RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES DE SAÚDE

INFORMATION SECURITY POLICY IN HEALTH ORGANIZATIONS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES DE SALUD

Jefferson Wanderson Pereira de Sena[1], Petrus Fabiano Araújo de Oliveira[2]

e27149
https://doi.org/10.53612/recisatec.v2i7.149

PUBLICADO: 07/2022

RESUMO
A utilização da Gestão e Segurança da Tecnologia da Informação como recurso para uma melhor gestão e segurança da informação nas organizações é o objeto da presente pesquisa, que tem por finalidade demonstrar aos gestores de tecnologia da informação, através de um estudo de caso em uma empresa, alguns temas de suma importância que busca favorecer o entendimento da segurança da informação, e também a conscientização da seriedade que se deve dar a ela nos dias atuais, para poder gerir as informações de maneira eficiente e eficaz.

PALAVRAS-CHAVES: Gestão da Tecnologia da Informação. Políticas e Normas da Segurança da Informação. Análise de Risco

ABSTRACT
The use of the Management and Security of the Technology of the Information as resource for one more good management and security of the information in the organizations, is the object of the present research, that has for purpose to demonstrate to the managers of technology of the information, through a study of case in a company, some subjects of utmost importance that it searchs to favor the agreement of the security of the information, and also the awareness of the seriousness that if it in the current days must give, for power to manage the information in efficient and efficient way.

KEYWORDS: *Management of the Technology of the Information. Politics and Norms of the Security of the Information. Analysis of Risk*

RESUMEN
El uso de la Gestión y Seguridad de las Tecnologías de la Información como recurso para una mejor gestión y seguridad de la información en las organizaciones es objeto de esta investigación, la cual tiene como objetivo demostrar a los gerentes de tecnologías de la información, a través de un estudio de caso en una empresa, algunos temas de suma importancia que buscan favorecer la comprensión de la seguridad de la información, así como la conciencia de la seriedad que se le debe dar en la actualidad, para poder gestionar la información de manera eficiente y eficaz.

PALABRAS CLAVE: *Gestión de Tecnologías de la Información. Políticas y Normas de Seguridad de la Información. Análisis de Riesgos*

[1] Mestre em Educação, Bacharel em Administração e em Sistemas de Informação. Linha de Pesquisa: Gestão Estratégica de Projetos e Metodologias Ágeis, com ênfase em Sistemas de Informação, Gestão do Conhecimento e Ciência de Dados. Professor da Universidade Estácio de Sá, Consultor Empresarial e Servidor Público do Estado do Pará.
[2] Professor da Universidade Estácio de Sá, Contador e Mestre em Administração. Linha de Pesquisa: Gestão Estratégica Contábil e Fiscal.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

1. INTRODUÇÃO

Cada século é acompanhado por alguma revolução tecnológica e por mudanças na sociedade, as quais passaram a acontecer de forma mais acelerada depois da Revolução Industrial no século XVIII, mesmo que apenas na Inglaterra de início, pela mecanização dos trabalhos artesanais, visando à larga produção de bens. Segundo Silva Filho[1] (2001) “o século XIX foi marcado pela expansão da Revolução Industrial e pela diminuição da distância entre os países, graças ao desenvolvimento de barcos a vapor, telégrafos, locomotivas etc.” No século XX, denominado por Eric Hobsbawm como a era dos extremos, em que as diferenças sociais se intensificaram, também cresceu o fenômeno da globalização, cultivado desde a época das grandes navegações, mas que no século XX tomou proporções mundiais. A globalização trouxe uma gama de transformações e mudanças, principalmente nos campos da ciência, da tecnologia e da informática, que passaram a ser incluídas em todos os ambientes organizacionais, inclusive na área de saúde.

Os avanços tecnológicos que tiveram início no século XX possibilitaram o surgimento da era da informação. Nessa era, segundo Santos (2006), “o homem se vê em um mundo globalizado e inconstante, onde se intensificam os relacionamentos entre os povos a nível social, político, cultural e principalmente econômico, o que facilita o intercâmbio entre eles.” Dentro desse contexto globalizado, as organizações devem saber administrar essas mudanças se desejarem permanecer no mercado. Elas devem diversificar suas estratégias, mas sempre visando aumentar a qualidade da produção de seus bens e serviços. Precisam se acostumar a lidar com um volume maior de informações e devem dispor dessas informações da melhor maneira possível para facilitar a criação do conhecimento a partir de dados comuns.

Toda essa tecnologia facilita a execução das tarefas, das estratégias e reforçam a competitividade da empresa (hospitais, laboratórios etc.). Vários são os motivos para isso, entre eles, os sistemas computadorizados que permitem maior controle da informação. Com essas transformações, a tecnologia torna-se uma das principais ferramentas de trabalho, e a má utilização desta ferramenta pode causar danos incalculáveis para a organização.

Nesta nova era, os computadores deixaram de servir apenas para processarem eficientemente dados e automatizar funções repetitivas e tornaram-se, de um mal necessário, a componentes imprescindíveis para o sucesso das organizações, inserindo-as na realidade atual de maneira mais ágil e competitiva. “Entretanto, esse crescimento da importância da informática, além de aumentar o número de pessoas com acesso aos computadores, dificultou seu gerenciamento, visto que a quantidade de informações que precisam ser processadas aumentou consideravelmente nos últimos anos” (SILVA FILHO, 2001). Os ambientes computacionais se tornaram heterogêneos e outras preocupações surgiram para os gerentes, como o combate a vírus, ameaças, vulnerabilidade, política de segurança etc.

[1] SILVA FILHO, Antônio Mendes da. Autor do livro A ERA DA INFORMAÇÃO.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

Em algumas organizações, os objetivos relacionados à gestão e segurança da informação geralmente não são claramente definidos, com isso, elas têm dificuldade em determinar metas, onde almejam chegar e quais caminhos devem percorrer para que possam atingir seus objetivos, dificultando a escolha de ferramentas adequadas e direcionamento para a otimização dos recursos em busca de diferencial competitivo. Essa indefinição de propósitos gerou a necessidade de uma gestão e segurança da tecnologia da informação (TI) nas organizações.

Esta carência nas organizações é gerada, principalmente, pela não conscientização da importância da informação em uma empresa e pelo desconhecimento de uma política e normas de segurança da tecnologia da informação. Cada vez mais empresas vêm adotando diversas formas de gerir suas informações com segurança, tornando-se assim, mais eficientes e eficazes, conseguindo com isso se organizar e se preparar para as mudanças que ocorrem a cada dia no mercado globalizado e competitivo.

O propósito deste artigo é sensibilizar a importância, Política de Segurança da Informação em qualquer organização, principalmente na área de saúde, por ser algo bem deligado quando falamos de dados de pacientes. Demonstraremos as principais atitudes que um gestor da tecnologia da informação deve ter para que a informação seja tratada de forma segura, além de falar dos métodos de segurança, como: níveis de segurança, segurança física, lógica, criptografia e etc. para posteriormente planejar, organizar e gerir esse planejamento, com intuito da implementação em uma empresa da área de saúde, tais como: hospitais, laboratórios, clínicas etc.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Com o desenvolvimento tecnológico e a globalização, foi transformado o método da segurança, como as grandes organizações tratam suas Informações, ou seja, um de seus patrimônios de maior valor. Em geral, o que se define de Segurança como um estado no qual estamos livres de perigos e incertezas, dentro da organização, esta segurança costuma aplicar a tudo aquilo que possui valor e consequentemente, demanda proteção, e são chamados de Ativos.

Com o advento da Internet no campo tecnológico e da globalização no campo socioeconômico transformando totalmente o mundo, essas transformações afetaram bastante as organizações, quebrando paradigmas e promovendo uma profunda reavaliação das prioridades daqueles que estão à frente das organizações.

Diariamente há notícias nas quais a palavra segurança está inserida. Tanto de conflito de guerra a fraudes bancárias, passando por crimes e desastres, a segurança assim tem obtido cada vez mais destaque, por oferecer abordagens práticas, viáveis no ponto de vista financeiro, e alinhadas com a estratégia das organizações.

Em geral, define-se que segurança significa estar livre de perigos e incertezas, já em Segurança da Informação define-se como sendo aquela que busca a proteção dos ativos de informação contra ameaças, buscando a diminuição das ocorrências, dos impactos e, consequentemente, dos riscos.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

Dentro de uma organização, esta segurança costuma se aplicar a tudo aquilo que possui valor e, consequentemente, demanda proteção. São os chamados ativos. Existem diversos tipos de ativos, que podem ser classificados em diversas propriedades. Tais propriedades muitas vezes classificam os ativos em grupos com características semelhantes no que se refere às necessidades, estratégicas e ferramentas de proteção.

Atualmente o conceito é padronizado pela norma ISO/IEC 17799:2005, influenciado pelo padrão inglês (*British Standard*) BS 17799. A série de normas ISO/IEC 27000 foi reservada para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos.

Categorias de ativos	**Exemplo**
Tangíveis	Informações impressas ou digitais Impressoras Móveis de escritório
Intangíveis	Imagem de uma empresa Confiabilidade de um órgão federal Marca de um produto
Lógicos	Dados armazenados em um servidor Sistema de ERP Rede de VoIP
Físicos	Estação de trabalho Sistema de ar-condicionado Fábrica
Humanos	Empregados Prestadores de serviço

Tabela 1 – Exemplo de classificação dos ativos

Do mesmo modo que os ativos possuem características específicas, devem-se utilizar abordagens especializadas para atender às demandas de segurança. Dá-se o nome de Proteção à medida que visam livrar os ativos de situações que possam trazer prejuízo.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

Tipo de Proteção	Exemplo
Lógica	Permissões em sistemas de arquivos *Firewalls*[2] Perfis de usuários em aplicações
Física	Portas Fechadura Guardas
Administrativa	Políticas Normas Procedimentos

Tabela 2 – Classificação das proteções

De acordo com a ação e o momento no qual ocorrem, pode-se classificar as proteções em diversos outros grupos. Uma eficaz implementação de segurança se baseia na utilização de tipos diferentes de proteções, variando bastante sua ação. Desta forma, as proteções completam-se, sobrepõem-se e fornecem redundância entre si, caso alguma delas falhe, ou seja, violada.

Tipo de proteção	Descrição
Preventiva	Evita que incidentes ocorram
Desencorajadora	Desencoraja a prática de ações
Limitadora	Diminui danos causados
Monitoradora	Monitora estado e funcionamento
Detectora	Detecta a ocorrência de incidentes
Reativa	Reage a determinados incidentes
Corretiva	Repara falhas existentes
Recuperadora	Repara danos causados por incidentes

Tabela 3– Tipos de proteções

Há diferença entre Segurança e Segurança da Informação (SI). Basicamente, em SI se lida com um tipo específico de ativo que chamamos de ativo de informação, isto é, ativos que geram, processam, manipulam, transmitem e armazenam informações, além das informações em si.

Muitas vezes, os ativos que fazem parte do escopo da SI são avaliados equivocadamente como sendo os ativos de Tecnologia da Informação (TI). A TI envolve basicamente o uso de *hardware* e *software* para processar informações em sistemas de forma autorizadas. Apesar do papel primordial desses ativos nas atividades de tratamento de informações, visualizar como um único

[2] *Firewalls* – São dispositivos de controle de acesso em redes de computadores.

universo onde as proteções devem ser implementadas leva a uma concepção extremamente limitada à falha. As informações das organizações são faladas em conversas telefônicas, impressas em relatórios e repassadas a terceiros. Isto mostra um campo de atuação muito mais amplo, e com uma série de particularidades.

2.1 ASPECTOS E PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

De forma simplificada a Segurança busca a proteção contra situações nas quais os prejuízos são causados por conta de danos diretos aos ativos ou por situações prejudiciais inesperadas. Especificamente no caso de SI, quando se observam os ativos de informação para que tais situações não ocorram, são definidos basicamente em três, ou seja, são chamados de pirâmide ou tríade da Segurança da Informação:

a) Confidencialidade.

b) Integridade.

c) Disponibilidade.

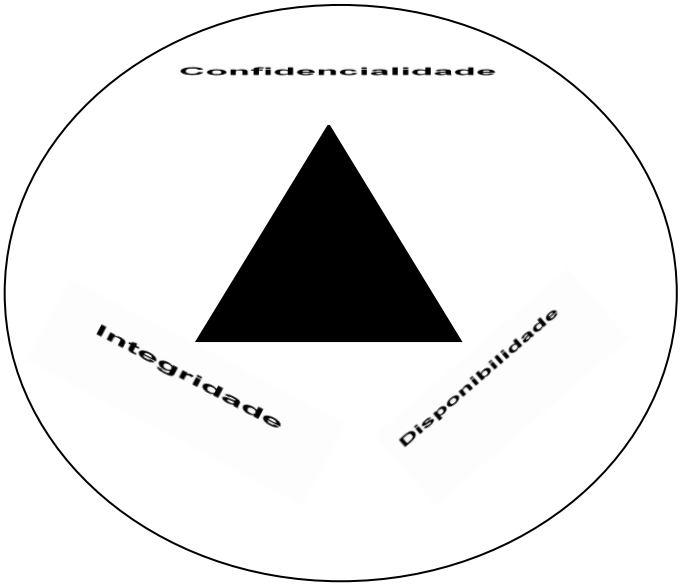

Diagrama 1 – Pirâmide ou tríade de Segurança da Informação[3]

a) Confidencialidade

Quando se refere a Confidencialidade estamos, basicamente, falando em sigilo. Preservar a informação significa garantir que apenas algumas pessoas, as quais deverão ter conhecimento a seu respeito, poderão acessá-la. cada tipo de informação deverá ter diferentes necessidades em termos de confidencialidade.

b) Integridade

[3] Formada pelos aspectos de confidencialidade, integridade e disponibilidade.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

A preservação da integridade envolve proteger as informações contra alterações em seu estado original. Essas alterações podem ser tanto intencionais quanto acidentais.

c) Disponibilidade

Uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento que precisam. Podem ter situações acidentais ou intencionais que comprometem este aspecto.

2.2 ELABORAÇÃO, ESTRUTURAÇÃO E IMPLEMENTAÇÃO NO DESENVOLVIMENTO DA POLÍTICA

A Política da Segurança da Informação possui requisitos básicos para sua melhor elaboração, estruturação e desenvolvimento, principalmente nos profissionais envolvidos no desenvolvimento da política até o usuário final bem treinado. É importante que o trabalho seja analisado de forma realista e os recursos disponíveis.

A elaboração da Política é composta de uma série de documentos, sendo que cada um deles tem características particulares que variam de acordo com o nível de detalhes e a audiência para a qual foi criado.

À medida que desenvolve as políticas, a recomendação de controles desponta como um de seus principais propósitos. Muitos controles têm como um ganho inquestionável em relação ao seu custo de adoção.

Normalmente o principal profissional responsável pelo desenvolvimento das políticas é o gestor de segurança e seu departamento. Caso a organização não possua este profissional, a responsabilidade fica a cargo de quem tiver duas áreas. O Comitê Executivo de Segurança da Informação é responsável por se considerarem importantes e fundamentais para o negócio da organização. Em locais onde não existe este comitê este deve ser desempenhado por gestores das principais áreas de negócios ou, ainda, em empresas de menor porte, pelo diretor geral a organização. Já para os documentos da política que possuem um detalhamento mais técnico, faz-se necessário o envolvimento de profissionais de tecnologia, que serão os responsáveis pela implementação de grande parte dos controles e, por isso, terão a responsabilidade de detalhá-lo.

Outras áreas podem participar, acrescentando informações e preocupações importantes. Estas áreas também ajudam a padronizar a iniciativa da política de acordo com a cultura da empresa e trazem informações importantes sobre o impacto das medidas no dia a dia.

A estruturação da política tem como foco principal a documentação, dividida em categorias como:

a) Diretrizes

São as regras de alto nível que representam os princípios básicos que a organização resolve incorporar à sua gestão de acordo com a visão estratégica da alta direção. Servem como base para

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

que as normas e os procedimentos sejam criados e detalhados da maneira como as áreas responsáveis (Segurança e Tecnologia) acharem mais adequada e eficaz.

b) Normas

Especificam no plano tático, por assim dizer, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégica definida nas diretrizes.

c) Instruções e Procedimentos

As instruções detalham, no plano operacional, as configurações de um determinado produto ou funcionalidade que devem ser feitas para implementar os controles e tecnologias estabelecidas nas normas. Já os procedimentos detalham atividades passo a passo, que normalmente envolvem a interação entre áreas e/ou pessoas.

2.2.1 NÍVEL DE SEGURANÇA

Depois de identificado o potencial de ataque, as organizações têm que decidir o nível de segurança a estabelecer para uma rede ou sistema os recursos físicos e lógicos a necessitar de proteção. No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de proteção para minimizar a probabilidade de ocorrência de um ataque.

2.2.2 SEGURANÇA LÓGICA

O controle de acesso, físico ou lógico, tem como objetivo proteger os recursos computacionais (equipamentos, softwares, aplicativos e arquivos de dados) contra perdas, danos, modificação ou divulgação não autorizada. Os sistemas computacionais, bem diferentes de outros tipos de recursos de uma organização, não podem ser facilmente controlados apenas com dispositivos físicos, como cadeado, alarmes, guarda de segurança etc. Ainda que os computadores estiverem conectados a redes locais ou de maior abrangência, é preciso controlar a acesso a esses recursos por meio de medidas preventivas e procedimentos adequados a cada tipo de ambiente computacional.

O Acesso Lógico nada mais é do que o sujeito ativo deseja acessar o sujeito passivo, sendo que este sujeito nada mais é que um usuário ou um processo, e o objeto pode ser um arquivo ou outro recurso como memória ou impressora. Os controles de acesso lógico são conjuntos de medidas e procedimentos, adotados pela organização ou intrínsecos aos *softwares* utilizados, cujo objetivo é proteger os dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por usuários ou outros programas.

3. PROCESSO DE LOGON E IDENTIFICAÇÃO DO USUÁRIO

É usado para obter acesso aos dados e aplicativos em um sistema informatizado. Normalmente esse processo envolve a entrada de um User ID (identificação de usuário) e uma senha

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

(autenticação de usuário). A identificação define para o computador quem é o usuário e senha é um autenticador, isto é, ela prova ao computador que o usuário é realmente quem ele diz ser.

Alguns controles lógicos já se encontram incorporados à maioria dos processos de logon dos sistemas operacionais disponíveis no mercado ou são recomendados pelos fornecedores de *software*. Porém, é possível que não constem da configuração default (padrão).

Para dificultar a tarefa de um invasor, recomenda-se limitar o número de tentativas incorretas de acesso (logon), bloqueando a conta do usuário ao alcançar o número limite.

Para que o usuário possa auxiliar no controle de acesso a sua própria conta, pode-se apresentar após o logon ter sido realizado com sucesso, data e hora do último logon e detalhes sobre tentativas frustradas. Dessa forma, o usuário pode identificar tentativas de uso não autorizado de sua conta e reportar o ocorrido à gerência de segurança (*Segcurity Office*).

A identificação do usuário, ou User ID, deve ser única, isto é, cada usuário deve ter uma identificação própria. Todos os usuários autorizados devem possuir um código de usuários, quer seja um código de caracteres, cartão inteligente ou outro meio de identificação. Essa unicidade de identificação permite um controle das ações praticadas pelos usuários por meio do log´s de acesso e atividades dos sistemas operacionais e aplicativos.

Após identificar-se ocorre a autenticação, ou seja, o sistema confirma se o usuário é ele mesmo. Os sistemas de autenticação são combinações de *hardware, software* e procedimentos que permitem o acesso de usuários aos recursos computacionais. Na autenticação o usuário apresenta algo que ele sabe ou possui tipo características físicas (formato da mão, da retina ou do rosto), cartões inteligentes (algo que somente o usuário possui).

As **Senhas de Acesso**, para que este método de acesso funcione é necessário que o usuário tenha conhecimento de política de composição e guarda de senha da organização a serem orientadas e seguidas. A recomendação que gestores em TI devem dar para os usuários de sistemas institucionais, é que devem ser escolhidas senhas seguras, evitando senhas muito curtas ou longas, não utilizar mesma senha em sistemas distintos, que é uma prática comum, mas, no entanto, muito vulnerável, quando um invasor descobre pela primeira vez, sua atitude é testar em vários sistemas, há sistemas que obrigam o usuário a utilizar senhas complexas.

O sistema de controle de senhas deve ser configurado para proteger senhas armazenadas contra o uso não autorizado, não apresentando na tela do computador, mantendo-se em arquivos criptografados e estipulando datas de expiração (recomenda-se a troca de senhas após 60 ou 90 dias), para evitar o uso constante das mesmas senhas o sistema de controle de senha deve conter um histórico das últimas senhas utilizadas por cada usuário, ressaltando que não é recomendada a troca frequente de senha podendo confundir o usuário. Alguns sistemas, além de criptografar senhas, guardam essas informações em arquivos escondidos que não podem ser visualizados, dificultando a ação dos *hackers*.

O gerente de TI deve desabilitar contas inativas, sem senhas ou com senhas padronizadas, esta deverá ser gerada de forma que já entre expirada no sistema, exigindo sempre uma nova senha

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

para os próximos logons. É aconselhável que haja um procedimento que force a troca de senha que será utilizada dali por diante. Deve também ser bloqueada contas de usuários após um determinado número de tentativas de acesso sem sucesso. Procedimento esse que diminui os riscos de alguém tentar adivinhar as senhas. Atingindo esse limite, só o administrador do sistema pode desbloquear a conta do usuário.

Tokens são objetos que o usuário possui que o diferencia das outras pessoas e o habilita a acessar algum objeto. A desvantagem é em relação as senhas por serem objetos, podem ser perdidas, roubadas ou reproduzidas com maior facilidade. Para dificultar a clonagem de cartões magnéticos é incorporado hologramas em sua confecção, como um dispositivo a mais de segurança.

Sistemas Biométricos – Com o passar dos anos foram desenvolvidas pesquisas na área de sistemas automáticos de verificação de identidade baseados em características físicas do usuário, tendo como principal objetivo suprir deficiências de segurança das senhas, que podem ser reveladas ou descobertas, e das tokens, que podem ser perdidas ou roubadas. Acredita-se que este tipo de sistema soa mais difícil de serem forjados, pois são muito mais caros.

Os sistemas biométricos automáticos são as evoluções naturais dos sistemas manuais de reconhecimento amplamente difundido há muito tempo, como a análise grafológica de assinaturas, as análises de impressão digitam e o reconhecimento de voz, e há os sistemas de análise da conformação dos vasos sanguíneos da retina, teoricamente qualquer.

As características de uma pessoa podem ser usadas como base para sua identificação biométrica. Na tecnologia deve haver medida em que as características do indivíduo sejam realmente únicas.

A desvantagem deste tipo de sistema é a grande margem de erro, em função das mudanças das características das pessoas com o passar dos anos. A tolerância a erros deve ser estabelecida com precisão, de forma a não ser grande o suficiente para admitir intrusos, nem pequena ao ponto de negar acesso aos usuários legítimos.

Principais características dos sistemas biométricos:

a) Impressão digital: São características únicas e consistentes. Nos sistemas biométricos que utilizam essa opção são armazenadas de 40 a 60 pontos para verificar uma identidade. O sistema compara a impressão lida com sua base de dados de impressões digitais de pessoas autorizadas;

b) Voz: São usados para controle de acesso, porém não sejam tão confiáveis, em função dos erros causados por ruídos no ambiente e problemas na garganta ou cordas vocais das pessoas;

c) Geometria da mão: Usada em sistemas de controle de acesso, porém essa característica pode ser alterada por aumento ou diminuição do peso ou artrite;

d) Análise da Íris e da retina: Os sistemas que utilizam essas características se propõem a efetuar identificação mais confiável de que as impressões digitais;

e) Reconhecimento facial por meio de um termograma: É uma imagem tirada com câmera infravermelha que mostra os padrões técnicos de uma face. Essa imagem é única, combinada com

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

algoritmos sofisticados de comparação de diferentes níveis de temperatura distribuídos pela face, constitui-se de técnicas não evasiva, altamente confiável, não sendo afetada por problemas de saúde, idade ou temperatura do corpo. São armazenados ao todo 19.000 pontos de identificação, podendo distinguir gêmeos idênticos, mesmo no escuro. Estão desenvolvendo pesquisar par baixar o custo dessa tecnologia para que possa ser usada por muitas aplicações de identificação e autenticação.

4. PROTEÇÃO DOS RECURSOS E DIREITOS E PERMISSÕES DE ACESSO

Quando um usuário está identificado e autenticado não quer dizer que poderá acessar qualquer informação ou aplicativo sem qualquer restrição. Há necessidade de programar um controle específico restringindo o acesso dos usuários apenas às aplicações, arquivos e utilizados imprescindíveis para desempenhar suas funções na organização, este controle pode ser feito no nível de menus, funções ou arquivos.

Os controles de menus podem ser feitos para subdividir os usuários em categorias, restringindo seu acesso apenas àqueles aplicativos ou utilitários indispensáveis.

No que diz respeito às funções internas dos aplicativos, os respectivos proprietários deverão definir quem poderá acessá-la e como através de autorização para uso de funções específicas ou restrição de acesso à funções de acordo com o usuário (menus de acesso predefinidos), horário ou tipo de recursos (impressoras, fitas de *backup* etc.).

Em se tratando de proteção e arquivos, a maioria dos sistemas operacionais possui mecanismo de controle de acesso em que são definidas as permissões e os privilégio de acesso para cada recurso de sistemas.

Os direitos de acesso podem ser definidos individualmente para cada sujeito e objeto, embora seja a maneira mais trabalhosa envolvendo grandes quantidades de sujeitos e objetos, a forma mais comum de definição de acesso é a matriz de controle de acesso. Para evitar a definição de uma matriz muito extensa, normalmente se associa o direito de acesso internamente ao sujeito ou ao objeto.

5. MONITORAMENTO E ARMAZENAMENTO

O monitoramento dos sistemas por meio de registros de log, trilhas de auditoria ou mecanismo de detecção de invasão são essenciais à segurança, pois é impossível eliminar por completo todos os riscos de invasão pela identificação e autenticação de usuários. Quando há ocorrência de invasão, erro ou atividade não autorizada, não há impossibilidade reunir evidências suficientes para que possam ser tomadas as medidas administrativas e/ou judiciais para investigar e punir os invasores. O método mais simples e mais difundido de monitoramento é a coleta de informações a respeito de eventos predeterminantes em arquivos históricos, mais conhecidos como logs. Os logs funcionam como trilha de auditoria, ou seja, são registros cronológicos de atividades do sistema suficiente para possibilitar a reconstrução, revisão e análise dos ambientes e atividades

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

relativas a uma operação, procedimento ou evento, desde seu início até seus resultados finais, são medidas utilizadas para detecção e monitoramento usadas para registrar atividades, falhas de acesso (tentativa frustrada de logon ou de acesso a recursos protegidos) ou uso do sistema operacional, utilitário e aplicativos, detalhando o que foi acessado, por quem e quando. Com dados do log, pode-se identificar e corrigir as falhas da estratégia de segurança, por conterem informações essenciais para a detecção de acesso não autorizado, os arquivos de log devem ser protegidos contra destruição ou alteração por usuários ou invasores tentando encobrir suas atividades.

É importante considerar que o uso de logs ou trilhas de auditoria podem degradar o desempenho dos sistemas, sendo aconselhável balancearem a necessidade de registro de atividades críticas e os custos em termos de desempenho global dos sistemas. Ao definir o que será registrado, é preciso levar em conta que quantidades enormes de registros podem ser inviáveis de serem monitoradas. Nada adianta ter um log se este não é periodicamente revisado.

Os logs são tradicionalmente armazenados nos discos rígidos, no próprio sistema onde são gerados. Essa é a opção mais comum, mas possui alguns riscos inerentes que devem ser compreendidos.

O log não pode ser mantido *on-line* por tempo indeterminado, pois ocupam muito espaço em disco. A melhor estratégia para resolver esta questão é transferi-los periodicamente, do disco para dispositivos de armazenamento ***off-line***[4], por exemplo, fitas, CD-R ou CD-RW.

6. RISCOS INERENTES A CONTROLES DE ACESSO LÓGICO INADEQUADOS

Os principais impactos causados por controles de acesso lógico inadequados são divulgados e não autorizado o acesso às informações, alteração não autorizadas de dados e aplicativos de dados e comprometimento da integridade do sistema. Os impactos podem ser ainda maiores em aplicativos que manipulam dados confidenciais ou registros financeiros da organização, ou se os sistemas estiverem conectados ao mundo externo, ou seja, conectados na internet.

O controle de acesso inadequado compromete a integridade e a confidencialidade dos dados e aumentam os riscos de destruição ou divulgação indevida de dados.

A inexistência de controle de acesso a arquivos de dados permite que um indivíduo faça mudanças não autorizadas para tirar alguma vantagem pessoal imediata, como por exemplo:

a) Alterar o número de conta de um pagamento, desviando dinheiro para si mesmo;

b) Alterar o inventário da empresa para esconder um furto cometido por ele;

c) Aumentar seu salário na folha de pagamento;

d) Obter informações confidenciais a respeito de transações ou indivíduos, visando futura extorsão ou chantagem.

Da forma análoga, o acesso irrestrito a aplicativos permite a modificação não autorizada de seus programas ou a introdução de códigos de programação mal-intencionados. A alteração dos

[4] *Off-line*, significa que nenhuma ligação por linha telefônica ou outra, que esteja no momento ativa.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

programas pode ser feita de tal forma a permitir acesso a arquivos de dados resultando nas mesmas situações citadas anteriormente.

A falta de controle de acesso sobre meios magnéticos, impressoras e de telecomunicações podem resultar nos mesmos problemas, já que permitem entrada nos sistemas computacionais, acesso a informações confidenciais, possível substituição de dados ou programas e danificação intencional de equipamentos e programas de computador.

Sem controles de acesso adequados, a organização pode se deparar com perdas financeiras decorrente de fraudes, extorsões ou custos de restaurações ao estado inicial de programas e dados. Uma quebra de segurança pode resultar em perda de credibilidade, seguida de perdas de fatias de mercado para a concorrência e eventualmente, dependendo do ramo de atividade da instituição, inviabilidade de continuidade de seus negócios. Caso exista alguma obrigação legal, no que diz respeito a armazenamento e não divulgação de dados (dados pessoas de seus funcionários, dados financeiros de clientes etc.), a organização pode ainda sofrer processos judiciais, se essas informações forem divulgadas e utilizadas indevidamente.

Os aspectos de segurança relacionados a seguir devem ser considerados como uma lista de verificações para gerência de segurança, essa lista pode servir como um conjunto de tarefas a serem realizadas para garantir a segurança de acesso lógico.

7. MANUTENÇÃO E REVISÃO PERIÓDICA

Por conta das constantes mudanças às quais as organizações se submetem, as políticas devem ser constantemente atualizadas para refletirem tais mudanças. Além disso, é importante que a política esteja sempre sendo adaptada aos novos problemas de segurança que vão surgindo, com o intuito de responder às alterações no ambiente.

Para que um sistema de segurança seja efetivo é necessário que todos colaborem com as medidas adotadas. Esse conceito fundamental de segurança, denominado participação universal, é considerado por muitos administradores uma utopia. Muitos especialistas acreditam que esperar cooperação por parte dos usuários é uma meta longínqua. Conseguir que eles apenas não atrapalhem já é um resultado extraordinário.

Com as medidas de segurança determinadas nas políticas esse problema é ainda maior, pois a maiorias desses procedimentos são simples ações que esperamos que os usuários façam. Infelizmente não podemos esperar que todas as pessoas da empresa colaborem. Por isso, devem ter implementados mecanismos que permitam avaliar o nível de conformidade por parte dos usuários com a prática exigida pela política.

Lista de Verificações de Controle de acesso lógico:

- Conceder acesso aos usuários, apenas aos recursos realmente necessários para a execução de suas tarefas;
- Restringir e monitorar o acesso a recursos críticos;
- Utilizar *software* de controles de acesso lógico;

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

- Utilizar Criptografia;
- Revisar periodicamente as listas de acesso;
- Evitar dar orientações ao usuário durante o processo de logon.
- Bloquear a conta do usuário após certo número de tentativas frustradas de logon.
- Restringir acesso a determinados periféricos.
- Fornecer contas a pessoas autorizadas.
- Não fornecer a mesma conta para mais de um usuário.
- Ao conceder ao usuário, informá-lo sobre as políticas de senha da organização.
- Bloquear se possível, a escolha de senhas consideradas frágeis e orientar o usuário na escolha de senhas mais seguras.
- Orientar os usuários para não armazenarem senhas em arquivos ou enviá-las por e-mail.
- Armazenar as senhas no sistema sob a forma criptografada.
- Prevenir o uso frequente de senhas já utilizadas pelo mesmo usuário anteriormente.
- Estabelecer um prazo máximo de utilização de uma mesma senha.
- Informar os usuários quanto aos perigos de divulgação de senhas.
- Impedir que os usuários sejam capazes de ler os arquivos de senha, identificar e trocar senhas de outros usuários.
- Desabilitar contas inativas, sem senhas ou com senhas padronizadas.
- Desabilitar as senhas de ex-funcionários.
- Não armazenar senhas em logs.
- Manter e analisar trilhas de auditoria de logs.
- Limitar o número de sessões concorrentes e o horário de uso dos recursos computacionais.
- Configurar *time-out* automático.
- Revisar e incorporar as listas de verificações propostas na política de segurança e nos outros tópicos de caráter mais específico, de acordo com a área ou plataforma a ser auditada.

O Controle de Ambiental, assim como o controle de acessos lógicos, os controles ambientais também constam na segurança da organização, pois estão relacionados com a disponibilidade e a integridade de sistemas computacionais. Os controles ambientais visam proteger os recursos computacionais contra danos provocados por desastres naturais (incêndio, enchentes), por falhas na rede de fornecimento de energia, ou no sistema de ar-condicionado etc.

a) Incêndio - Os controles associados a incêndios podem ser preventivos ou supressivos, isto é, procedimentos para evitar incêndios ou combatê-lo de forma eficiente.

b*) Controles Preventivos* - As medidas preventivas muitas vezes são implementadas logo na construção do prédio, com o uso de material resistente à ação do fogo, dispositivo de detecção de fumaça ou calor, e a instalação de para-raios. Após a construção, durante o funcionamento normal da organização, é aconselhável.

c) Controles Supressivos - A instituição deve estar preparada para suprimir ou minimizar os efeitos de um incêndio, deve possuir mangueiras e/ou extintores de incêndio em número suficiente e do tipo adequado para especificações técnicas, e instalar sistemas automáticos de combate ao fogo. É necessário o treinamento de funcionários para utilização adequada dos dispositivos.

7.1 CRIPTOGRAFIA

Estuda os princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

Figura 1 –Máquina Enigma, utilizada na cifragem e decifragem de mensagens secretas.

8. PRÍNCIPIOS BÁSICOS E OBJETIVOS

Os príncipios básicos da segurança são: Autenticidade,Confidencialidade e Integridade das informações. Os benefícios evidentes são reduzir os riscos como vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas e assim consequentemente, aumentar a produtividadedos usuários através de um ambiente mais organizado, com maior controle sobre os recursos de informática e, finalmente, viabilizar aplicações críticas da empresa.

A criptografia tem quatro objetivos principais:

a) *Confidencialidade da mensagem*: só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua cifrada. Além disso, a obtenção de informação sobre o conteúdo da mensagem (como uma distribuição estática de certos caracteres) não deve ser possível, uma vez se o for mais fácil a análise criptográfica.

b*) Integridade da mensagem*: o destinatário deverá ser capaz de deteminar se a mensagem foi alterada durante a tranmissão.

c) *Autenticação da mensagem*: o destinatário deverá ser capaz de identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

Nem todos os sistemas ou algoritmos criptográficos são utilizados para atingir todos os objetivos listados acima. Normalmente, existem algoritmos[5] específicos para cada uma destas funções. Mesmo em sistemas criptográficos bem concebidos, bem implementados e usados adequadamente, alguns dos objetivos acima não são práticos (ou mesmo desejáveis) em algumas circunstâncias. Por exemplo, o remetente de uma mensagem pode querer permanecer anônimo, ou o sistema pode destinar-se a um ambiente com recursos computacionais limitados, ou pode não interessar a confidencialidade.

9. ASSINATURAS E CERTIFICADOS DIGITAIS

Um benefício da utilização da criptografia assimétrica é a utilização de assinaturas digitais, que permitem ao destinatário verificar a autenticidade e integridade da informação recebida. Além disso, uma assinatura digital não permite o repúdio, isto é, o emitente não pode alegar que não realizou a ação, considerando sua assinatura digital. O mecanismo de funcionamento da assinatura digital, antes de encriptar a informação utilizando a chave pública do destinatário, encripta-se utilizando a chave privada do emitente, se todo o processo ocorrer corretamente à informação só pode ter sido gerada pelo emitente alegado. O importante é que não deve confundir com assinatura digital com assinatura digitalizada. Esta última consiste em uma assinatura feita à mão por um indivíduo que depois é capturada através de *scanner* e incluída em documentos. No Brasil uma das empresas que fornecem assinatura digital é a CERTSIGN (http://www.certisign.com.br/).

A utilização de sistemas criptografados de chave pública deve considerar sempre a encriptação para a pessoa correta. A manutenção de chaves públicas em locais públicos requer a correta identificação do proprietário da chave, para evitar o denominado "***man-in-the-middle***[6]", onde um impostor disponibiliza chaves falsas que serão utilizadas para encriptar dados, e posteriormente, interceptá-los.

Em ambiente pequeno, pode-se controlar a disponibilidade e validade das chaves públicas através da verificação física, simplesmente atentando se a pessoa que está entregando a chave pública é realmente a proprietária dela. Em ambientes públicos como a internet, e para comunicação com pessoas nunca encontradas pessoalmente, é difícil a manutenção.

Os certificados digitais simplificam esta tarefa, funcionando como credenciais, semelhante a um cartório, os cartórios digitais atestam a autenticidade das informações incluídas no certificado, considerando que existe confiança frente ao cartório digital. Um certificado é constituído em três componentes básicos:

- Uma chave pública;
- Informação de certificado (identificação do usuário, dados pessoas e profissionais, contatos etc.);

[5] Algoritmos é uma sequência não ambígua de instruções que é executada, até que determinada condição se verifique.
[6] É um tipo de ataque que são usados em sistemas de segurança, consiste em interceptar os tráfegos entre dois computadores.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

- Uma ou mais assinaturas digitais do cartório digital.

A assinatura digital irá atestar somente a combinação de dados contida no certificado digital, com a chave pública existente, porém não atestando o certificado como um todo.

A distribuição do certificado digital pode ser realizada, basicamente, de três maneiras:

- Distribuição manual, através de disquetes, rede e e-mails, de abrangência reduzida, devido às dificuldades de escalabilidade;

- Distribuição por servidor de certificados, que é um banco de dados que permite, a seus usuários, o envio e recebimento de certificados digitais;

- PKIs (*Public Key Infrastructures*), atuam como servidor de certificado, adicionando capacidade de administração de certificados por um *Certification Authority* (CA).

A criptografia apresenta-se como uma ferramenta de grande utilidade para uma série de aplicações. Uma aplicação típica da criptografia é sua utilização em canais de tráfego de mensagens, construídos a partir de tecnologias bem conhecidas. Tais sistemas podem ter diferentes níveis de complexidade. Dentre estas aplicações incluem: segurança de comunicações, identificação e autenticação. Outras aplicações envolvem sistemas para comércio eletrônico e correio eletrônico seguro.

a) *Segurança de comunicações* - As aplicações que envolvem segurança de comunicação são as que mais demandam o uso da criptografia. Duas pessoas podem se comunicar de forma segura encriptando as mensagens trocadas entre elas. Isto pode ser feito de forma que uma terceira pessoa que esteja interceptando estas mensagens, nunca possa ser capaz de decifrá-las.

b) *Identificação e Autenticação* - São as mais vastas aplicações da criptografia Identificação é o processo de verificação da identidade de alguém ou de alguma coisa. Na eletrônica o uso da criptografia, é o seguinte os cartões de terminais automáticos são associados a uma senha a qual vincula o proprietário do cartão ao proprietário da conta. Quando o cartão é inserido em um terminal, a máquina pede a senha, a quem tem este cartão. Caso esta senha esteja correta, a máquina infere que aquela pessoa seja o proprietário da conta e libera o acesso. Uma outra aplicação importante da criptografia é a Autenticação. A autenticação é similar à identificação, uma vez que ambos os processos permitem a uma entidade o acesso a determinados recursos. Porém, a autenticação é mais abrangente, dado que ela não envolve necessariamente a identificação da pessoa ou entidade. A autenticação meramente determina se dada pessoa ou entidade é autorizada.

c) *Comércio Eletrônico* - Ao longo dos anos tem havido um crescimento do número de negócios conduzidos via internet. Esta forma de negócios é conhecida como Comércio Eletrônico. O comércio eletrônico envolve uma série de atividades realizadas de forma eletrônica, dentre as quais se destacam as transferências de fundos que são também realizadas desta forma.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

10. REVISÃO PERIÓDICA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

As organizações estão em constantes mudanças, o tempo todo se aprimorando e se repensando, a fim de se adaptarem às constantes demandas de mercado e buscarem novas oportunidades.

Por isso, as políticas não devem ser vistas com um conjunto estático de documentos, pois estariam invariavelmente fadadas ao esquecimento e abandono. Sendo sua elaboração um processo que demanda tremendo esforço e alocação de recursos, o abandono das políticas por falta de atualização pode ser considerado um completo desperdício. Quanto mais tempo levar para atualizar as políticas, maior será a probabilidade de que elas se tornem inadequadas. Com isso, provavelmente terá duas situações:

1 – As alterações necessárias serão tantas que não haverá tempo e recursos para fazê-las;

2 – A não atualização da política será tamanha que ela precisará ser praticamente refeita.

Sendo assim, aconselha-se a fazer um processo de revisão constante das políticas. Assim, o tempo do intervalo entre os processos de revisão será determinado por uma série de fatores que variam de uma organização para outra:

1 – Disponibilidade de recursos.

2 – Tamanho.

3 – Taxa de crescimento.

4 – Frequência com a qual as mudanças são feitas por conta de fatores externos, entre outras coisas.

Em geral, a revisão anual atende grande parte das organizações, sendo o prazo de dois anos recomendado para as de grande porte. Fora o processo periódico de revisão, outros eventos de grande magnitude podem também disparar um processo de revisão fora de hora, como fusões, novas regulamentações sobre Segurança da Informação, mudanças políticas, porte de investimentos com vistas à expansão das operações etc.

11. CONCLUSÃO

A Gestão e Segurança da Tecnologia da Informação é uma área que não abre muito os olhos dos profissionais da informática, porém é um assunto muito importante em qualquer ramo que se possa seguir e no ramo organizacional da saúde não é diferente, pois o mesmo manipula dados de suma importância, em virtude de seu sucesso.

A globalização e a rapidez com que as empresas precisam se comunicar fazem com que o volume de informações geradas seja cada vez maior e mais estratégico, tornando a informação um valioso ativo para a empresa.

Com funcionários bem treinados e conscientes de suas responsabilidades com a Segurança da Informação para a empresa, certamente as tecnologias posteriormente implementadas apresentarão melhores resultados.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

Cada vez mais as empresas vêm adotando diversas formas de planejamento dessa informação, tornando assim, mais eficazes e eficientes, conseguindo com isso se organizar e se preparar para as mudanças que ocorrem a cada dia no mercado globalizado e competitivo, porém muitas empresas esquecem de gerenciar a segurança dessa informação, onde poderão fazer com que a empresa perca mercado e/ou consequências muito mais graves.

Diante disso, a Segurança da Informação apresenta-se não apenas como modismo entre as empresas e sim como uma área realmente necessária, que pode oferecer um diferencial competitivo e principalmente garantirá que sempre que uma informação seja solicitada esta esteja íntegra, disponível e com sua confidencialidade garantida.

Assim, efetiva-se essa primeira contribuição, certos de que as empresas para ter a integridade e confidencialidade de suas informações devem promover uma política de segurança da informação voltadas para a proteção dos Ativos, proporcionando uma credibilidade no mercado no qual opera.

Identificou-se, ainda, que existe um número pífio da aglutinação de informações voltadas para a área de segurança da informação, onde este compendio servirá no futuro como base para estudos de desenvolvimento de conhecimento nesta área, proporcionando assim identidade e uma linguagem única entre os estudiosos.

12. REFERÊNCIAS

BURNETT, Esteve; STEPHEN Parine. **Criptografia e Segurança.** Porto Alegre: Editora Campus, 2002.

DIAS, Claudia. **Segurança e Auditoria da Informação.** Porto Alegre: Editora Axcel Books, 2000.

HORTON, Mike; MUGGER, Clinton. **Hack Notes:** Segurança de Redes, Referência Rápida. Rio de Janeiro: Editora Campus, 2003.

KUROSE, James; ROSS, Keith. **Redes de Computadores e a Internet:** Uma Abordagem Top/Down. 3. ed. São Paulo: Editora Pearson Addison Wesley, 2006.

NAKAMURA, Emilio Tissato; GLUS, Paulo Lício de. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Editora Futura, 2003.

RAMOS, Anderson; BASTOS, Alberto; LYRA, Alexandre; ANDRUCIOLI, Alexandre; AFFONSO, Carlos; POGGI, Eduardo; PINTO, Elaine; BLUM, Renato Opice; ALEVATE, William; MARINHO, Zilta. **Security Officer:** Guia Oficial para Formação de Gestores em Segurança da Informação. Porto Alegre: Editora Zouk, 2006.

REZENDE, Denis Alcides. **Sistemas de Informações Organizacionais:** guia prático para projetos em cursos de administração, contabilidade e informática. São Paulo: Editora Atlas, 2005.

SANTOS, Antônio Silveira Ribeiro dos. **As Empresas e a Era da Informação.** [*S. l.: s. n.*], 2006. Disponível em: http://www.aultimaarcadenoe.com/artigo16.htm. Acesso em: 12 out. 2006.

RECISATEC – REVISTA CIENTÍFICA SAÚDE E TECNOLOGIA
ISSN 2763-8405

SILVA FILHO, Antonio Mendes da. **A Era da Informação.** [*S. l.: s. n.*], 2001. Disponível em: http://www.espacoacademico.com.br/002/02col_mendes.htm. Acesso em: 12 out. 2007.

SITES CONSULTADOS:

MÓDULO. Disponível em: http://www.modulo.com.br. Acesso em: 15 out. 2007.

SMARTSEC. Disponível em: http://www.smartsec.com.br/ Acesso em: 08 fev. 2008.