um grupo, para que ele amplie sua capacidade de agir coletivamente, viabilizando objetivos comuns, baseados nos princípios da cooperação. Atuando em conjunto, essas empresas conseguem, por exemplo, partilhar riscos e custos para explorar novas oportunidades, dividir o ônus na realização de pesquisas tecnológicas, oferecer produtos diversificados e com qualidade superior, exercer pressão no mercado, combinar competências e fortalecer seu poder de compra." (http://g1.globo.com/minas-gerais/especial-publicitario/sebrae/historias-de-sucesso/noticia/2015/07/unindo-esforcos-pelo-bem-comum.html)

Após a leitura do texto, analise as asserções e assinale a alternativa correta:

I. Ao abrir um negócio, por exemplo, o risco é inevitável.

II. Se bem administrados, os riscos de um negócio podem ser extintos.

III. Risco é um impacto negativo, motivado pela exploração de uma vulnerabilidade.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) Somente a asserção III está correta.
d) As asserções I e III estão corretas.
e) As asserções II e III estão corretas.

02. O Gerenciamento de Riscos é um processo que tem como objetivo dar subsídios à organização realizar sua missão institucional, de forma a: (leia as asserções e assinale a alternativa correta)

I. Possibilitar a segurança efetiva dos sistemas de Tecnologias de Informação e Comunicação.

II. Criar uma base sólida para a tomada de decisões.

III. Permitir aos gestores equilibrarem seus custos de proteção e desempenho dos sistemas de informação.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) Somente a asserção III está correta.
d) As asserções I e II estão corretas.
e) As asserções I, II e III estão corretas.

03. Existem alguns passos sequenciais para avaliar os riscos. Sobre estes passos, assinale a alternativa incorreta.

a) Caracterização do ambiente.
b) Identificação de ameaças.
c) dentificação de vulnerabilidades.
d) Implementação de correções.
e) Determinação de probabilidades.

REFLEXÃO

Este capítulo tratou especificamente dos Riscos Organizacionais. Sabemos que este assunto é muito importante, pois o fluxo de dados interorganizacional implica em riscos e, portanto, demanda segurança para proteger os mesmos.

Entretanto, antes de se pensar em quaisquer políticas de segurança, é necessário conhecer o que se vislumbra proteger, contra quem e de que forma. Além disto, é necessário distinguir que a segurança da informação é vulnerável a: ocorrências naturais (desastres da natureza, falta de energia etc.), erro humano (seja ele proposital/intencional/doloso ou não).

Como já vimos através do texto deste capítulo, enfatizamos que a avaliação dos riscos siga os passos propostos por Stoneburner et al (2002): Caracterização do ambiente; Identificação de ameaças; Identificação de vulnerabilidades; Análise de controles; Determinação de probabilidades; Análise de impacto; Definição dos riscos; Recomendações de controle; e Documentação dos resultados.

LEITURA

Recomendamos a leitura de Miranda (2015): "Otimização da receita em hospitais por meio da gestão de riscos", conforme segue parcialmente abaixo (o artigo na íntegra encontra-se disponível através do link: http://www.segs.com.br/saude/50764-otimizacao-da-receita-em-hospitais-por-meio-da-gestao-de-riscos.html)

"Certamente a prioridade dos hospitais é a excelência na qualidade do atendimento e assistência médico-hospitalar. Mas é preciso entender que uma boa gestão administrativa pode garantir, além da perenidade da organização, a qualidade no atendimento ao paciente.

O conceito de gestão de riscos para quem trabalha em hospitais é bastante conhecido e envolve a segurança do paciente e dos profissionais, mas existe outra oportunidade para aprimorar a gestão hospitalar ainda pouco explorada. A abordagem de Gestão dos Riscos de Negócio que é amplamente utilizada e com excelentes resultados em outros setores como telecomunicações, energia, agronegócio, varejo, transporte e financeiro.

[...]

Hospitais que optam por não darem a devida prioridade à gestão de seus riscos, estão expostos aos mesmos problemas que a maior parte das empresas: insuficiência de caixa, margens apertadas, indisponibilidade e/ou desvio de ativos, falta de indicadores, ineficiências no processo, falhas e fraudes. Portanto, é fundamental conhecer e gerenciar os principais riscos da organização, de forma ampla, estruturada e alinhada à sua estratégia.

"A adoção da Gestão de Riscos de Negócio traz melhoria e preservação dos resultados operacionais e financeiros, valorização da organização, minimização de riscos e aumento de eficiência e segurança dos processos. [...]", aponta Whitaker.

Situações que podem gerar ineficiências, danos e perdas precisam ser devidamente tratadas por meio da Gestão de Riscos de Negócio, composta por três etapas:

1. Diagnóstico de riscos – etapa de levantamento e entendimento da situação considerando as camadas de processos, sistemas, pessoas, infraestrutura e gestão. Vulnerabilidades e riscos são identificados e classificados;

2. Desenvolvimento das soluções – etapa de definição de soluções e da abordagem para a implantação;

3. Implantação das soluções – detalhamento e implantação de soluções, priorizando as ações de ganho rápido (baixo esforço, benefício alto) e as ações de caminho crítico (em que outras soluções são dependentes para evoluir).

[...]"

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. ABNT NBR ISO/IEC 27002:2005: **Tecnologia da Informação:** Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ABNT. ABNT NBR ISO/EIC 27005:2008: **Tecnologia da Informação:** Técnicas de Segurança : Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008.

DILLARD, K.; PFOST, J.; RYAN, S. **Security Risk Management Guide.** [S.l.]: Microsoft Corporation, Disponível em: http://technet.microsoft.com/enus/library/cc163143.aspx, outubro, 2004.

GONÇALVES, A. J. **Metodologias de Gerenciamento de Riscos em Sistemas de Tecnologia da Informação e Comunicação** – abordagem prática para conscientização e implantação nas organizações. Trabalho de Conclusão de Curso de Pós-Graduação (Especialização), Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008.

LA ROCQUE, E. **Guia de Orientação para o Gerenciamento de Riscos Corporativos.** São Paulo: IBGC – Instituto Brasileiro de Governança Corporativa, Disponível em: http://www.audicaixa.org.br/arquivos_auditoria/GerenciamentoRiscosCorporativos-IBGC.pdf , 2007.

KERZNER, H. **Gestão de Projetos:** as melhores práticas. Editora Bookman, 2ª edição, 2004.

PMBOK. **Um guia do Conjunto de Conhecimento em Gerenciamento de Projetos.** 4ª Edição, Project Management Institute, 2008.

SEMOLA, M. **Gestão da Segurança da Informação:** Uma Visão Executiva, Editora Campus, 2003.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. **Risk Management Guide for Information Technology Systems.** Gaithersburg: NIST - National Institute of Standards and Technology. Disponível em: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, julho, 2002.

VALERIANO, D. **Gerenciamento Estratégico e Administração por Projetos.** Editora Makron Books, 2001.

VARGAS, R. V. **Gerenciamento de Projetos:** estabelecendo diferenciais competitivos. Editora Brasport, 6ª edição, 2005.

5

Normas de Segurança da Informação e Estratégias de Proteção

Olá, pessoal. Neste quinto capítulo vamos falar sobre o normas e regulamentações que devem ser cumpridas/respeitadas no que tange à gestão da segurança das informações. Tais normas visam tanto a certificar as empresas como também a apresentar diretrizes para que elas se adaptem.

Para compreensão deste amplo assunto, faremos, *a priori*, uma contextualização do mesmo.

Vamos juntos!

OBJETIVOS

Nossos objetivos serão:

- Compreender os conceitos de norma e regulamentação;
- Compreender a importância de se utilizar as normas e regulamentações;
- Analisar as normas e regulamentações no contexto organizacional;
- Conhecer a lei Sarbanes-Oxley;
- Conhecer as Normas NBR ISO/IEC 27001 e ISO/IEC 27002;
- Conhecer o Modelo ITIL.

5.1 Introdução

A Tecnologia da Informação (TI) disponibiliza, cada vez mais, novas ferramentas para facilitar nosso dia a dia e apoiar nossas tarefas organizacionais. Toda esta gama de ferramentas torna nossas tarefas mais ágeis, mais velozes, mais assertivas.

Entretando, existem também alguns riscos que acompanham toda esta diversidade tecnológica. Tais riscos fazem parte da nossa realidade, de nosso dia a dia e devem ser devem ser detectados, analisados e "enfrentados"/corrigidos através de medidas técnicas (ex.: utilização de softwares para proteção das informações), sociais (ex.: orientação aos funcionários sobre a política organizacional) etc.

empresa requer uma série de controles e cuidados. A falta de visão e conhecimento sobre o assunto em pequenas e médias empresas, assim como de alguns administradores, conduz o gestor de TI à necessidade de gerar e utilizar métricas que transformem em números todos os acontecimentos, impactos e ações importantes de TI na empresa da qual é parte integrante.

O Brasil ainda é carente de leis que direcionem ações de usuários e empresas para o uso correto de tecnologia da informação, por isso recai sobre cada empresa a responsabilidade de tomar as medidas possíveis para evitar fraudes, perda de produtividade e impactos sociais ou operacionais. A cada novo dia sai uma nova decisão, norma ou regulamentação, estamos tratando de um assunto relativamente novo, em desenvolvimento, e que por isso ainda é polêmico.

Apenas para contextualizar o assunto, foi publicado que, conforme decisão do Tribunal Regional do Trabalho de São Paulo (TRT-SP), a privacidade do trabalhador só se aplica a contas pessoais. Comunicadores e e-mails corporativos podem ser vigiados e, portanto, o conteúdo das mensagens neles contidas pode ser usado como prova em casos de demissão por justa causa e processo trabalhista. Para a Justiça, o e-mail corporativo é uma ferramenta de trabalho, que pertence à empresa, e não ao funcionário, o que justificaria o direito da empresa de monitorar estas contas. O Tribunal Superior do Trabalho, através da decisão TST – AIRR 613/2000, determinou que o empregador tem o direito de monitorar os e-mails corporativos e o acesso à internet por parte de seus empregados, entendendo, em suma, que a empresa é a

> proprietária dos instrumentos de trabalho utilizados para o acesso e de que o ambiente de trabalho não é um ambiente com expectativa de privacidade. Como o e-mail, o acesso à Internet e o computador são de propriedade da empresa, a justiça avaliou que não há problema em fiscalizar qualquer tipo de uso que os funcionários estão fazendo de sua propriedade (PITELI, 2007, p.1)

Ainda no contexto do acesso à Internet no ambiente de trabalho, e enquanto horário de trabalho, deve-se analisar até que nível de liberdade de acesso terão os colaboradores. Já são considerados conteúdos passíveis a proibição de acesso os sites com conteúdo pornográfico e/ou ilegal, sites de chat, sites de relacionamento, programas de troca de mensagens instantâneas, e assim por diante.

O empregador pode monitorar os acessos de seus colaboradores à Internet de forma moderada. Por exemplo: monitorar o e-mail de seus colaboradores pode ser considerado invasão à privacidade. No entanto, pode ser que o colaborador esteja se utilizando do e-mail corporativo de forma abusiva e/ou que prejudique a imagem e credibilidade da organização.

Diante do contexto, é aconselhável que a organização tenha um regimento de como devem ser utilizados os meios e ferramentas de trabalho, de forma que os colaboradores saibam as normas, fiquem cientes de que seus acessos podem estar sendo monitorados, dentre outros aspectos.

5.2 Compreendendo o Conceito de Norma

Uma norma é um documento que contém uma descrição técnica, específica e precisa de critérios a serem cumpridos como regras/diretrizes.

As normas fazem sentido se tornam a vida mais simples e elevam o nível de confiabilidade de produtos e serviços que utilizamos.

> As normas são criadas formando um conjunto de experiência e conhecimento de todas as partes interessadas, tais como os produtores, vendedores, compradores, usuários e regulamentadores de material, produto, processo ou serviço em particular. As normas são desenvolvidas para uso voluntário e não impõem nenhuma regulamentação. Entretanto, as leis e regulamentações podem referir-se a certas normas e tornar a conformidade com as mesmas compulsória. Por exemplo, as características

físicas e o formato dos cartões de crédito são definidos na norma número BS EM ISO/IEC 7810:1996. Aderir a esta norma significa que os cartões podem ser usados globalmente.
Qualquer norma é um trabalho coletivo. Comitês de fabricantes, usuários, organizações de pesquisa, departamentos governamentais e consumidores trabalham em conjunto para criar normas que evoluem para atender às demandas da sociedade e da tecnologia. (Fonte: http://www.bsibrasil.com.br/publicacoes/sobre_normas/normas/, consultado em 16/04/2013).

Significados de Norma:
Princípio que serve de regra, de lei.
Modelo, exemplo.
Sinônimos de norma: bitola, craveira, determinação, escantilhão, estalão, formalidade, lei, mandamento, medida, padrão, preceito e regra

Fonte: www.dicio.com.br

5.2.1 Benefícios de utilizar Normas

A norma serve de apoio às organizações, independentemente seus portes pois ela é capaz de apoiar a inovação, promover concorrência entre outros aspectos.

Quando abordamos o assunto "normas", referenciamos inevitavelmente a British Standards Institution (BSI), que é líder mundial na defesa, definição e implementação das melhores práticas em todos os campos da atividade humana, desde continuidade de negócios até segurança alimentar.

Portanto, de acordo com dados extraídos do British Standards Institution (BSI), através de seu site http://www.bsibrasil.com.br/publicacoes/sobre_normas/beneficios/, as normas permitem que uma companhia:

- Atraia e mantenha clientes;
- Demonstre liderança de mercado;
- Crie vantagens competitivas; e
- Desenvolva e mantenha as melhores práticas.

Uma empresa que está de acordo com as normas estabelecidas para seu setor se diferencia das demais que não estão e, consequentemente, torna-se mais respeitada no mercado. Por tal fator, podemos afirmar que as normas são poderosas ferramentas de marketing para as empresas.

O mercado consumidor é cada vez mais exigente e, por consequência, demanda por produtos e serviços que estejam em conformidade com as normas estabelecidas, além de preferirem também as empresas que cumprem padrões de sustentabilidade e responsabilidade ambiental.

Os clientes buscam a verificação independente que as normas técnicas provêm. As marcas de certificação obtidas pelas empresas cujos produtos e práticas passam consistentemente por um exame rigoroso são instantaneamente reconhecíveis e agem como símbolos respeitados de qualidade, segurança e desempenho.
Em se tratando do negócio, sabe-se que uma comunicação eficaz ao longo da cadeia de fornecimento e com organismos legisladores e clientes é indispensável. A normatização pode gerar benefícios mensuráveis quando aplicada dentro da infraestrutura da própria companhia. Os custos e riscos do negócio podem ser minimizados, os processos internos racionalizados e a comunicação melhorada. A normatização promove a interoperabilidade, gerando uma margem competitiva necessária para um eficaz comércio global de produtos e serviços (Fonte: http://www.bsibrasil.com.br/publicacoes/sobre_normas/beneficios/, consultado em 16/04/2013).

CONEXÃO

Assista ao vídeo sobre normas, tendo como exemplo a ergonomia no ambiente de trabalho: http://www.youtube.com/watch?v=qzSidOA8EaM

5.2.2 Como as Normas são criadas e utilizadas?

De acordo com o British Standards Institution (BSI), a tarefa de criar o primeiro "esboço" das normas cabe a um comitê técnico. Caso haja necessidade, este grupo pode subcontratar um consultor para complementar o esboço.

Vale lembrar que até mesmo para elaborar este "esboço" (rascunho) é necessário seguir padrões/regras de elaboração. Os princípios básicos que devem ser cumpridos é que uma norma só é passível de ser criada se for usável, verificável e comum.

Os tempos de desenvolvimento para as normas variam desde meses até vários anos. As Normas Britânicas são normalmente desenvolvidas em 12 – 15 meses, enquanto que normas internacionais tomam aproximadamente 3 anos. Normas comissionadas como as de qualidade PAS e OS podem ser desenvolvidas em meses para atender aos requisitos do cliente (Fonte: http://www.bsibrasil.com.br/publicacoes/sobre_normas/criacao/, consultado em: 16/04/2013)

É notável que o mercado consumidor demanda cada vez mais qualidade e credibilidade nos produtos e serviços que adquire. Por este e outros motivos as empresas têm buscado cada vez mais se adequar e se certificar nos padrões e normas estabelecidas, mesmo que estes não tenham de ser obrigatoriamente cumpridos por lei.

As normas também são usadas como uma alternativa flexível para a regulamentação. Em indústrias e setores velozes, as normas podem também oferecer economias significativas nos custos de Pesquisa e Desenvolvimento. Onde se estabelecem plataformas comuns para avanços tecnológicos, testadas e compartilhadas com todas as partes interessadas, isto pode assegurar a viabilidade comercial e a confiança do consumidor. As normas são essenciais para o comércio em mercados cada vez mais competitivos. Elas asseguram que qualquer empresa que oferece produtos, serviços ou processos seja:

- Eficaz em custos e eficiente no tempo;
- Comercialmente viável;
- Digna de confiança; e
- Segura.

Elas também podem fazer um impacto significativo sobre a sociedade como um todo. Por exemplo, como compradores ou usuários de produtos, nós rapidamente nos daríamos conta de que estes se tornaram de baixa qualidade, que não servem, que são incompatíveis com equipamentos que já temos, que são não confiáveis ou perigosos.

Nós não estamos normalmente conscientes do papel desempenhado pelas normas em elevar os padrões de qualidade, segurança, confiabilidade, eficiência e permutabilidade – bem como o de prover estes benefícios a um custo econômico (Fonte: http://www.bsibrasil.com.br/publicacoes/sobre_normas/utilizacao/, consultado em: 16/04/2013).

5.3 Compreendendo o Conceito de Regulamentação

A Confedereção Nacional da Indústria (CNI), órgão que representa nacionalmente todas as indústrias, afirma que:

Um regulamento técnico é um documento, adotado por uma autoridade com poder legal para tanto, que contém regras de caráter obrigatório e o qual estabelece requisitos técnicos, seja diretamente, seja pela referência a normas técnicas ou a incorporação do seu conteúdo, no todo ou em parte. Em geral, regulamentos técnicos visam assegurar aspectos relativos à saúde, à segurança, ao meio ambiente, ou à proteção do consumidor e da concorrência justa (Fonte: http://www.abimaq.org.br/site.aspx/Normalizacao, consultado em: 16/04/2013).

Um regulamento técnico estabelecido deve ser obrigatoriamente cumprido. Caso contrário, ou seja, no caso de descumprimento, haverá uma implicação legal com multa e "punição" (de acordo com o descrito no regulamento).

Significados de Regulamento:
Ato ou efeito de regular.
Estatuto, instrução que prescreve o que se deve fazer: regulamento de polícia.
Conjunto de prescrições que determinam a conduta de militares em qualquer circunstância.
Conjunto de regras para qualquer instituição ou corpo coletivo.
Conjunto de disposições governamentais que contém normas para execução de uma lei, decreto etc.: regulamento do consumo de água.

Ato de determinar, de regular em geral: regulamento de um negócio.
Sinônimos de regulamento: determinação, estatuto, preceito, regimento, regra e roteiro.

Fonte: www.dicio.com.br

De acordo com a Confedereção Nacional da Indústria (CNI), no Brasil ainda não há uma compilação oficial completa dos regulamentos estabelecidos. Desta forma, os interessados em adequar seus produtos, processo e serviços devem procurar os diversos órgãos do governo designados/competentes por cada assunto.

No âmbito do PBQP - Programa Brasileiro da Qualidade e Produtividade, o INMETRO liderou o projeto de modernização da regulamentação técnica federal, que inclui uma compilação dos regulamentos técnicos federais em vigor, bem como o estabelecimento de novas diretrizes para a sua redação.
Esse projeto ainda está em andamento, mas os resultados encontram-se numa Base de Dados, contendo a regulamentação técnica emitida pelo Ministério do Desenvolvimento, Indústria e Comércio Exterior, pelo Ministério de Ciência e Tecnologia e do próprio INMETRO (Fonte: http://www.normalizacao.cni.org.br/normas_tecnicas_regulamentos.htm, consultado em 16/04/2013).

É importante ressaltar que, quando uma empresa nacional deseja exportar um produto, ela deverá conhecer a regulamentação técnica vigente do país de destino da mercadoria, a fim de adequar-se para conseguir enviar o produto. Caso contrário, encontrará barreiras e impedimentos para tal procedimento.

Diante do exposto, e para que não haja tais barreiras, é aconselhável que os governos adotem regulamentos técnicos baseados em normas internacionalmente aceitas, conforme estipulado pelo Acordo de Barreiras Técnicas ao Comércio da Organização Mundial do Comércio (OMC).

Sempre que um governo decidir adotar um regulamento técnico que não siga uma norma internacional deve notificar formalmente os demais membros da OMC com antecedência mínima de 60 dias, apresentado uma justificativa.
Os demais membros da OMC podem solicitar esclarecimentos e apresentar comentários e sugestões ao regulamento proposto. Estas informações são veiculadas pelos chamados "pontos focais" (inquiry points).
Estas organizações, designadas por cada um dos membros da OMC, são as responsáveis por efetuar as notificações da regulamentação a ser adotada por esse país e pelo recebimento da comunicação das notificações efetuadas pelos outros países.
O inquiry point do Brasil é o **INMETRO**, onde se podem obter informações sobre as notificações efetuadas à OMC, tanto brasileiras quanto dos demais países da OMC (Fonte:http://www.normalizacao.cni.org.br/normas_tecnicas_regulamentos.htm, consultado em 16/04/2013).

A título informativo e de exemplo, vejam alguns dos órgãos regulamentadores por setor:

AGRICULTURA	www.agricultura.gov.br
AEROESPACIAL	www.mct.gov.br; www.inpe.br
AERONÁUTICA	www.defesa.gov.br; www.cta.br; www.ctex.eb.mil.br
MARINHA	www.defesa.gov.br; www.dpc.mar.mil.br
TRANSPORTES	www.transportes.gov.br; www.mj.gov.br/denatran; www.mte.gov.br

5.4 Normas e Regulamentações no Ambiente Organizacional

Os gestores de cada uma das áreas de uma empresa, e não somente o de T.I, devem conhecer suas respectivas demandas, normas, regulamentações etc. a fim de atender os objetivos traçados com eficiência, eficácia, segurança, e assim por diante.

As regulamentações internas de cada setor da empresa devem ser redigidas de forma clara para que seus respetivos colaboradores possam compreender seus papéis/funções/deveres com exatidão. Isto acarretará, entre outros fatores, a minimização dos riscos, a maximização do desempenho, a segurança de informações etc.

Tais regulamentações devem estar expressas em um documento formal, o qual deve ser explicado e assinado por cada funcionário no momento de sua contratação.

A seguir, apresentaremos itens considerados básicos para compor esta documentação. É certo que cada empresa possui necessidades peculiares, mas, de forma geral, os aspectos englobados podem ser considerados comuns.

5.4.1 Itens Básicos propostos para Regulamentarização

Se a empresa monitorar o uso dos recursos tecnológicos por parte de seus colaboradores, então isto deve estar claro e explícito no regulamento, de forma que eles possam compreender que não necessariamente a privacidade será garantida.

Sendo assim, e de forma geral, o documento deverá contemplar, dentre outras, as seguintes informações:

- Os colaboradores deverão estar cientes de que a empresa possui sistemas que realizam o monitoramento das atividades realizadas por eles na Internet (a exemplo: sites visitados, e-mails trocados, ligações feitas e/ou recebidas);
- Os colaboradores deverão estar cientes de que a empresa poderá a vir inspecionar todo e qualquer arquivo trafegado na rede;
- Os colaboradores deverão estar cientes do que podem ou não fazer com os recursos disponibilizados a eles pela empresa, a fim de cumprirem seus respectivos trabalhos;

• Os colaboradores deverão estar cientes de que não poderão instalar quaisquer outros softwares sem a autorização expressa e formal por parte da empresa;

• Os colaboradores deverão estar cientes de que não poderão alterar quaisquer parâmetros de proteção do firewall da empresa;

• Os colaboradores deverão estar cientes de que não podem copiar as ferramentas (softwares) disponibilizadas pela empresa para uso externo;

• Os colaboradores deverão estar cientes de que, se divulgarem quaisquer informações confidencias da empresa, poderão sofrer penalidades inclusive judiciais, além de demissão;

• Os colaboradores deverão estar cientes de que não poderão divulgar seus dados de "usuário" e "senha" para quaisquer outras pessoas, incluindo outros colaboradores, sob pena de responsabilizarem-se por tudo que for feito;

• Os colaboradores deverão estar cientes de que utilizar quaisquer recursos da empresa para atividades ilegais, implica em penalidades judiciais, além de demissão por justa causa;

• Os colaboradores deverão estar cientes de que poderão utilizar-se da Internet para atividades que não tenham a ver com a empresa, porém que sejam atividades legais, mas somente em seus respectivos horários de almoço ou fora do horário de expediente (a exemplo: acessar sites de redes sociais somente poderá ser feito no horário de almoço).

5.4.2 Política de Senhas

A empresa deverá ter uma política estabelecida para o uso de senhas e direitos de acesso de cada colaborador. Para tanto, existem algumas normas já estabelecidas que regulamentam o uso correto de senhas, com padrões de nível de segurança etc.

> [...] a seguir se apresenta o básico destas normas para se estipular senhas de usuários com mínimo risco. Da mesma forma, tais normas também devem ser apresentadas e explicadas a cada funcinário no momento de sua integração à empresa.
>
> - Histórico de senhas utilizadas: não deve ser possível reutilizar, pelo menos, as últimas 24 senhas;
> - Prazo para mudança da senha: pelo menos a cada 42 dias o usuário deve ser obrigado a alterar sua senha de trabalho;

- Prazo para poder trocar a senha depois da última troca: o usuário só poderá alterar a sua senha 02 dias após a última troca;
- Tamanho mínimo da senha: 06 caracteres;
- Senha precisa ser complexa (usar letras, números e caracteres especiais): Não, apenas em casos especiais, como administradores de sistema, deve ser exigida uma senha complexa. Para usuários finais, a senha pode ser de composição mais simples;
- Bloqueio da senha do usuário: depois de 03 tentativas sem sucesso a senha deve ser bloqueada por um período mínimo de 30 minutos (Fonte: http://lpiteli.wordpress.com/2012/02/16/regulamentacaoemti/, consultado em 16/04/2013).

5.4.3 Política de Acesso Lógico

Em uma empresa dinâmica, colaboradores podem ser realocados para setores e/ou cargos diferentes (inclusive de hierarquia diferente – abaixo ou acima). Com isto, carregarão também suas respectivas heranças de permissões de acesso aos sistemas da empresa. Isto deve ser tratado com minusciosa atenção.

Um estagiário aprendiz, por exemplo, que é encarregado de cobrir as férias em vários departamentos, acaba utilizando diversos módulos dos sistemas e a cada departamento lhe são dadas novas permissões, de forma que ao final de um período ele acaba se tornando um super usuário (Fonte: http://lpiteli.wordpress.com/2012/02/16/regulamentacaoemti/, consultado em 16/04/2013).

Diante do exposto, a empresa deverá periodicamente rever as permissões de acesso aos sistemas concedidas a cada usuário. A frequência desta "revisão de permissões" dependerá de cada empresa, ou seja, dependerá do fluxo de alterações de cargos e remanejamentos.

5.5 Lei Sarbanes-Oxley

A Lei Sarbanes-Oxley, conhecida também como SOX, é uma lei americana promulgada em 30/06/2002 pelos Senadores Paul Sarbanes e Michael Oxley.

Nela estão envolvidas as empresas que possuem capitais abertos e ações na Bolsa de NY e Nasdaq, inclusive várias empresas brasileiras estão se adequando a esta Lei.

O motivo que a fez entrar em vigor foi justamente a onda de escândalos corporativos-financeiros envolvendo a Eron (do setor de energia), a Worldcom (telecomunicações), entre outras empresas.

Os escândalos ocorreram, pois as empresas vinham forjando seus dados contábeis para mascarar a real situação financeira da empresa, ou seja, as informações não eram confiáveis. Os prejuízos financeiros foram imensos e atingiram milhares de investidores. Era necessário, portanto, uma pronta resposta, com o intuito de garantir que as informações contidas nesses balanços financeiros fossem condizentes com a realidade, dando mais segurança e transparência para o mercado de ações. Hoje, qualquer empresa que negocie ações na Bolsa de Nova York com na Nasdaq devem estar sujeitas a esta lei.

Uma vez que a lei foi implantada nos Estados Unidos, seus efeitos foram sentidos em todo o mercado de tecnologia ao redor do mundo. Em primeiro lugar porque, conforme mencionado anteriormente, qualquer empresa que negocie seu capital na Bolsa de Nova York ou Nasdaq deve se adequar a ela. Além disso, todas as empresas que são subsidiárias de multinacionais norte-americanas se viram obrigadas a se adequar à nova legislação.

Portanto, o objetivo desta lei é justamente aperfeiçoar os controles financeiros das empresas e apresentar eficiência na governança corporativa, a fim de evitar que aconteçam outros escândalos e prejuízos conforme os casos supracitados.
A lei visa garantir a transparência na gestão financeira das organizações, credibilidade na contabilidade, auditoria e a segurança das informações para que sejam realmente confiáveis, evitando assim fraudes, fuga de investidores etc. Esta lei pode ser deduzida como uma Lei de Responsabilidade Fiscal Sarbanes-Oxley (Fonte:http://www.smartsec.com.br/sarbanes-oxley.html, consultado em: 17/04/2013)

Segundo Baldissera e Nunes (2007), a empresa de auditoria KPMG destaca como principais tópicos da desta lei os seguintes:

- A promoção da boa governança corporativa e práticas de negócio;
- O aumento na independência do auditor externo;
- A obrigação de ter um Comitê de Auditoria Independente;
- A definição do papel de crítica de controle interno através de certificações e declarações;
- A transparência nos relatórios e nas informações aos acionistas e restrição de trabalhos *non-audit* pelo auditor externo.

As principais seções da lei definem que o principal executivo (CEO) e o principal executivo de finanças (CFO) assumam a responsabilidade por definir, avaliar e monitorar a eficácia dos controles internos sobre relatórios financeiros e divulgações da empresa e que a validação dos controles e procedimentos internos sobre os relatórios financeiros deva ser formal e realizada anualmente por auditores externos. (BALBO, 2007).

Diante deste cenário, a ação da TI é de fundamental importância nesse processo. É a área responsável pelo controle, segurança da informação e sistemas. Portanto, deverá estar alinhada na adequação desta Lei para garantir às regras de transparência fiscal e financeira.

Empresas brasileiras como Petrobras, TAM Linhas Aéreas, Sabesp, Brasil Telecom, dentre outras, tiveram de adequar sua área de TI para suportar a Lei Sarbanes-Oxley.

5.6 Gestão da Segurança da Informação Segundo as Normas NBR ISO/IEC 27001 e ISO/IEC 27002

A norma ABNT NBR ISO/IEC 17799:2005 é referenciada como indispensável para a aplicação da norma ABNT NBR ISO/IEC 27001. Contudo, a ABNT NBR ISO/IEC 17799:2005 foi cancelada e substituída pela ABNT NBR ISO/IEC 27002, a qual iremos conhecer.

No entanto, e apenas para iniciar a contextualização do assunto, explicita-se que o grande objetivo dessa norma (ISO/IEC 17799:2005) é determinar as diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão de segurança de informação em uma empresa.

Os objetivos de controle e os controles desta Norma têm como finalidade ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. Esta Norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão de segurança, e para ajudar a criar confiança nas atividades interorganizacionais (ABNT, 2005).

5.6.1 Norma ISO/IEC 27001

A ABNT NBR ISO/IEC 27001 – Sistemas de gestão de segurança da informação - Requisitos especifica requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Um SGSI é um sistema de gestão desenvolvido para a segurança da informação de uma organização, baseado em uma abordagem de riscos do negócio. O documento da norma é estruturado em oito seções. A título de informação, nesta disciplina abordaremos somente os prontos principais de tal norma.
A norma sugere a adoção de uma abordagem de processo para um SGSI, ou seja, que a organização deve identificar e gerenciar os processos envolvidos em um Sistema de Gestão de Segurança da Informação, bem como reconhecer suas interações.
Além disso, a ABNT NBR ISO/IEC 27001 também adota o ciclo denominado PDCA (Plan, Do, Check, Act) para estruturar todos os processos envolvidos em um SGSI.
O PDCA é uma ferramenta gerencial que possibilita a melhoria contínua de processos e a solução de problemas. (Fonte: http://qualitnews.blogspot.com/2010/10/conhecendo-abnt-nbr-isoiec-27001-parte.html, consultado em 18/04/2013)

CONEXÃO

Assista à animação que ilustra o conceito de PDCA: http://www.youtube.com/watch?v=ekl2DvV-dOo

O Ciclo PDCA, também conhecido como Ciclo de Shewhart ou Ciclo de Deming, é uma ferramenta de gestão muito utilizada pelas empresas do mundo todo. Este sistema foi concebido por Walter A. Shewhart e amplamente divulgado por Willian E. Deming e, assim como a filosofia Kaizen, tem como foco principal a melhoria contínua. Seu foco é tornar os processos da gestão de uma empresa mais ágeis, claros e objetivos. Pode ser utilizado em qualquer tipo de empresa como forma de alcançar um nível de gestão melhor a cada dia, atingindo ótimos resultados dentro do sistema de gestão do negócio.

O Ciclo PDCA tem como estágio inicial o **planejamento da ação,** em seguida tudo o que foi planejado é **executado**, gerando, posteriormente, a necessidade de **checagem** constante destas ações implementadas. Com base nesta análise e comparação das ações com aquilo que foi planejado, o gestor começa então a **implantar medidas** para correção das falhas que surgiram no processo ou produto.

Fonte: http://www.sobreadministracao.com/o-ciclo-pdca-deming-e-a-melhoria-continua/>. Consultado em: 18/04/2013

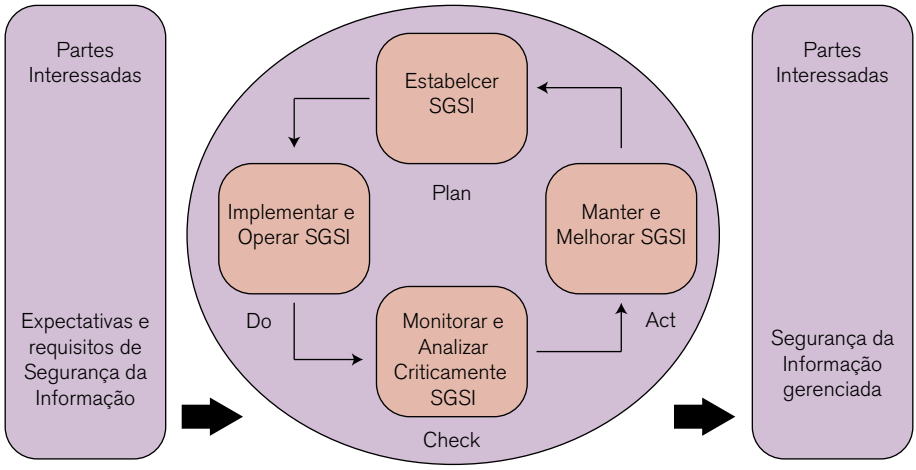


Figura 5.10 – Ciclo PDCA aplicado aos processos de um Sistema de Gestão de Segurança da Informação. Fonte: http://qualitnews.blogspot.com/2010/10/conhecendo-abnt-nbr-i-soiec-27001-parte.html (consultado em 18/04/2013).

Na fase **PLAN** estabelece-se a política, metas, processos etc. de um Sistema de Gestão de Segurança da Informação (SGSI). Na fase **DO,** implementa-se e operaciona-se o que foi estabelecido pela fase anterior (Plan). Na fase **Check**, é

feito o monitoramento e avaliação do desempenho do SGSI. Os resultados são dispostos para a alta direção, a fim de fazerem uma análise detalhada. Por último, na fase **ACT** são colocadas em prática, ou seja, em ação, as ações corretivas preventivas que foram identificadas ao longo do ciclo.

Ressalta-se que a ABNT NBR ISO/IEC 27001 está alinhada às normas ABNT NBR ISO 9001:2000 e ABNT NBR ISO 14001:2004, de forma a permitir que seja compatível com outros sistemas de gestão.

A ABNT NBR ISO/IEC 27001 tem como objetivo especificar requisitos para o estabelecimento, implementação, operação, monitoração, análise crítica, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação (SGSI). Os requisitos são genéricos, de maneira a permitir que sejam aplicáveis a quaisquer organizações, independentemente do tipo, tamanho e natureza.

É importante salientar que não é aceitável que uma organização que pretenda estar conforme a norma exclua quaisquer requisitos. Porém, qualquer exclusão de controles considerada necessária para satisfazer aos critérios de aceitação de riscos precisa ser justificada e as evidências de que os riscos associados foram aceitos pelas pessoas responsáveis precisam ser fornecidas. Onde quaisquer controles forem excluídos, reivindicações de conformidade a esta Norma não são aceitáveis, a menos que tais exclusões não afetem a capacidade da organização, e/ou responsabilidade de prover segurança da informação que atenda os requisitos de segurança determinados pela análise/avaliação de riscos e por requisitos legais e regulamentares aplicáveis.

A ISO/IEC 27001 é a única norma internacional auditável que define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). A norma é designada para assegurar a seleção de controles de segurança adequados e proporcionais. Ela ajuda a empresa a proteger seus ativos da informação e dar confiança para todas as partes interessadas, especialmente os clientes. A norma adota uma abordagem de processo para o estabelecimento, implementação, operação, monitoramento, revisão, manutenção e melhoria de seu SGSI.

A ISO/IEC 27001 é aplicável para qualquer organização, grande ou pequena, em qualquer setor ou parte do mundo. A norma é especialmente aplicável onde a proteção da informação é crítica, assim como finanças, saúde, setores público e de TI.

A ISO/IEC 27001 é também altamente eficaz para organizações que gerenciam informação em nome de terceiros, assim como companhias terceirizadas de TI: Ela pode ser usada para garantir a seus clientes que suas informações estão sendo protegidas. (Fonte: http://qualitnews.blogspot.com/2010/10/conhecendo-abnt-nbr-isoiec-27001-parte.html, consultado em 18/04/2013)

A certificação de seu SGSI na ISO/IEC 27001 pode trazer os seguintes benefícios para sua organização, de acordo com o British Standards Institution (BSI):

• Demonstra a garantia independentemente de seus controles internos e que os requisitos de governança corporativa e de continuidade do negócio estão sendo atendidos;

• Demonstra de forma independente que as leis e os regulamentos aplicáveis são observados;

• Proporciona uma vantagem competitiva por cumprir requisitos contratuais e demonstrar para seus clientes que a segurança da informação é levada como de suma importância pela sua organização;

• De forma independente verifica que os seus riscos organizacionais são corretamente identificados, avaliados e gerenciados, enquanto formaliza os processos de segurança da informação, de procedimentos e de documentação;

• Comprova o comprometimento da alta direção na segurança de suas informações;

• O processo de auditoria regular ajuda sua empresa a monitorar continuamente o seu desempenho e melhoria.

5.6.2 Norma ISO/IEC 27002

A norma NBR ISO/IEC 27002 – Código de Prática para a Gestão de Segurança da Informação, tem como objetivo "estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização". Mas, o que é Segurança da Informação (SI)? Significa proteger as informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio da organização.

É preciso esclarecer que anteriormente esta norma era conhecida como NBR ISO/IEC 17799, mas a partir de 2007 a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração como ISO/IEC 27002 (ABNT, 2005).

Entre os tópicos abrangidos pela norma, citamos suscintamente:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	deve ser formalizada através de um documento e comunicada a todos de forma clara. Da mesma forma, tal política deve ser revisada periodicamente e fim de se analisar se os padrões estabelecidos permanecerão ou deverão ser alterados/substituídos/extintos.
ORGANIZANDO A SEGURANÇA DA INFORMAÇÃO	através de uma estrutura de gerenciamento, contendo representantes (estratégicos) de diversas áreas da organização. Importante também estabelecer acordos de sigilo para informações confidenciais ou de acesso restrito;
GESTÃO DE ATIVOS	visa a manter e proteger os ativos organizacionais. Para tanto, deve-se primeiramente identificá-los, classificá-los, catalogá-los, etc. de forma que um inventário de ativos possa ser estruturado e posteriormente mantido;
SEGURANÇA EM RECURSOS HUMANOS	as descrições de cargo e os termos e condições de contratação devem ser explícitos, especialmente no que tange às responsabilidades de segurança da informação. É importante também analisar minuciosamente os candidatos a cargo que forem lidar diretamente com informações sigilosas; Durante todo o tempo em que funcionários, fornecedores e terceiros estiverem trabalhando na empresa, eles devem estar conscientesdas ameaças relativas à segurança da informação, bem como de suas responsabilidades e obrigações.

SEGURANÇA FÍSICA E DO AMBIENTE	deve ser feito o controle de forma rigorosa, contendo níveis e controles de acesso apropriados, incluindo proteção física. Os equipamentos também devem ser protegidos contra ameaças físicas e ambientais, incluindo aqueles utilizados fora do local.

5.7 ITIL

Como já exemplificamos ao longo do curso, são de fundamental importância os mecanismos de controle rígidos sobre os processos de negócios das empresas. Por mais que os funcionários das empresas sempre julguem suficientes os mecanismos existentes, sempre que há algum escândalo de fraude, como ocorreu no caso da lei de Sarbanes-Oxley, os profissionais da área de segurança se perguntam o que pode ser feito para garantir tal segurança. Um dos caminhos que se buscam nesse caso é um controle sobre o ambiente de TI.

Um modelo que vem obtendo sucesso e reconhecimento é o ITIL (Information Technology Infrastructure Library). Ele foi desenvolvido pela CCTA (Central Computer and Telecommunication Agency), hoje conhecido como OGC (Office of Government Commerce), do Reino Unido, no final dos anos 80. Trata-se de um conjunto de referência com as melhores práticas para o Gerenciamento de Serviços de TI (Fonte: http://www.leansixsigma.com.br/acervo/acervo_4713547.pdf, consultado em 18/04/2013)

O ITIL está dividido em Processos Operacionais e Processos Estratégicos. A tabela a seguir descreve os processos do ITIL:

PROCESSOS OPERACIONAIS	PROCESSOS ESTRATÉGICOS
Service Desk (Função)	Gerenciamento de Nível de Serviço
Gerenciamento de Incidente	Gerenciamento de Disponibilidade
Gerenciamento de Problema	Gerenciamento de Capacidade
Gerenciamento de Mudança	Gerenciamento de Continuidade de Serviços de TI
Gerenciamento de Configuração	Gerenciamento Financeiro de TI
Gerenciamento de Liberação	

Tabela 5.2 – Processos do ITIL. Fonte: Adaptado de Jesus (2007).

CONEXÃO

Para conhecer mais sobre o que é determinado em cada processo do ITIL, acesse: http://www.viacerta.com.br/informatica/itil/itil_proc.html

O uso efetivo das melhores práticas definidas na ITIL traz inúmeros benefícios às organizações, como: melhoria na utilização dos recursos; maior competitividade; redução de retrabalhos; eliminação de trabalhos redundantes; melhoria da disponibilidade, confiabilidade e segurança dos serviços de TI; qualidade dos serviços com custos justificáveis; fornecimento de serviços alinhados aos negócios, aos clientes e às demandas dos usuários; processos integrados; responsabilidades documentadas e comunicadas amplamente, e registro e controle de lições aprendidas (BALBO, 2007, p. 26).

ATIVIDADES

01. Sobre o conceito de Norma, leia as asserções e assinale a alternativa correta.

I. Uma norma é um documento que contém uma regulamentação;

II. Uma norma é um documento que contém uma descrição técnica, específica e precisa de critérios a serem cumpridos;

III. As normas fazem sentido se tornam a vida mais complicada.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) Somente a asserção III está correta.
d) As asserções I e III estão corretas.
e) As asserções II e III estão corretas.

02. "Um (I) é um documento, adotado por uma autoridade com poder legal para tanto, que contém regras de caráter obrigatório e o qual estabelece requisitos técnicos, seja diretamente, seja pela referência a normas técnicas ou a incorporação do seu conteúdo, no todo ou em parte."

No texto acima, (I) refere-se a: (assinale a alternativa correta)

a) Recurso.
b) Norma.
c) Projeto.
d) Regulamento técnico.
e) Processo.

03. Considerando o contexto organizacional, leia as asserções e assinale a alternativa correta.

I. Os gestores de cada uma das áreas de uma empresa devem conhecer suas respectivas demandas, normas, regulamentações etc.

II. As regulamentações internas de cada setor da empresa devem ser redigidas de forma clara para que seus respectivos colaboradores possam compreender seus papéis/funções/deveres com exatidão.

III. As regulamentações devem estar expressas em um documento formal, o qual deve ser explicado e assinado por cada funcionário no momento de sua contratação.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) Somente a asserção III está correta.
d) As asserções I e II estão corretas.
e) As asserções I, II e III estão corretas.

REFLEXÃO

Vimos neste capítulo o quão importante é a segurança da informação em nível de normas e regulamentações. Ou seja, não basta apenas implantar uma política de segurança organizacional, incluindo dispositivos de segurança, restrições de acesso, treinamento de usuários etc. É necessário também cumprir algumas exigências (normas/regulamentações) a fim de se atingir certo nível de segurança e, portanto, conquistar, entre outras coisas, a credibilidade dos clientes e do mercado.

Ou seja, as normas e regulamentos certificam que a empresa está fazendo algo do jeito preestabelecido por determinado padrão nacional ou mundial.

LEITURA

Como já tratamos dos mais diversos aspectos para a Gestão da Segurança, desde a conscientização de sua importância, passando pelos mecanismos que devemos seguir para obter tal gestão e finalizando com as normas que regulam e orientam esse setor, temos certeza de que você está apto a avaliar o processo de uma empresa e, focando-se em TI, propor melhorias, controles ou até mesmo correções em procedimentos que hoje são encarados com naturalidade.

Entretanto, para tornar um pouco mais concreta a prática da nossa disciplina, vamos apresentar na sequência um estudo de caso da American Express. A empresa é uma Instituição Financeira prestadora de serviços de viagens e turismo. Foi criado na empresa um programa de segurança denominado "Security Awareness Training". Destacaremos as 13 Políticas de Segurança que a American Express possui e que foram relatadas por Araujo (2005), da seguinte forma:

1. Gerenciamento de Segurança: a liderança executiva endossa a missão, "charte" (estatutos, o documento escrito), a autoridade e estrutura da segurança de informação;

2. Gerenciamento de Risco: risco é o impacto em potencial ou nível de dano que a perda de um bem ou recurso poderia ter. Controles de segurança apropriados devem ser embutidos nas fontes de informação da American Express;

3. Segurança de Pessoal: controles de segurança de informação devem ser implementados para assegurar que indivíduos contratados pela American Express sejam monitorados apropriadamente e de que estes estejam cientes das políticas de segurança da American Express;

4. Segurança Física: as instalações de processamento e as fontes de informação devem ter controles de acesso físico apropriados instalados para protegê-los de qualquer acesso físico não autorizado e devem ser protegidas contra quaisquer perigos ambientais e penetração eletrônica passiva ou ativa;

5. Gerenciamento de Operações: gerenciadores de sistema e de aplicativos devem ter o nível mínimo de privilégio de acesso exigido para desempenharem suas funções, e devem aderir aos procedimentos formais quando trabalharem com todas as fontes de informação. Adicionalmente, tarefas operacionais devem ser segregadas de acordo com o papel e responsabilidades do usuário;

6. Monitoração de Segurança e Resposta: fontes de informação devem ser monitoradas para detectar eventos operacionais, de segurança e de sistema. A reação a incidentes e procedimentos de investigação deve registrar eventos para assegurar uma resposta rápida a incidentes de segurança de informação;

7. Gerenciamento de Comunicação: a troca de informação entre a American Express e outras organizações deve ser protegida por controles adequados. Fontes de comunicação devem ser usados para fins comerciais apenas;

8. Controle de acesso: funcionários devem ser identificados positivamente e autorizados antes de ter acesso às fontes de informação da American Express. Acesso baseado na função de um funcionário é limitada a um mínimo necessário para a realização de sua tarefa;

9. Segurança de Rede: para explorar os benefícios comerciais oferecidos pelo acesso externo e gerenciar os riscos associados eficientemente, controles de segurança rigorosos devem ser implementados. Existem controles de segurança que são exigidos quando a rede interna da American Express está conectada a redes, equipamentos ou aparelhos externos;

10. Serviços Terceirizados: terceiros devem aderir às Políticas de Segurança da American Express e devem reconhecer sua responsabilidade através de uma declaração formal por escrito;

11. Desenvolvimento de Aplicativos: atividades de desenvolvimento de aplicativos devem se conformar a uma metodologia de desenvolvimento que incorpore controles de segurança de informação em cada estágio do desenvolvimento.

12. Recuperação e Continuidade Comercial: as fontes críticas de informação da American Express devem desenvolver planos de contingência que possibilitem a continuidade de serviços de informação crítica em caso de interrupção; e

13. Políticas de Conformidade Legal e Regulatória: todos os funcionários devem estar em conformidade com requerimentos contratuais e regulatórios legais locais e internacionais.

O intuito de mostrar esse estudo de caso é para enfatizar mais uma vez a importância da gestão de segurança e como ela é encarada pelas empresas. Com um exemplo concreto talvez fique mais fácil você pensar em organizar a política de segurança de sua empresa.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – **Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 – Tecnologia da informação** – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2005.

ABNT – **Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001 – Tecnologia da informação** – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2006.

ARAUJO, E. E. A **Vulnerabilidade Humana na Segurança da Informação.** Monografia de Conclusão do Curso de Sistemas de Informação, UNIMINAS, 2005.

ARAUJO, E. N. **Curso de Direito Administrativo.** Editora Saraiva, 2009.

BALBO, L. O. **Uma Abordagem Correlacional dos Modelos CobiT / ITIL e da Norma ISO 17799 para o tema Segurança da Informação.** Monografia de Especialização em Tecnologia da Informação - Departamento de Engenharia de Computação e Sistemas Digitais, Escola Politécnica - USP, São Paulo, 2007.

BALDISSERA, T. A.; NUNES, R. C. **Impacto na Implementação da Norma NBR ISO/IEC 17799 para a Gestão da Segurança da Informação em colégios:** um estudo de caso. In: Encontro Nacional de Engenharia de Produção – ENEGEP, Foz do Iguaçu, Anais, 2007.

BRITISJ STANDARDS INSTITUTION (BSI) – consultado em: www.bsibrasil.com.br

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA (CNI) – consultado em: http://www.normalizacao.cni.org.br

FONTES, E. **Praticando a Segurança da Informação.** Editora Brasport, 1ª edição, 2008.

JESUS, A. **Gestão Estratégica de TI por meio dos Princípios da ITIL e da Utilização da Ferramenta Balance Scorecard.** Monografia de Conclusão de curso, Centro de Ciencias Exatas e Tecnologia, Pontífica Universidade Católica, 2007.

PITELI, L. **Regulamentação e governança em tecnologia da informação.** Trabalho de Conclusão de Curso de Pós Graduação em Gestão Estratégica de Negócios, Faculdades Integradas Dom Pedro II, 2007.

GABARITO

Capítulo 1

01. B

A informação pode ser classificada em níveis de prioridade dentro da organização, conforme segue:

- Informação Pública: informação que pode vir ao público sem consequências prejudiciais ao funcionamento normal da empresa, e cuja integridade não é vital;
- Informação Interna: informação que deveria ter o livre acesso evitado, embora não haja consequências prejudiciais/sérias do acesso e uso não autorizado. A integridade deste tipo de informação é importante, porém não vital;

- Informação Confidencial: informação que é restrita aos limites da empresa e cuja divulgação ou perda pode acarretar a desequilíbrio operacional e, eventualmente, perdas financeiras ou de confiabilidade perante o cliente externo;
- Informação Secreta: informação muito crítica para as atividades da empresa e cuja integridade deve ser preservada a qualquer custo. O acesso deve ser restrito e a segurança deste tipo de informação é crucial/vital para a empresa.

02. C

Um dado é uma entidade matemática sintática, ou seja, os dados podem ser descritos por estruturas de representação. Assim sendo, podemos dizer que o computador é capaz de armazenar dados. Estes dados podem ser quantificados, conectados entre si e manipulados pelo processamento de dados. Da mesma forma, pode-se definir dados como fatos brutos, ainda não organizados nem processados.

A informação depende de algum tipo de relacionamento, avaliação ou interpretação dos dados. Podemos agrupar dados isolados e torná-los consistentes ao se transformarem em informações.

O conhecimento é uma abstração interior, pessoal, de algo que foi experimentado, vivenciado, por alguém.

03. D

Para melhorar a segurança de um sistema, deve-se prioritariamente considerar alguns aspectos, dentre os quais:

- Conhecer os possíveis oponentes, identificando o que eles desejam fazer, e os perigos que podem vir a causar à organização;
- Contabilizar os valores, uma vez que a implementação e o gerenciamento da política de segurança pode significar, além da necessidade de mais recursos pessoais, a necessidade de significativos recursos de software e de hardware. Os custos das medidas de segurança devem, portanto, ser compatíveis e proporcionais às necessidades da organização e às probabilidades de ocorrerem incidentes de segurança;
- Considerar os fatores humanos, uma vez que muitos procedimentos de segurança falham, porque as reações dos usuários a esses procedimentos não são considerados com seu devido valor;
- Conhecer os pontos fracos, pois todo sistema possui vulnerabilidades;
- Aplicar a segurança de acordo com os negócios da organização, a fim de definir uma estratégia de segurança que melhor se adapte às necessidades dela.

04. D

As informações devem cumprir os seguintes requisitos:

- Autenticação: irá definir que as partes envolvidas na comunicação sejam autenticadas a fim de garantir que cada um deles seja realmente quem diz ser;
- Integridade: irá definir que a informação é originária de quem diz originar, de forma a impedir que alterações na mensagem original confundam as partes envolvidas na comunicação. E, mesmo que haja alguma alteração na mensagem original, que esta seja passível de ser detectada;
- Não repúdio: irá garantir que a informação enviada por quaisquer partes envolvidas na comunicação não seja negada pelo seu respetivo remetente (em outras palavras, irá garantir que quem enviou a informação não poderá negar sua transmissão);
- Disponibilidade: irá definir que as informações devidas estarão disponíveis para seus respectivos usuários. Aqui cabe uma ressalva: para garantir esta disponibilidade da informação somente para o usuário devido, deve-se implementar controles de acesso, a fim de conter usuários não autorizados.

05. E

Para melhorar a segurança de um sistema, deve-se prioritariamente considerar alguns aspectos, dentre os quais:

- Conhecer os possíveis oponentes, identificando o que eles desejam fazer, e os perigos que podem vir a causar à organização;
- Contabilizar os valores, uma vez que a implementação e o gerenciamento da política de segurança podem significar, além da necessidade de mais recursos pessoais, a necessidade de significativos recursos de software e de hardware. Os custos das medidas de segurança devem, portanto, ser compatíveis e proporcionais às necessidades da organização e às probabilidades de ocorrerem incidentes de segurança;
- Considerar os fatores humanos, uma vez que muitos procedimentos de segurança falham, porque as reações dos usuários a esses procedimentos não são considerados com seu devido valor;
- Conhecer os pontos fracos, pois todo sistema tem vulnerabilidades;
- Aplicar a segurança de acordo com os negócios da organização, a fim de definir uma estratégia de segurança que melhor se adapte às necessidades dela.

06. C

Ao mencionarmos a segurança da informação, e antes de cogitarmos a possibilidade de nos "munir" com aparatos tecnológicos, devemos prioritariamente fazer um levantamento e nos questionar/indagar:

- O que minha empresa quer proteger? (ou seja, tomar ciência do que se almeja proteger);

- Por que minha empresa quer proteger? (ou seja, descobrir a relevância de tais informações que se almeja proteger);
- Minha empresa quer se proteger de quê? (ou seja, fazer um mapeamento/levantamento do que se deve monitorar para que as informações não sejam extraviadas/corrompidas);
- Como minha empresa deve proteger? (ou seja, determinar normas/regras de como, quando, onde, quem poderá ter acesso).

Capítulo 2

01. C

Descarte: conforme deduzimos, o descarte ocorre no momento em que a informação não é mais útil. Desta forma, arquivos em papel são descartados em lixeiras, arquivos eletrônicos são apagados do banco de dados, CD's contendo informações sem serventia são descartados, e assim por diante.

Ao mencionarmos a etapa de descarte, é importante ressaltar que ela não pode ser realizada sem critérios. Descartar informações confidenciais, com valor legal etc. de qualquer forma acarreta sérios impactos negativos.

Aliás, e em se tratando dos documentos com valor legal, deve-se atentar que o seu descarte deve obedecer aos prazos determinados em lei.

Outra ressalva diz respeito a documentos com valor histórico permanente, pois eles não poderão ser descartados. Um documento secreto, por exemplo, pode vir a ser considerado (a princípio) como sendo um documento de valor histórico permanente.

02. E

Vulnerabilidades naturais: são aquelas decorrentes de fenômenos naturais e que trazem riscos para equipamentos e informações. Exemplos: inundações, terremotos, maremotos, furacões etc.

Vulnerabilidades físicas: são os ambientes que têm pontos fracos em nível do espaço físico, comprometendo o armazenamento e gerenciamento correto das informações. Exemplos: instalações inadequadas para o trabalho, falta de extintores de incêndio, local desorganizado, pessoas não autorizadas transitando no local etc.

Vulnerabilidades de Hardware: são aquelas relacionadas aos equipamentos que apresentam defeitos de fabricação ou configuração inadequada, podendo permitir o ataque de vírus ou violações. Exemplos: a falta de atualizações dos programas e equipamentos não dimensionados corretamente;

Vulnerabilidades de Software: são os pontos fracos existentes nos aplicativos de software, permitindo o acesso de indivíduos não autorizados. Por esta razão que os softwares, são os preferidos dos elementos que buscam as ameaças. Exemplos: Aplicativos com configura-

ções ou instalações inadequadas, programas de e-mail que permitem a execução de códigos maliciosos e falta de atualizações necessárias;

Vulnerabilidades de Armazenamento: as informações são armazenadas em suportes físicos (disco rígido) ou magnéticos (CD, DVD, cartão de memória, pen drive etc.). Suas utilizações inadequadas podem ocasionar uma vulnerabilidade, afetando, portanto, a integridade, a disponibilidade e a confidencialidade das informações. Consequentemente, isto pode danificar ou indisponibilizar os meios de armazenamento. Exemplos: defeito de fabricação de um meio de armazenamento, uso incorreto destes meios, prazo de validade e expiração ultrapassados;

Vulnerabilidades de Comunicação: são aquelas relacionadas com o tráfego de informações, os quais podem ser realizados através de fibra óptica, ondas de rádio, satélite ou cabos. Independentemente do meio escolhido, o sistema de comunicação escolhido deve ser seguro e garantir que as informações transmitidas alcancem o destino desejado sem intervenção alheia. Além disso, as informações trafegadas devem ser criptografadas, pois, caso haja alguma falha no processo, a informação não pode ser acessada por pessoas não autorizadas;

Vulnerabilidades Humanas: são aquelas atitudes intencionais ou não que podem gerar vulnerabilidades às informações, como, por exemplo: uso de senha fraca, compartilhamento de credencial de acesso, falta de treinamentos para o usuário, a não consciência ou desconhecimento de segurança da informação e funcionários descontentes.

Capítulo 3

01. E

Existem três fontes principais, conforme explicitado pelas normas da ABNT (2008), para que uma organização identifique seus requisitos de segurança:

- A primeira é o conjunto de princípios, objetivos e necessidades para o processamento da informação que uma organização tem de desenvolver para apoiar suas operações;
- A segunda é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm de atender;
- As duas anteriores são utilizadas como referências para desenvolver a principal fonte de requisitos de segurança, que é derivada da avaliação de riscos, processo responsável por identificar as ameaças aos ativos, as vulnerabilidades com suas respectivas probabilidades de ocorrência e os impactos ao negócio.

02. D

As ameaças à segurança de uma organização estão, sempre, relacionadas com a perda de uma (ou mais) das suas três características principais, que são:

- Perda da Integridade, que acontece quando certa informação fica exposta ao manuseio de uma pessoa não autorizada, que acaba por efetuar alterações não aprovadas e sem o controle, privado ou corporativo, do proprietário da informação;
- Perda de confidencialidade. Ocorre quando há uma quebra de sigilo de uma determinada informação, como a senha de um usuário ou administrador, por exemplo, o que permite que informações restritas, que deveriam estar acessíveis apenas para um determinado grupo de usuários, fiquem expostas;
- Perda de disponibilidade, que acontece quando a informação deixa de estar acessíve justamente por quem necessita dela. É o caso que ocorre com a perda de comunicação com um sistema importante para a empresa, que pode acontecer com a queda de um servidor, de uma aplicação crítica de negócio, que pode apresentar uma falha, devido a um erro causado por motivo interno ou externo ao equipamento.

03. B

Vírus propagado através do e-mail: recebido como um arquivo anexado ao e-mail cujo conteúdo induz o usuário a executá-lo. Ao fazer isto, o vírus infecta arquivos e programas e replica cópias de si mesmo para os contatos de e-mails armazenados no computador infectado;

Vírus de script: escrito em linguagem como VBScript e JavaScript por exemplo, e recebido ao acessar uma página Web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML;

Vírus de macro: tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem, como, por exemplo, os que compõem o Microsoft Office (Word, Excel, Power Point, etc);

Vírus de Smartphone: se propaga de celular a celular por meio da tecnologia Bluetooth ou de mensagens multimídia. Esta infecção ocorre quando um usuário permite o recebimento do arquivo infectado e o executa em seu celular. Após infectar o aparelho, o vírus pode destruir, sobrescrever arquivos, remover contatos, drenar a carga de bateria, propagar-se para outros celulares etc;

Capítulo 4

01. D

O risco é inevitável. Por exemplo, quando:

- Investidores compram ações;

- Cirurgiões realizam operações;
- Engenheiros projetam pontes;
- Empresários abrem seus negócios;
- Políticos concorrem a cargos eletivos etc.

Ou seja, administrar os riscos – que sempre irão existir – torna-se estratégico e, além disto, pode vir a se transformar em oportunidades. Portanto, deve-se transcender o "medo aos riscos" para "saber lidar de forma estratégica com os riscos".

Na área de tecnologia da informação e comunicação, risco é considerado como o impacto negativo motivado pela exploração de uma vulnerabilidade, considerando a possibilidade e o impacto da sua ocorrência. O processo para identificar, mensurar e planejar passos para reduzir um determinado risco a níveis aceitáveis pela organização é definido como Gerenciamento de Riscos (STONEBURNER, 2002 apud GONÇALVES, 2008, p. 15)

02. E

O gerenciamento de riscos é um processo que tem como objetivo dar subsídios à organização para realizar sua missão institucional, de forma a:

- Possibilitar a segurança efetiva dos sistemas de Tecnologias de Informação e Comunicação, responsáveis pelo processamento, armazenagem e transmissão de dados;
- Criar uma base sólida para as tomadas de decisão, principalmente no que se relaciona com execução coerente do orçamento e no investimento em tecnologias necessárias para minimizar riscos de impacto ou potencial impacto para o negócio; e
- Permitir aos gestores equilibrarem seus custos de proteção e desempenho dos sistemas de informação vitais para o negócio.

03. D

Existem alguns passos sequenciais para avaliar os riscos:

1. Caracterização do ambiente;
2. Identificação de ameaças;
3. Identificação de vulnerabilidades;
4. Análise de controles;
5. Determinação de probabilidades;
6. Análise de impacto;
7. Definição dos riscos;
8. Recomendações de controle; e
9. Documentação dos resultados.

01. B

Uma norma é um documento que contém uma descrição técnica, específica e precisa de critérios a serem cumpridos como regras/diretrizes.

As normas fazem sentido se tornarem a vida mais simples e elevarem o nível de confiabilidade de produtos e serviços que utilizamos.

As normas são criadas formando um conjunto de experiência e conhecimento de todas as partes interessadas, tais como produtores, vendedores, compradores, usuários e regulamentadores de material, produto, processo ou serviço em particular.

As normas são desenvolvidas para uso voluntário e não impõem nenhuma regulamentação.

02. D

Um regulamento técnico é um documento, adotado por uma autoridade com poder legal para tanto, que contém regras de caráter obrigatório e o qual estabelece requisitos técnicos, seja diretamente, seja pela referência a normas técnicas ou à incorporação do seu conteúdo, no todo ou em parte.

03. E

Os gestores de cada uma das áreas de uma empresa, e não somente o de TI, devem conhecer suas respectivas demandas, normas, regulamentações etc., a fim de atender aos objetivos traçados com eficiência, eficácia, segurança, e assim por diante.

As regulamentações internas de cada setor da empresa devem ser redigidas de forma clara, para que seus respectivos colaboradores possam compreender seus papéis/funções/deveres com exatidão. Isto acarretará, entre outros fatores, minimização dos riscos, maximização do desempenho, segurança de informações etc.

Tais regulamentações devem estar expressas em um documento formal, o qual deve ser explicado e assinado por cada funcionário no momento de sua contratação.

ANOTAÇÕES