UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
Centro de Ciências Jurídicas e Econômicas
Faculdade de Administração e Ciências Contábeis
Curso de Biblioteconomia e Gestão de Unidades de Informação

Hugo Bauer Rego

A importância da Segurança da Informação para os Sistemas de Automação de Unidades de Informação

Rio de Janeiro
2011

Hugo Bauer Rego

A importância da Segurança da Informação para os Sistemas de Automação de Unidades de Informação

Trabalho de Conclusão de Curso (TCC) apresentado como requisito para obtenção do título de Bacharel em Biblioteconomia, da Universidade Federal do Rio de Janeiro.

Orientadora: Profª Ms. Maria Irene da Fonseca e Sá
Orientadora de forma: Profª Ms. Maria de Fátima Borges Gonçalves de Miranda

Rio de Janeiro
2011

R343i REGO, Hugo Bauer.
A importância da Segurança da informação para os sistemas de automação / Hugo Bauer Rego. – Rio de Janeiro, 2011.

29 f. ; 30 cm.

Orientadora: Maria Irene da Fonseca e Sá.
Orientadora de forma: Maria de Fátima Borges Gonçalves de Miranda.
Projeto Final II (Graduação em Biblioteconomia) – Curso de Biblioteconomia e Gestão de Unidades de Informação, Universidade Federal do Rio de Janeiro.

1. Segurança da Informação. 2. Sistemas de automação. 3. Segurança Lógica. I. Sá, Maria Irene da Fonseca e. II. Miranda, Maria de Fátima Borges Gonçalves de Miranda. III. Título.

CDD: 658.472

Hugo Bauer Rego

A importância da Segurança da Informação para os Sistemas de Automação de Unidades de Informação

Trabalho de conclusão de curso apresentado ao Curso de Biblioteconomia e Gestão de Unidades de Informação (CBG/FACC) da Universidade Federal do Rio de Janeiro como requisito parcial à obtenção do grau de Bacharel em Biblioteconomia.

BANCA EXAMINADORA

Aprovado(a) em:

Prof. Maria Irene da Fonseca e Sá
Mestre em Engenharia de Sistemas e Computação
Orientadora

Prof. Maria de Fátima Borges Gonçalves de Miranda
Mestre em Ciência da Informação
Orientadora de forma

Prof. Ana Maria Ferreira de Carvalho
Mestre em Computação
Professor(a) Convidado(a)

Prof. Maria das Graças Freitas Souza Filho
Mestre em Ciência da Informação
Professor(a) Convidado(a)

Dedico este trabalho aos meus pais Enaldo e Cláudia que sempre me apoiaram e me deram condições de ter uma graduação, à minha companheira Christiene que foi constante apoio nos momentos difíceis, ao meu filho grande filho Leonardo, a toda minha família que foi fonte de apoio durante toda a minha vida e a todos os meus amigos que contribuíram para a minha feliz caminhada até aqui.

AGRADECIMENTOS

Agradeço muito a Deus, pois ele me proporciona muitas alegrias, me guia e abençoa minha vida com mais essa vitória.

A toda a minha família que mora no Rio de Janeiro, principalmente de Campo Grande.

As minhas orientadoras Maria Irene e Fátima por terem prestado grande auxílio.

A todos meus verdadeiros amigos, pelo apoio, carinho e os ótimos momentos de descontração.

A minha turma 2007, por compartilhar comigo quatro anos muita dedicação, preocupação, sufoco, mas principalmente de alegrias. Vou sentir muitas saudades.

E a todos aqueles que de alguma forma contribuíram para o meu sucesso.

RESUMO

REGO, Hugo Bauer. **A importância da Segurança da Informação para os sistemas de automação**. 2011. 28 f. Trabalho de Conclusão de Curso (Graduação) - Curso de Biblioteconomia e Gestão de Unidades de Informação. Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2011.

O presente trabalho aborda a questão da Segurança da Informação como requisito indispensável na escolha de um Sistema de Automação em Unidades de Informação. No estudo é usada a metodologia de levantamento bibliográfico. A sociedade atual se tornou extremamente dependente e direcionada pelo recurso informação, fato que também mudou a forma das organizações lidarem com esse novo insumo estratégico. Esta pesquisa estabelece as principais características da Segurança da Informação que a colocam como requisito indispensável na escolha de um eficiente sistema. São apresentados os princípios e mecanismos que fortalecem o papel da segurança na composição dos sistemas em uma organização. Também é explicitado como a segurança física e a segurança lógica devem convergir para formar um eficiente sistema. Após inferir sobre a importância de se proteger a informação, foi possível indicar quais requisitos tecnológicos são determinantes para a escolha de um sistema de automação seguro para as unidades de informação. Portanto, o reconhecimento da informação como uma mercadoria incalculável já é uma realidade no mundo empresarial. O que as organizações ainda buscam perceber é que como as informações são gerenciadas por sistemas, e os sistemas para serem confiáveis devem ser seguros, a Segurança da Informação se tornou um fator crítico de sucesso.

Palavras-chave: Informação. Segurança da Informação. Sistemas de Automação. Organizações. Unidades de Informação.

SUMÁRIO

1 INTRODUÇÃO

Atualmente, a população global gira em torno do fluxo de informações, podendo também ser caracterizada como uma sociedade da informação propriamente dita. Esse fluxo tem extrema importância, visto que está presente em diversas áreas, como no setor tecnológico, no setor financeiro, nas telecomunicações entre outros.

A demanda por informações relevantes, exatas, atuais, rápidas e facilmente acessíveis, é bastante elevada. Existem algumas questões debatidas como o acesso e o consumo da informação, que foram modificados pelo crescimento da demanda informacional na sociedade moderna. Dessa forma, os consumidores passaram a exigir serviços de informação que os atendam prioritariamente e em tempo hábil.

Nos anos 70, os governos já se empenhavam em busca de soluções que protegessem suas informações, que eram sigilosas e de conteúdos secretos.

> Os EUA, através de seu departamento de defesa, elaboraram um documento que foi o marco "zero" na história da Segurança da informação, o "Orange Book". Este documento serviu de precursor para todas as medidas que buscavam tornar um ambiente computacional seguro (LONGO, 2008).

Contudo, somente com o advento da era digital na sociedade contemporânea é que a questão sobre a segurança da informação teve seus avanços para a área de negócios. A globalização a partir dos anos 90 aumentou exponencialmente as comunicações entre os pólos, formando redes globais entre os países e indivíduos. Esse crescente acesso em tempo real às informações, fez com que a informação se tornasse produto lucrativo, sendo assim altamente disputado pelas instituições.

No atual ambiente empresarial, a informação é encarada como insumo estratégico. Cada vez mais as organizações criam sistemas de informação para que possam extrair toda capacidade produtiva e lucrativa das informações. Tanto é verdade que a gestão do conhecimento, a tomada de decisões, a produção, todos esses processos demandam de informação. Uma vez que a mesma se torna vital para as organizações, ela passa a ter um valor para o negócio, contribuindo diretamente para a geração de lucros. Portanto, pode-se dizer que a informação

nos dias de hoje passou a ser um bem, um patrimônio das empresas, ou então, um ativo das organizações.

Logo, já que a informação se tornou um ativo das empresas, resta a essas organizações protegerem e controlaram seu ativo intangível mais promissor. E para que essa proteção seja eficaz é necessário torná-la prática, através de mecanismos de Segurança da Informação (SI), que consistem em uma série de práticas e controles que buscam controlar os riscos e as incertezas com as informações. Segundo Carvalho (2010) é necessário adotar controles físicos, tecnológicos, humanos etc, que viabilizem a redução e a administração dos riscos, levando a organização a atingir níveis de segurança adequados ao seu negócio.

2 JUSTIFICATIVA

Podemos perceber o avanço tecnológico atual, de forma que a sociedade se baseia em troca de informações a todo tempo, e que exibe uma crescente propensão para coletar e armazenar informações para um uso efetivo (KATZAM, 1977 apud LAUREANO, 2005). Esses recursos advindos da tecnologia da informação necessitam cada vez mais de proteção e controle. As organizações já reconhecem a informação como seu patrimônio ativo, e como qualquer outro ativo importante para os negócios, tem um valor para as empresas, e, por conseguinte, necessita ser adequadamente protegida (NBR 17999, 2003 apud LAUREANO, 2005).

Davenport (2000 apud SILVA, 2009) propõe que é importante uma "ecologia da informação" para o gerenciamento da mesma, ou seja, é necessário criar métodos e aplicações que façam com que a informação seja tratada de modo responsável e seguro. Portanto, é vital identificar a SI como um fator crítico de sucesso essencial para as unidades de informação.

Visto a importância social e econômica do "recurso" (informação), torna-se necessário um controle do acesso, do uso e da produção informacional. Entre outras medidas, as organizações procuram implantar sistemas de automação em unidades de informação, para que assim possam usar a informação de maneira mais eficiente. Para tanto, é preciso uma atenção especial principalmente com a segurança de tais sistemas de informação. Logo, é perceptível que a Segurança da Informação é um assunto vital para tais sistemas. Assim, este trabalho terá o intuito de analisar como a segurança é um mecanismo necessário na implementação de sistemas de automação em unidades de informação.

3 OBJETIVOS

Para elaboração deste Projeto Final, foram definidos os objetivos.

3.1 Objetivo geral

- Destacar a importância da Segurança da Informação nos sistemas de automação de unidades de informação.

3.2 Objetivo específico

- Analisar a importância dos três pilares fundamentais da Segurança da Informação.
- Identificar os requisitos de segurança pertinentes a sistemas de informação, especialmente os de sistemas de automação de unidades de informação.

4 FUNDAMENTAÇÃO TEÓRICA

A seguir serão explicitados os estudos e teorias acerca da Segurança da Informação (SI).

4.1 Segurança da Informação (SI)

Percebendo o cenário de valorização da informação como insumo fundamental para os negócios, os sistemas e seus recursos necessitam cada vez mais de segurança. A informação é um bem crítico para o negócio (FONTES, c2011). E como também é um ativo das organizações, ela precisa ser protegida. E para que haja essa proteção, deve-se incorporar os conceitos e diretrizes de Segurança da Informação (SI) nas empresas e nos seus sistemas.

Por conseguinte, a segurança tem por objetivo facilitar a realização do negócio, de maneira que a organização se sinta protegida e os riscos sejam aceitáveis. Dessa forma, a SI consiste em um "conjunto de orientações, normas e procedimentos que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada" (FONTES, 2006 apud SILVA, 2009).

A segurança é vital para que a informação somente seja acessada e usada pelas pessoas devidamente autorizadas. Em um mundo virtual no qual vivemos hoje, esse controle de níveis de acesso é fundamental.

> A segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação não autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (NBR 17999, 2003; Dias, 2000; Wadlow, 2000; Krause e Tipton, 1999; apud Laureano, 2005).

É evidente que a informação em meio digital – que é aquela manipulada pelas novas tecnologias existentes – mudou completamente a relação de segurança nas organizações. Atualmente as empresas possuem sistemas de informação baseados em redes de computadores para gerenciarem seus negócios. Esses sistemas são baseados nas tecnologias

da informação (hardware, software etc.), que proporcionam novas formas de trabalho e relações entre as organizações, mudando completamente a forma de fazer negócio no mundo. Assim, a SI é a forma de proteção desses sistemas contra ameaças físicas (incêndios, inundação, curto circuito), ameaças tecnológicas (vírus, invasão na web) e ameaças humanas (sabotagem, fraude, erro humano), tornando assim cada unidade de informação prevenida e preparada para lidar com esses possíveis casos de incidentes de segurança.

Portanto, visto que a segurança tem importância fundamental para as organizações e seus sistemas, torna-se necessário conscientizar que até mesmo as unidades de informação mais simples demandam de um controle do acesso, do uso e da produção da informação. Logo, cada vez mais as empresas dão importância a uma eficaz gestão interna das informações. O quesito segurança se tornou uma das bases necessárias para as empresas possam abrir novas oportunidades no mercado. Segundo Ferreira (2003 apud CARVALHO, 2010), a SI tem por objetivo proteger a informação de forma a garantir a continuidade do negócio, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades que surgir.

4.1.1 PILARES DA SI

Como mencionado anteriormente, as organizações ficam cada vez mais dependentes das tecnologias da informação, que por sua vez precisam estar baseadas nas premissas da SI (integridade, confidencialidade e disponibilidade), para que todo o conteúdo informacional que seja produzido, disseminado e tratado nas organizações esteja seguro.

Basicamente, a SI se baseia em três premissas básicas (NBR ISO/IEC 17799, 2000, p. 8):

a) Confidencialidade: Quando somente as pessoas autorizadas, e devidamente permitidas tem acesso à informação. É muito importante para garantir a identificação e a autenticação das partes envolvidas no sistema;

b) Integridade: Uma informação se torna íntegra quando ela não sofre alterações e está completa, se tornando assim confiável. É por este pilar da SI que ocorre a minuciosa

proteção dos dados contra ameaças acidentais ou propositais, realizadas por pessoas autorizadas ou não;

c) Disponibilidade: Ocorre quando a informação e o sistema estão acessíveis e prontos para uso no momento que as pessoas autorizadas forem acessá-las.

Portanto, para que essa informação se torne segura, ela deve estar íntegra, ser confidencial e estar sempre disponível, reafirmando assim os pilares fundamentais da SI.

Esses pilares que norteiam a SI contribuem para salvaguardar as informações, evitando diversos cenários de perdas ou danos, seja em qual fase de tratamento ou uso elas estiverem. Todavia, tradicionalmente as organizações tinham a tendência de dar mais atenção a seus ativos tangíveis, físicos e financeiros em detrimento dos os ativos intangíveis. A partir dos últimos anos, as instituições vêm percebendo o aumento da relação custo-benefício da informação como um bem intangível de alto valor estratégico, tanto para a manutenção dos negócios quanto para a dinâmica do mercado e as transações em tempo real.

Conforme Dias (2000 apud LAUREANO, 2005) é possível afirmar que atualmente a informação é considerada um dos principais patrimônios de uma empresa, o qual está sob constante risco. Contudo, muitos sistemas de informação em empresas não foram projetados para conter ataques e ameaças. A segurança dessas informações deve ser feita com técnicas e procedimentos que fortaleçam e estabeleçam uma gestão adequada das informações.

Neste contexto, a segurança da informação por meio de seus pilares fundamentais, tornou-se área fundamental na sociedade e no mundo empresarial. As organizações se esforçam para tornar suas informações restritas a quem compete saber, ou seja, já fazem uso de um dos pilares da SI, **a confidencialidade**. Outro fator que demonstra a mudança de paradigma nas instituições é que, por exemplo, consumidores comuns procuram cada vez mais empresas que realizem transações via Web, quebrando tabus sobre a segurança dessas atividades. Esses consumidores já confiam nesse tipo de negócio, de maneira que as empresas já passam uma maior confiança em suas atividades e principalmente na responsabilidade que é armazenar os dados dos clientes.

Por isso **a integridade** de uma informação se torna característica predominante de ambientes e de empresas confiáveis. Da mesma forma, se um cliente deseja adquirir um produto ou serviço de uma empresa, e a mesma não disponibiliza em tempo hábil as informações necessárias ao negócio, essa instituição perde credibilidade frente aos consumidores, ou seja, é vital que haja **disponibilidade** (acessibilidade). Assim, uma unidade de informação que preza por sua quantidade habitual de lucros, percebe a relação diretamente proporcional com a segurança (confiabilidade, integridade e disponibilidade) das suas atividades.

4.2 Sistemas de Automação em Unidades de Informação (SAUI)

As organizações, que tratam a informação como fator preponderante no negócio, precisam criar sistemas que padronizem e potencializem esse ativo intangível. Para isso, as instituições precisam adequar suas unidades de informação através da nova estrutura organizacional exigida pela sociedade e economia atual. Os sistemas de automação são compostos por equipamentos que passam desde microcomputadores até softwares específicos. Dessa forma, para criação e uso de todo e qualquer sistema de automação que gerencie a informação, necessita-se do quesito segurança.

Usando como exemplo uma biblioteca de uma organização, podemos analisar como um sistema de automação é importante e, principalmente, como é vital que esse sistema informatizado funcione e esteja seguro. As bibliotecas começaram a se modernizar a partir do começo dos anos 90. O movimento se iniciou pelas bibliotecas de grande porte que passaram a buscar softwares que tornassem os ambientes automatizados. Com essa procura inicial, as empresas responsáveis pelo desenvolvimento dos softwares passaram a expandir a funcionalidade dos programas, percebendo a oportunidade de um novo negócio. Em seguida, os fornecedores (ou seus representantes) passaram, eles próprios, a procurar as bibliotecas para oferecer seus serviços. Com essa expansão, as bibliotecas de pequeno porte também puderam se automatizar e proporcionar a seus usuários um melhor acesso à informação.

Atualmente, com a internet permeando todos os setores da sociedade (Comércio, Cultura, Governos), os centros de documentações e bibliotecas também procuram se inserir na área virtual. As unidades de informação agora desejam criar as “bibliotecas virtuais”. Com mais

essa expansão em vista, as bibliotecas necessitarão de um sistema de automação que possa salvaguardar todos os dados e esteja sempre disponível para uso. Contudo, como alerta Laureano (2005), quando grandes quantidades de informações são armazenadas e manipuladas em meio eletrônico, elas ficam vulneráveis a muito mais tipos de ameaças do que quando estão em formato manual, logo, a SI se insere e interfere nessa opção por sistemas automatizados que alicercem novas formas de bibliotecas.

Rowley afirma:

> A segurança é importante em qualquer ambiente multiusário de base de dados. O primeiro nível de segurança diz respeito a segurança de base de dados. Certas características como a restauração automática após uma pane do sistema, são importantes para manter a integridade da base de dados. O acesso à base de dados é outro aspecto da segurança de dados. Os melhores sistemas proporcionam acesso selecionado, conforme o grupo usuário, a base de dados, documentos, registros ou campos que hajam sido devidamente especificados. Assim, a definição antecipada de tipos e atributos de documentos é um dispositivo importante para determinar as visualizações de documentos que cada usuário tem na base de dados. Alguns usuários terão acesso apenas para leitura, enquanto outros terão permissão para alterar dados. São categorias importantes de usuários as de produtor, consumidor e administrador. [...] As principais medidas de segurança adotadas são as senhas e números de identificação dos usuários. A entrada no sistema com segurança é útil para registrar quaisquer tentativas de violação de segurança. (ROWLEY, 2002, p. 274-275).

Podemos citar como exemplo o software de automação de bibliotecas utilizado pela Universidade Federal do Rio de Janeiro (UFRJ), o Aleph. Este software despertou o desenvolvimento e disponibilização de um OPAC[1]. O programa Aleph trabalha como um sistema integrado de bibliotecas, funcionando para automatização de toda a rede de unidades de informação da UFRJ. Seu papel é gerenciar e armazenar toda a base de dados da universidade (Base Minerva). Logo, medidas de segurança devem existir tanto para com os bibliotecários que usam a base, quanto para os responsáveis pelo suporte ao sistema. Dessa forma, o próprio software Aleph implementa diferentes níveis de acesso para os usuários. Por exemplo, um estagiário de Biblioteconomia possui autorização (login e senha) para acessar o software e trabalhar na catalogação e na circulação dentro do sistema. Contudo, ele não pode fazer modificações em catalogações e em empréstimos que já tenham sido modificados ou gerados por bibliotecários. Isso evidencia os diferentes perfis de acesso que um Sistema de Automação em Unidades de Informação (SAUI) deve possuir para manter a integridade das informações contidas em uma base de dados.

[1] Online Public Access Catalog. É um grande catálogo online.

Partindo desse pressuposto, é importante analisar algumas diretrizes e conceitos acerca de segurança que um sistema deve possuir, permitindo assim uma opção mais adequada para cada unidade de informação. Portanto, a seguir serão explicitados os mais importantes princípios de segurança a serem respeitados na utilização de um sistema de automação para uma biblioteca.

Princípios de Segurança que um sistema deve respeitar (Laureano, 2005):

a) Autenticidade: Visa garantir que a informação ou o usuário da mesma é verdadeiro, ou seja, procura garantir que determinado usuário só possa ter acesso às informações que lhe são determinadas; atesta com acurácia a origem dos dados;

b) Não repúdio: É o princípio que confirma uma operação ou serviço que modificou ou criou uma informação, ou seja, não permite negar uma ação qualquer realizada por determinado usuário. Capacita o sistema a realizar a auditoria;

c) Legalidade: Deve garantir o valor legal (jurídico) da informação, ou seja, a aderência de um sistema à legislação. Este princípio permite o valor legal das transações comerciais, públicas e econômicas que envolvam pessoa física e pessoa jurídica;

d) Privacidade: Busca garantir que a informação seja manipulada apenas pelo seu(s) dono(s), não sendo necessariamente confidencial. É a capacidade do usuário realizar ações em um sistema sem que seja identificado;

e) Auditoria: Este princípio é vital dentro de um sistema que gerencie as informações. Permite a rastreabilidade dos diversos passos que um negócio ou processo realizou ou que uma informação foi submetida, identificando os participantes, os locais e os horários de cada etapa. Auditoria em um software permite um exame do histórico dos eventos de um sistema para determinar quando e onde ocorreu uma violação de segurança;

f) Vulnerabilidade: É onde qualquer sistema pode estar suscetível a ataques e falhas na segurança, seja em seus processos ou em seus recursos. Identificar as vulnerabilidades

é fundamental para prever incidentes de segurança que podem vir a ocorrer no sistema. A auditoria contribui para a percepção e prevenção de futuras invasões no sistema.

4.2.1 SEGURANÇA FÍSICA E SEGURANÇA LÓGICA

Os computadores quando foram inseridos no cotidiano das unidades de informação como ativo tangível, passaram a ampliar as precauções com segurança nas empresas. Não era mais somente a segurança física que trazia preocupação, mas surgia também a prevenção com a segurança em meio eletrônico, ou seja, a segurança com as informações digitais. Desde que os computadores passaram a se comunicar e compartilhar dados via rede (time-sharing), surgiu a necessidade de implantação de mecanismos de segurança lógica das informações usadas eletronicamente.

Dentro de uma política de SI, a segurança física e a segurança lógica são dois meios diferentes para proteger o mesmo produto, a informação. A segurança física corresponde ao uso de ferramentas e equipamentos que permitam uma forma de controle tangível (material) da informação, ou seja: câmeras de vigilância, controle de intrusão, controle de acesso etc. Podemos usar como exemplo um terminal de computador. Se não houver uma segurança física que controle a entrada e a saída de pessoas, pode acontecer de um indivíduo não autorizado tenha acesso a este terminal e manipule uma informação confidencial àquela empresa. A segurança física é primordial, por exemplo, para manter a integridade das informações.

Já a segurança lógica corresponde ao controle e proteção da informação em meio digital (eletrônico), ou seja: criptografia de arquivos, controle de acesso à internet, controle de acesso ao banco de dados, etc. A segurança lógica tem importância direta em manter a confidencialidade e a disponibilidade das informações. Por exemplo, em uma rede interna de uma organização (intranet), é vital o uso de login e senha para funcionários, visto que deve haver uma restrição e controle de uso ao banco de dados da unidade de informação, para que possíveis intrusos ou indivíduos não autorizados (internos ou externos) não tenham acesso ao conteúdo da rede.

Portanto, uma organização que queira ter eficácia na proteção de suas informações, deve buscar convergir esses dois tipos de segurança, a lógica e a física dentro de seu sistema. Não basta somente instalar câmeras de monitoramento e logo após não armazenar estes dados para um futuro acesso do conteúdo. Como também não é suficiente, por exemplo, controlar o acesso externo de pessoas à organização se por vezes os próprios funcionários da empresa podem causar algum incidente de segurança. É necessário unir as duas formas de controle, podendo assim evitar possíveis ataques, ou até mesmo corrigir e detectar outras ameaças.

O autor Zaniquelli (2010) diz que a convergência melhora a eficiência e dificulta possíveis ataques a organização, ao mesmo tempo em que pode ser uma grande ferramenta de auditoria quando há ocorrência de algum incidente. Dessa forma, já existem alguns métodos como uso de cartões de acesso para atividades internas na empresa (acesso a rede interna, acesso remoto seguro, email com assinatura digital, entre outros) e Biometria de acesso (múltiplas credenciais de usuário numa identidade unificada), que funcionam como medidas de segurança para a organização.

Portanto, a seguir explicaremos alguns mecanismos que possibilitam o controle da segurança física e lógica em unidades de informação.

Mecanismos de controle:

1) Autorização e Autenticação: É o mecanismo que controla e fornece permissão para os indivíduos autorizados acessaram os sistemas de informação. É por esse processo que se pode ter a certeza que o usuário remoto realmente é quem está afirmando ser. Através desse mecanismo é definido os perfis e níveis de acesso. São três os mecanismos de autenticação:

    a) *Identificação positiva*: É quando o usuário possui determinadas informações que serão requeridas na hora de se conectar e usar o sistema. Ex: senhas e logins;
    b) *Identificação proprietária*: É o tipo de identificação física, onde o usuário possui um determinado item para realizar a sua autenticação. Ex: cartões de acesso;

c) *Identificação biométrica*: É o tipo de identificação em que o indivíduo possui uma característica única que a diferencia dos outros usuários. Ex: impressão digital.

2) Firewall: É o mecanismo de controle projetado para proteger as fontes de informação de uma organização, controlando o acesso entre a rede interna segura da unidade e as redes externas não confiáveis (como a internet). Um firewall é programado para relatar e evitar a qualquer momento algum tipo de situação ou ameaça ao sistema de informação das empresas. Ele registra os eventos que ocorrem e emite alarmes sobre possíveis incidentes e violações na rede. Existem dois tipos de Firewalls, são eles:

   a) *Filtros de pacotes*: Mecanismo elaborado de acordo com as regras definidas pelo administrador do sistema para filtrar as informações da rede. Ou seja, determinar quais tipos de informações podem ser acessadas por outrem. Este tipo de firewall permite ou não a passagem de datagramas (pacotes) IP[2] em uma rede. Ex: um firewall que determina quais informações podem ser trocadas entre uma rede intranet e a internet;

   b) *Servidores Proxy*: É o firewall que permite executar a conexão ou não a serviços em uma rede de modo indireto. São também muito usados como caches (memória) de conexão para serviços Web. Ex: pode ser utilizado para aceleração de conexão em links lentos.

3) Detector de intrusos (Intrusion Detection System – IDS): Como já diz o nome, é o mecanismo que busca e procura prováveis intrusões indesejadas na rede. A principal fonte de pesquisa de detector de intrusos são as auditorias. O que o IDS faz é tentar reconhecer comportamentos padrões ou ações intrusivas recorrentes. Para isso, se realiza uma constante análise das informações disponíveis e coletadas pelo sistema através da auditoria. O IDS na maioria desses casos alerta o administrador e, se necessário, automaticamente dispara contra-medidas. Ex: usam este mecanismo através de análises estatísticas, inferências, inteligência artificial, data mining, redes neurais etc.

[2] Internet Protocol. Endereço de rede local ou pública.

4) Criptografia: É o mecanismo que permite descrever mensagens codificadas e cifradas. Seu uso é essencial para autenticar a identidade de usuários, proteger as comunicações feitas dentro da rede e manter a integridade durante a transferência e troca de informações. A criptografia permite que haja troca de mensagens privadas, ou seja, somente o emissor e o receptor da mensagem terão acesso ao conteúdo da mensagem. Além disso, ela permite que uma mensagem tenha assinatura digital, podendo assim verificar se o remetente realmente é a pessoa que diz ser e se a mensagem foi modificada. Existem dois mecanismos de criptografia, a simétrica ou de chave privada e assimétrica ou de chave pública:

    a) *Simétrica*: Este tipo de criptografia realizado por algoritmos convencionais, emite uma chave secreta (privada) que é utilizada tanto para cifrar a mensagem quanto para decifrá-la. Dessa forma, é primordial que as duas partes participantes contenham a chave de modo seguro, para que assim seja possível realizar as trocas e transações entre elas;

    b) *Assimétrica*: É a forma de criptografar utilizando uma chave pública. Consiste em uma técnica com a qual a informação criptografada com uma chave poderia ser decifrada por uma segunda chave, que pode não ter relação com a primeira. São utilizados algoritmos assimétricos que utilizam duas chaves diferentes em cada extremidade do processo. Essas duas chaves são geradas de forma que não é possível calcular uma através da outra, possibilitando assim a divulgação de uma das chaves, ou seja, a chave pública. Enquanto isso a chave secreta ou privada não é colocada em risco.

5) Assinatura digital: É o mecanismo que consiste na criação de um código pelo emissor de uma mensagem, por meio de uma chave privada, que permitirá ao remetente identificar através de uma chave pública (do próprio emissor) se o mesmo realmente é quem diz ser. Por exemplo, se um usuário A enviar uma mensagem codificada por sua chave privada a um usuário B. Neste processo, será gerada uma assinatura referente ao usuário A que será adicionada a mensagem. O usuário B ao receber a mensagem irá decodificá-la usando uma chave pública do usuário A. Logo, será gerada então uma

segunda assinatura, que se verificada com a primeira, e se for comprovada que as duas são idênticas, este usuário B terá certeza que a mensagem realmente foi enviada pelo usuário A.

6) Redes Privadas Virtuais (Virtual Private Networks – VPN): São redes compostas por "túneis" de criptografia em pontos autorizados. São criadas usando a própria Internet ou outras redes (públicas ou privadas) para a transferência de informações de maneira segura entre as redes internas corporativas ou usuários remotos. A VPN é uma das formas mais seguras de troca de informações dentro da rede corporativa, visto que os dados são protegidos de forma a não permitir que sejam modificados ou interceptados.

7) Infra-estrutura de Chaves Públicas (ICP): Este mecanismo é super valorizado no meio comercial e empresarial. Ele consiste em uma segurança baseada em tecnologia para estabelecer e garantir a confiabilidade de chaves públicas de criptografia. A grande contribuição do ICP para a segurança dos sistemas de informação é que este mecanismo atrela as chaves públicas as suas entidades, possibilitando que outras entidades verifiquem a validade das chaves públicas, podendo ser feito assim um sistema distribuído. Dessa forma, o mecanismo de ICP protege a distribuição da informação em sistemas altamente ramificados, nos quais as empresas, suas unidades e seus funcionários podem estar localizados em locais diferentes.

4.2.2 REQUISITOS DE SEGURANÇA NA SELEÇÃO DE UM SAUI

"O fato é que não existe um sistema ideal, e mesmo que a escolha seja a mais acertada, poderá não atender completamente aos requisitos funcionais e de performance [...] a custo compatível com o orçamento escolhido" (EPSTEIN apud CÔRTE, 1999, p.2). Na citação acima podemos perceber que não existe um modelo de sistema padrão para todas as unidades de informação e que a seleção do sistema de informação deve merecer atenção e cuidados especiais. Cada instituição deverá avaliar qual o sistema de automação que mais se adequa à sua rotina de trabalho e às suas diferentes necessidades. Para tal, um dos critérios de avaliação para seleção

de um SAUI deverá ser a análise dos requisitos de segurança, existentes no software de automação de unidades de informação.

Rowley alerta:

> É fácil negligenciar a segurança durante a implementação, quando a prioridade está em garantir o funcionamento do sistema. Sua operação permanente depende, porém, da segurança dos componentes. A perda de segurança deve-se a ameaças acidentais ou propositais. As acidentais resultam de características deficientes do sistema, como sobrecarga nas redes ou defeitos de programas. As propositais devem-se a dolo, como furto, fraude, vandalismo e outras tentativas de interromper o funcionamento do sistema. Em geral, essas ameaças causam:
>
> . a interrupção da preparação e entrada de dados
> . a destruição ou corrupção de dados armazenados
> . a destruição ou corrupção de programas
> . a quebra de sigilo de informações pessoais
> . danos ao pessoal
> . retirada de equipamentos ou informações. (ROWLEY, 2002, p. 156).

Já vimos que a SI possui uma série de princípios e mecanismos que são indispensáveis a um sistema de informação, logo, serão mencionados abaixo, alguns requisitos de segurança necessários para a seleção de um SAUI. São eles (CÔRTE, 1999):

Requisitos:

I. **Arquitetura de rede cliente servidor***:* é importante para que a infra-estrutura tecnológica da rede tenha proteção de controle e acesso, mediante dispositivos como monitoramento, filtragem etc.

II. **Auditoria no sistema**: é fundamental para o controle do histórico de eventos ocorridos no sistema, permitindo assim medidas preventivas para possíveis ameaças e incidentes de segurança.

.

III. **Capacidade de atualização dos dados em tempo real**: Permite que o sistema atenda uma das premissas da SI, a disponibilidade, pois o fluxo de troca de informações permanecerá constante.

IV. **Capacidade de suportar acima de 16 (dezesseis) milhões de registros bibliográficos**: Também atende a premissa da disponibilidade, pois um sistema que não permita uma alta na quantidade de tráfego de dados provavelmente corre um grande risco de interrupção do serviço.

V. **Disponibilidade de help online sensível ao conteúdo em língua portuguesa**: Do ponto de vista de segurança o help online facilita a resposta dos administradores mediante os ataques e ameaças ao sistema. Possibilita uma solução mais rápida à incidentes.

VI. **Garantia de manutenção e disponibilização de novas versões**: Resguarda o sistema contra problemas de ordem técnica ou então a possíveis reparos necessários ao funcionamento da rede. Também é vital para a contínua atualização das tecnologias dos SAUI.

VII. **Leitura de código de barras**: È uma forma clara de controlar a segurança física no sistema. O uso de cartões de acesso para usuários, por exemplo, é uma medida de segurança importante. O código de barras também pode ser usado para cadastro e registro de itens no sistema, de forma a permitir agilidade e segurança nos diversos serviços a serem realizados no acervo (especialmente, no processo de circulação).

VIII. **Níveis diferenciados de acesso aos documentos**: Esse requisito é fundamental e indispensável num SAUI. Ele retrata corretamente o que um sistema deve ter como princípio da autenticidade, ou seja, as pessoas autorizadas a usar a rede só devem ter acesso aos documentos à elas pré-determinados. Este requisito também é indispensável para manter uma das principais premissas da SI, a confidencialidade.

IX. **Segurança na forma de registro e de gerenciamento dos dados**: É vital que os registros inseridos e as ações efetuadas no sistema sejam controlados. Dessa forma, é possível manter a integridade das informações e ainda fortalece princípios como o do não repúdio.

X. **Senha para funções que atualizem dados**: É uma das aplicabilidades do requisito de níveis de acesso. É muito importante, pois restringe somente a quem tem permissão e competência fazer algum tipo de manipulação com as informações. É um dos exemplos de autenticidade no sistema, através da "identificação positiva".

Portanto, um SAUI que atenda a estes requisitos de tecnologia e segurança está capacitado para proteger e regular o uso das informações dentro de uma unidade de informação.

5 METODOLOGIA

Primeiramente o estudo será baseado em um levantamento bibliográfico, visto que através deste método é possível identificar, particularizar e fazer as devidas associações ao problema proposto, que é a Segurança da Informação e sua importância para os sistemas de automação de unidades de informação.

Será abordado como as informações passaram de apenas documentos burocráticos, apenas dados, para se tornarem patrimônio ativo das organizações. Posteriormente, visto o novo papel do conteúdo informacional nas instituições, será explicitado porque as empresas necessitam reconhecer a importância de segurança nas unidades de informação, visto que os pilares da SI reforçam o novo paradigma de que transações e trocas de informações em ambientes virtuais se tornou uma atividade segura.

Também será visto porque é importante as organizações conhecerem os riscos que existem contra o seu principal insumo, a informação, de forma que identificadas as suas vulnerabilidades e prováveis ameaças, se possa estimar algum impacto em potencial.

> "A necessidade de segurança é um fato transcendendo o limite da produtividade e da funcionalidade. Enquanto a velocidade e a eficiência em todos os processos do negócio significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios." (CARUSO; STEFFEN, 1999, apud SILVA, 2009).

Portanto, será realizada pesquisa bibliográfica, de maneira que seja possível constatar a aplicação da SI em sistemas de automação de unidades de informação. Serão confrontados estudos que apresentem princípios e mecanismos vitais para a segurança do sistema, de modo que essas características da SI possibilitem estabelecer quais os melhores requisitos para escolha de um sistema de automação.

6 CONSIDERAÇÕES

Na sociedade moderna, só sobreviverão as organizações que tomarem as medidas corretas e necessárias em relação à segurança de suas informações, tornando assim a SI um fator crítico de sucesso para os negócios. Nesse novo século onde todas as atividades e serviços convergem para o mundo virtual, a incessante troca de informações em tempo real é a expertise maior que vivemos em um novo tipo de sociedade.

Ao longo do projeto foi possível apontar quais diretrizes e princípios sobre segurança são essenciais em um sistema de automação. Entre os mais importantes princípios pode-se citar: o da autenticidade, da legalidade, e do não repúdio que se tornaram imprescindíveis no cotidiano do gerenciamento de um sistema de automação de unidades de informação.

É fato que durante a implementação do sistema de automação de unidades de informação, a preocupação se concentra no funcionamento do sistema, mas é fundamental que o projeto de automação contemple uma política de segurança que:

> . identifique os riscos aos quais o sistema se acha exposto
>
> . avalie a probabilidade de qualquer ameaça vir a ser concretizada e as possíveis conseqüências de qualquer ameaça
>
> . selecione as contramedidas que possam fazer face a ameaças com base na eficácia, custo e exigências de segurança
>
> . defina as medidas de emergência para lidar com situações em que a perda de segurança seja inevitável. (Rowley, 2002, p. 156).

Uma vez que encarar a informação como um patrimônio da entidade é um requisito fundamental no atual universo empresarial, é indispensável que as organizações procurem priorizar os recursos em estratégias que potencializem seu principal insumo. Consequentemente a Segurança da Informação já não pode ser postergada na escolha dessas estratégias. Todo o aparato de proteção de um sistema em uma empresa perpassa por soluções e mecanismos que correspondem a SI. Não se encontra mais sucesso nos negócios se as instituições não estiverem um ambiente interno seguro, o que só ocorre por meio das soluções de segurança.

Se as organizações e suas unidades buscam se automatizar, elas necessariamente devem inserir em seus processos de trabalho os mecanismos de segurança. A criptografia, a assinatura digital, o ICP são exemplos de diretrizes vitais em qualquer sistema de automação utilizado, posto que as unidades de informação administram uma quantidade muito grande de informações, sejam elas confidenciais ou não.

Para manter um bom sistema de automação é preciso ter estabelecido determinadas normas de segurança, seja na parte física ou na parte lógica. Portanto, medidas como controle de intrusão, controle de acesso a banco de dados, biometria, Firewalls, criptografia entre outros, são fundamentais para proteger o sistema e seus bancos de dados.

Segundo Fontes (c2011), o processo de Segurança da Informação é um ativo que por vezes se tornou difícil de mensurar do ponto de vista financeiro. Ou seja, o intangível só se torna visível para aqueles que o entendem como essencial para a continuidade da organização. Portanto, a SI sendo indispensável para um sistema de automação se torna também vital para as empresas, logo, para o negócio. Mas o verdadeiro empreendedor, aquele que pensa na sustentabilidade do seu negócio ao longo dos anos, entende o valor da proteção da sua informação (FONTES, c2011).

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da Informação – Código de Prática para Gestão da segurança de Informações:** NBR ISO/IEC 17799:2000. Rio de Janeiro, 2001.

CARVALHO, Ana. **Segurança da informação.** Rio de Janeiro: Ufrj, 2010. 31 p. Aula 2.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet**. São Paulo: Cgi.br, 2006. 95 p.

CONSTANTE, Rosiane. Resultados obtidos com a aplicação da norma nbr iso/iec 17799:2000 no centro universitário de brusque. **Revista da Unifebe**, Brusque, n. 8, 2010. Semestral. Disponível em: <http://www.unifebe.edu.br/revistadaunifebe/2010/artigo015.pdf>. Acesso em: 18 jul. 2011.

CÔRTE, Adelaide Ramos e; ALMEIDA, Iêda Muniz de; PELLEGRINI, Ana Emília. Automação de bibliotecas e centros de documentação: o processo de avaliação e seleção de softwares. **Ciência da Informação**, Brasília, v. 28, n. 3, p.241-256, set./dez. 1999.

DICWEB. Dicionário de informática. Disponível em: <http://www.dicweb.com/cc.htm>. Acesso em: 19 jul. 2010.

FONTES, Edison. **Clicando com segurança:** tratando as questões atuais da proteção da informação na organização e na família. Rio de Janeiro: Brasport, 2011. 257 p.

MARCIANO, José Luiz Pereira. **Segurança da Informação:** uma abordagem social. 2006. 212 f. Tese (Doutorado em Ciência da Informaçã) - CID-FACE, UNB, Brasília, 2006.

LAUREANO, Marcos Aurelio Pchek. **Gestão de segurança da informação.** Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 02 jul. 2010.

LONGO, Gustavo Dobkowski. **Segurança da Informação**. Universidade Estadual Paulista. Faculdade de Ciências Campus de Bauru. Disponível em: <http://www.firewalls.com.br/files/ArtigoCientifico.pdf. Acesso em: 02 de ago. de 2010.

ROWLEY, Jennifer. **A biblioteca eletrônica**. Tradução de Antonio Agenor Briquet de Lemos. Brasília: Briquet de Lemos, 2002.

SILVA, Claudete Aurora da. **Gestão da Segurança da Informação:** um olhar a partir da ciência da Informação. 2009. 99 f. Dissertação (Mestrado em Ciência da Informação) - Puc, Campinas, 2009.

ZANIQUELLI, Tiago. **Convergência Segurança Física e Lógica.** DevMedia. Disponível em: <http://www.devmedia.com.br/post-15760-Convergencia-Seguranca-Fisica-e-Logica.html>. Acesso em: 26 out. 2011.