Documentos

ISSN 1517-3135
Maio, 2009
70

Segurança da Informação na Embrapa Amazônia Ocidental – Boas Práticas: Conceitos e Aplicações

Embrapa

ISSN 1517-3135
Maio, 2009

Empresa Brasileira de Pesquisa Agropecuária
Embrapa Amazônia Ocidental
Ministério da Agricultura, Pecuária e Abastecimento

Documentos 70

Segurança da Informação na Embrapa Amazônia Ocidental – Boas Práticas: Conceitos e Aplicações

Victor Leonard Nascimento de Souza
Maria Augusta Abtibol Brito
Francisco Célio Maia Chaves
Araluce Regina de Souza Lima
Síglia Regina dos Santos Souza
José Raimundo da Silva Barbosa
Alexandre Menezes da Costa
Deise Maria Pessoa de Souza
Adriana Barbosa de Souza

Embrapa Amazônia Ocidental
Manaus, AM
2009

Exemplares desta publicação podem ser adquiridos na:

Embrapa Amazônia Ocidental
Rodovia AM-010, km 29, Estrada Manaus/Itacoatiara
Caixa Postal 319
Fone: (92) 3303-7800
Fax: (92) 3303-7820
www.cpaa.embrapa.br

Revisor de texto: *Síglia Regina dos Santos Souza*
Normalização bibliográfica: *Maria Augusta Abtibol Brito*
Diagramação: *Gleise Maria Teles de Oliveira*
Capa: *Gleise Maria Teles de Oliveira*
Fotos da capa: *Neuza Campelo e Raimundo Nonato C. da Rocha*
1ª edição
1ª impressão (2009): 300

CIP-Brasil. Catalogação-na-publicação.
Embrapa Amazônia Ocidental.

Segurança da informação na Embrapa Amazônia Ocidental – boas práticas: conceitos e aplicações. / Victor Leonard Nascimento de Souza... [et al.]. Manaus: Embrapa Amazônia Ocidental, 2009.
36 p. (Embrapa Amazônia Ocidental. Documentos; 70).

ISBN 1517-3135

1. Segurança da informação. I. Souza, Victor Leonard Nascimento de. II. Brito, Maria Augusta Abtibol. III. Chaves, Francisco Célio Maia. IV. Lima, Araluce Regina de Souza. V. Barbosa, José Raimundo da Silva. VI. Costa, Alexandre Menezes da. VII. Souza, Síglia Regina dos Santos. VIII. Souza, Deise Maria Pessoa de. IX. Adriana Barbosa de. X. Série.

Autores

Victor Leonard Nascimento de Souza
Analista de Sistemas, Especialista em Tecnologia Web, analista da Embrapa Amazônia Ocidental, Manaus, AM, victor.souza@cpaa.embrapa.br

Maria Augusta Abtibol Brito
Bibliotecária, Especialista em Monitoramento e Inteligência Competitiva, analista da Embrapa Amazônia Ocidental, Manaus, AM, augusta.abtibol@cpaa.embrapa.br

Francisco Célio Maia Chaves
Engenheiro agrônomo, D. Sc. em Plantas Medicinais, pesquisador da Embrapa Amazônia Ocidental, Manaus, AM, celio.chaves@cpaa.embrapa.br

Araluce Regina de Souza Lima
Bióloga, M.Sc. em Biotecnologia, analista da Embrapa Amazônia Ocidental, Manaus, AM, araluce.lima@cpaa.embrapa.br

Síglia Regina dos Santos Souza
Jornalista, Especialista em Comunicação Empresarial, analista da Embrapa Amazônia Ocidental, Manaus, AM, siglia.regina@cpaa.embrapa.br

José Raimundo da Silva Barbosa
Analista de Rede, B.Sc. em Processamento de Dados, analista da Embrapa Amazônia Ocidental, Manaus, AM, jose.barbosa@cpaa.embrapa.br

Alexandre Menezes da Costa
Administrador de Empresas, Pós-Graduando em Logística Empresarial, analista da Embrapa Amazônia Ocidental, Manaus, AM, alexandre.costa@cpaa.embrapa.br

Deise Maria Pessoa de Souza
Administradora de Empresas, Especialista em Administração de Recursos Humanos, analista da Embrapa Amazônia Ocidental, Manaus, AM, deise.souza@cpaa.embrapa.br

Adriana Barbosa de Souza
Bacharel em Relações Públicas, analista da Embrapa Amazônia Ocidental, Manaus, AM, adriana.ribeiro@cpaa.embrapa.br

Apresentação

Na sociedade da informação, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança da informação tornou-se ponto crucial para a sobrevivência das instituições.

Diante desse cenário, a Embrapa Amazônia Ocidental, demonstrando preocupação com a segurança das informações geradas e mantidas nessa instituição, criou o Comitê de Gestão e Segurança da Informação da Embrapa Amazônia Ocidental, o qual vem, por meio desta publicação, trazer algumas informações para proporcionar maior familiarização com o tema, por meio do conhecimento dos erros mais frequentes, e orientação sobre boas práticas para gerenciar os riscos e adotar medidas mais confiáveis ao lidar com os recursos de que dispomos, objetivando com isso estimular a consolidação da segurança de informação.

Maria do Rosário Lobato Rodrigues
Chefe-Geral

Sumário

Segurança da Informação na Embrapa Amazônia Ocidental – Boas Práticas: Conceitos e Aplicações

Victor Leonard Nascimento de Souza
Maria Augusta Abtibol Brito
Francisco Célio Maia Chaves
Araluce Regina de Souza Lima
Síglia Regina dos Santos Souza
José Raimundo da Silva Barbosa
Alexandre Menezes da Costa
Deise Maria Pessoa de Souza
Adriana Barbosa de Souza

Introdução

Na sociedade atual, o fluxo da informação vem se constituindo em uma das etapas mais importantes no processo de avanço da tecnologia da informação. Um dos aspectos mais relevantes relacionados à informação diz respeito a sua segurança. Ela se aplica a pessoas e empresas, é, portanto, de natureza corporativa, envolvendo todos os setores que lidam com a informação. Nesse sentido, informação é todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode ter caráter de uso restrito ou público.

A Empresa Brasileira de Pesquisa Agropecuária (Embrapa) tem como missão viabilizar soluções de pesquisa, desenvolvimento e inovação para a sustentabilidade da agricultura, em benefício da sociedade brasileira. É responsável pela coordenação do Sistema Nacional de Pesquisa Agropecuária (SNPA), constituído por instituições públicas federais, estaduais, universidades, empresas privadas e fundações, as quais, de forma cooperada, executam pesquisas nas diferentes áreas geográficas e campos do conhecimento científico. Diante do desafio de gerar conhecimento e tecnologia com importância estratégica para o desenvolvimento do País, a Empresa tem a responsabilidade de proteger e buscar formas de implementar a segurança das informações com as quais trabalha.

A Embrapa Amazônia Ocidental, também preocupada com essa questão, busca implementar a segurança da informação por meio de ações básicas, como: constituir comissão para análise e melhoria do processo, promover palestras e participar de eventos sobre o tema. Entre essas ações, está a disseminação de boas práticas junto a seu público interno. Dessa forma, esta publicação tem o objetivo de internalizar conceitos relativos à segurança da informação no âmbito da Embrapa Amazônia Ocidental.

Ao mesmo tempo que a tecnologia de informação nos coloca em conexão com o mundo e oferece múltiplas possibilidades para disponibilização e troca de informações com rapidez, também estamos sujeitos a diversas situações que ameaçam o bom funcionamento e a continuidade dos negócios da empresa.

O que é Segurança da Informação

A Segurança da Informação baseia-se em três princípios básicos: confidencialidade, integridade e disponibilidade, os quais orientam a análise, o planejamento e a implementação das informações.
Esses princípios, segundo padrões internacionais vigentes, são assim definidos:

- Confidencialidade – propriedade que limita o acesso a informações tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
- Integridade – propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).
- Disponibilidade – caracteriza-se por garantir que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

A segurança da informação já é realidade em muitos sistemas corporativos institucionais e prática adotada e incorporada na rotina gerencial. Em relação à sua adoção, é consenso a necessidade de implementação de uma política de segurança que norteie e garanta os princípios, resultando no alcance dos objetivos desejados.

Definições úteis

- ANTISPYWARE – Programa para combater *spyware*.

- FIREWALL – Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a determinado ponto de controle da rede.
- GATEWAY – É uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão ou mesmo traduzir protocolos.
- HACKERS – Indivíduos que elaboram e modificam *software* e *hardware* de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas.
- INPUTS – São dados que se recebe.
- MALWARE – É um *software* destinado a se infiltrar em um sistema de computador alheio, de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não).
- OUTPUTS – São dados que são produzidos e emitidos.
- POP-UP – É uma janela extra que abre no navegador, ao se visitar uma página web ou acessar uma hiperligação específica.
- PROTEÇÃO WPA – É um protocolo de comunicação via rádio que garante uso de senha como item de segurança.
- SPAM – É uma mensagem eletrônica não solicitada enviada em massa.
- SPYWARE – Consiste num programa automático de computador que recolhe informações sobre o usuário, sobre os seus costumes na internet e transmite essas informações a uma entidade externa na internet, sem o seu conhecimento ou consentimento.
- TAXA DE FRANQUIA – Valor fixo pago no início da negociação em contratos de franquia.
- TAXA DE PUBLICIDADE – Percentual sobre a venda de produto ou serviço, pago pelo franqueado ao titular do produto ou serviço.
- TAXA DE ROYALTIES – Percentual sobre preço líquido de vendas, pago pelo licenciado ao titular dos direitos.
- URLs (Uniform Resource Locator) – em português: Localizador de Recursos Universal, é o endereço de um recurso (um arquivo, uma impressora, etc.), disponível em uma rede, seja a internet, seja uma rede corporativa, uma intranet.
- WEB PROXY – É um servidor que atende a requisições dos usuários repassando os dados a outros servidores e, depois, encaminhando a resposta do servidor ao usuário.

- WI-FI – Refere-se a uma rede de computadores sem a necessidade do uso de cabos, sejam estes telefônicos, coaxiais ou ópticos, por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho.

Erros mais frequentes na segurança da informação

Ações de segurança da informação devem ser prioridade para as organizações. Apesar de comumente associadas apenas à esfera tecnológica, as informações mais valiosas das empresas não estão somente em formato digital trafegando pelas redes, mas também em papéis impressos ou manuscritos, em reuniões, em conversas informais ou via telefone e, principalmente, na memória dos funcionários. Diante disso, é importante vislumbrar que os problemas de segurança são físicos, tecnológicos e também humanos.

Para minimizar riscos, são relacionados, nos itens seguintes, alguns erros frequentes – mas que podem ser facilmente evitados – quanto à segurança da informação.

Ausência de política e de normas formais de segurança

Não há como tratar de segurança da informação, ou de segurança em termos gerais, se não há regras claras e definidas sobre o assunto.

Falha na aplicação de política de segurança

Todos os empregados devem estar conscientes e comprometidos com a política de segurança institucional; caso contrário, não há como evitar falhas na sua aplicação.

Aplicação de uma política padronizada para todos, desprezando as particularidades de cada grupo

Não há como criar linhas gerais de segurança da informação na instituição como um todo sem considerar as peculiaridades de cada setor. Por exemplo: o nível de acesso à biblioteca e ao almoxarifado da empresa é diferenciado em função da especificidade de suas atribuições, sendo permitida a entrada de terceiros nas dependências da biblioteca, bem como permitida a consulta aos documentos do acervo. Já no setor de almoxarifado, apenas pessoas autorizadas têm acesso.

Atribuição à área de TI como a única responsável pela política de segurança

A segurança da informação deve envolver todos os setores da instituição, pois a promoção da integridade dos ativos institucionais depende da segurança patrimonial, dos recursos humanos, da propriedade intelectual, entre outros.

Centralização das informações

Sem a participação e o envolvimento de todas as pessoas da equipe na construção de um projeto ou de uma ideia, as chances de fracasso são grandes. Essa concepção pode ser aplicada à segurança da informação. A falha na disseminação das informações referentes à política de segurança institucional a todos os empregados certamente inviabilizará a aplicação das normas de segurança da instituição. Portanto, há de se considerar os aspectos legais, físicos, éticos, políticos, técnicos e de negócio de todos os setores, de forma integrada.

Falta de comunicação eficaz

Em todo processo de gestão, a falta de comunicação ocasiona falhas nas ações e nos objetivos organizacionais. Necessário se faz promover a cultura de uma comunicação eficaz, de forma que os *inputs* e *outputs* de um processo ou sistema sejam efetivamente conhecidos por todos os colaboradores envolvidos.

Falta de estabelecimento de parcerias

O não estabelecimento de parcerias internas entre os diversos setores, bem como de parcerias externas com instituições da mesma área, amplia as chances de fracasso. Portanto, um projeto de gestão, seja ele qual for, não pode ser visto ou tratado isoladamente dentro de um contexto. A busca de parcerias simplifica ações e procedimentos a ser adotados para o alcance dos objetivos e resultados esperados. Dessa forma, um projeto de gestão de segurança da informação, para ter êxito, não pode ser elaborado e desenvolvido isoladamente. O ideal é estabelecer parcerias que garantam a eficácia de sua implantação e sustentação.

Não valorização de novas ideias

Para que um projeto de gestão de segurança da informação se concretize e se realize eficazmente, é necessário que a instituição esteja atenta ao cenário e busque continuamente se antecipar às mudanças nos ambientes interno e externo. É necessário também que se valorizem novas ideias capazes de promover a melhoria do sistema de segurança institucional.

Ausência de monitoramento regular da atividade de Internet

A ausência de monitoramento provoca falhas no combate aos códigos maliciosos no *gateway,* ocasionando: ataques não documentados*,* invasão de *spywares*, bloqueio apenas de URLs, filtragem apenas do tráfego de entrada, falha no bloqueio de arquivos compactados, falta de confiança no tipo informado de arquivo, assim como outros riscos à segurança da informação.

Ausência de controle eficiente de *downloads* de *shareware* e executáveis por parte dos usuários da rede

O que pode parecer uma tarefa inocente pode trazer muitos danos à rede de dados de uma corporação, pois muitos *hackers* utilizam programas de fachada para embutir seus códigos maliciosos e disseminar vírus ou *spyware* nas corporações com ajuda do próprio usuário sem que este tenha consciência disso.

Uso de *notebooks* ou similares, em locais de rede pública (Wi-fi), sem a utilização de uma chave de segurança

Usuários corporativos também são usuários finais e, justamente por isso, podem comprometer a segurança do ambiente profissional, já que nem sempre sabem que põem a empresa em risco com certas ações. Por falta de conhecimento, muitos funcionários conectam seus *notebooks* ou *smartphones* a uma rede aberta, na qual todos os seus dados transitam sem proteção. Ou seja, ao acessar seu e-mail em um aeroporto, por exemplo, o nome de usuário e senha trafegarão livremente na rede do local.

Salvamento de dados *online* ou em mídias removíveis

Se a pessoa não tem um *notebook* da empresa, ela pode salvar arquivos em *pen drive*, CDs ou em aplicativos *online*; porém se a máquina onde a mídia for usada estiver contaminada ou o dado for roubado, além de colocar em risco as informações confidenciais da empresa, os funcionários podem contaminar o computador corporativo com um código malicioso adquirido na máquina impropriamente utilizada.

Encaminhamento de arquivos institucionais para *e-mail* pessoal

Mesmo sem intenção de burlar políticas de segurança, o usuário, muitas vezes, quer aproveitar um dado para usar depois, e daí o erro, pois ele sairá de uma estrutura segura e poderá comprometer a integridade das informações institucionais contidas no arquivo.

Acesso a *links* maliciosos

Caso a empresa não imponha limites de navegação aos seus funcionários, é comum o acesso a qualquer *link*, sem avaliar a sua procedência.

Utilização da internet para fins particulares

A maioria dos funcionários não vê problemas em pagar uma conta pelo *bankline* ou acessar alguns sites, como redes sociais e lojas virtuais, durante o expediente. Atheniense (2009) cita o exemplo de uma usuária que costumava acessar com frequência um site de cosméticos, e que um *spyware* instalado em sua máquina detectou esse hábito. "O *cracker* criou um *phishing* especial, dizendo que ela ganharia alguns cosméticos por ser cliente preferencial, e pediu seus dados para cadastro". O golpe, que é típico, afetou a empresa, porque a usuária tinha acesso à conta bancária daquela, e informações foram roubadas juntamente com os dados pessoais da usuária.

Burla ao bloqueio de aplicativos

É comum que os usuários ignorem as ordens da empresa relacionadas a limites de acesso – como bloquear redes sociais e comunicadores instantâneos. Com ferramentas de *web proxy*, o usuário acessa o que quer, usando um servidor de *proxy*, que não é o da empresa. Por isso, o bloqueio de sites não é feito à toa pelas empresas. Em recados deixados no *Orkut*, por exemplo, são distribuídos vários *malwares*, em golpes simples que pedem ao usuário para "clicar para ver fotos" – e é nesse momento que acontece a contaminação do computador do usuário e uma possível ameaça a toda a rede da instituição.

Ausência de política de segurança no uso de senhas

Falhas quanto ao uso de senhas

Abaixo estão relacionados exemplos de práticas a ser evitadas quando do uso ou da escolha de senha:

- Escolha de palavras que estejam em dicionários. As senhas não devem ser palavras com sentido, isso evita o ataque por dicionário, onde todas as palavras são experimentadas sequencialmente.

- Uso do próprio nome, iniciais ou apelido como senha.
- Utilização de nome de marcas. Exemplo: Microsoft
- Utilização da própria identificação (User ID)
- Utilização da composição de apenas uma mesma letra. Exemplo: eeeeeee.
- Utilização de sequências particulares do teclado. Exemplo: ZXCVB
- Utilização de palavras simples de forma invertida. Exemplo: ahnes (senha).
- Utilização de senhas compostas apenas por letras.
- Utilização de senhas sequenciais. Exemplo: ABC123, ABC456, ...
- Utilização de senhas pronunciáveis, ou seja, uma cadeia de caracteres composta de consoantes e vogais de forma alternada. Escolher uma sequência que gere uma palavra sem sentido. Exemplo: BACEDIFO.
- Utilização de iniciais de uma frase fácil de lembrar, para a memorização da senha. Exemplo: O meu nome é Maria OMNEM.

Boas práticas em segurança da informação

No aspecto social

A importância das pessoas no processo de Segurança da Informação

Uma informação pode sofrer ameaças à sua integridade em qualquer das etapas, desde a coleta, organização, armazenagem, recuperação, interpretação, transmissão, transformação à utilização. A segurança de determinada informação pode ser afetada por fatores comportamentais de quem a utiliza, por fatores do ambiente ou da infraestrutura que a cerca ou por pessoas mal intencionadas que têm como objetivo furtar, destruir ou modificar a informação. Por mais que se adotem as melhores tecnologias, as pessoas têm responsabilidade fundamental em resguardar as condições para a segurança da informação. Por isso, é necessário considerar usuário e informação como elementos complementares e interdependentes. A informação poderá ser protegida utilizando-se meios tecnológicos, porém essa proteção não terá efeito sem a conscientização do usuário.

Entre os controles adotados para reduzir os riscos de segurança da informação, nos aspectos humanos, Araújo (2005) relaciona os seguintes :

- Seminários de sensibilização.
- Cursos de capacitação.

- Campanhas de divulgação da política de segurança.
- Crachás de identificação.
- Procedimentos específicos para demissão e admissão de funcionários.
- Procedimentos específicos para tratamento de recursos terceirizados.
- Termo de responsabilidade.
- Termo de confidencialidade.
- *Softwares* de auditoria de acessos.
- *Softwares* de monitoramento e filtragem de conteúdo.

Muitas vezes, a segurança da informação é reforçada no nível físico e técnico, mas negligenciada em relação ao comportamento humano. E é justamente nesse aspecto que as vulnerabilidades abrem espaço para vazamento de informações, ataque de *hackers* e atuação de pessoas que roubam informações pela prática denominada "Engenharia Social".

A engenharia social é uma prática para obter informações sigilosas e importantes aproveitando-se das falhas de segurança das pessoas e explorando a ingenuidade, a falta de informação ou a confiança excessiva, para manipular uma situação e violar procedimentos de segurança. Isso pode ocorrer, por exemplo, quando uma pessoa se faz passar por alguém que precisa de informações simples, mas por meio delas adentra na rotina da empresa e consegue captar informações privilegiadas e detalhes estratégicos e repassá-los ao concorrente, e com isso compromete determinado projeto ou todo o funcionamento de uma empresa.

Araújo (2005) afirma que as técnicas de engenharia social estão constantemente em evolução, explorando principalmente características do comportamento humano e falhas na estrutura de segurança, para conseguir seus objetivos. Porém, há alguns aspectos clássicos que podem servir de alerta. Um deles é não ser negligente, ao entregar informações a pessoas não autorizadas, mesmo quando as informações parecem ser inofensivas, pois estas podem ser a chave para acessar outras informações relevantes.

Diante disso, é necessário orientar e alertar os empregados para evitar que caiam nas técnicas da engenharia social. Uma regra básica é não fornecer informação pessoal ou interna da empresa, qualquer que seja, a menos que o solicitante seja alguém autorizado a obter tais informações.

Silva Filho (2004) indica algumas medidas que podem atenuar a vulnerabilidade humana diante de ataques da engenharia social:

- **Educação e Treinamento** – Conscientizar as pessoas sobre o valor da informação que elas dispõem e manipulam, seja de uso pessoal ou institucional. Informar aos usuários como age um engenheiro social.
- **Segurança Física** – Permitir o acesso a dependências de uma organização apenas às pessoas devidamente autorizadas, bem como dispor de funcionários de segurança para monitorar entrada e saída de pessoas na organização.
- **Política de Segurança** – Estabelecer procedimentos que eliminem quaisquer trocas de senhas. Por exemplo, um administrador jamais deve solicitar a senha e/ou ser capaz de ter acesso a senha de usuários de um sistema. Estimular o uso de senhas de difícil descoberta, além de remover contas de usuários que deixaram a instituição.
- **Controle de Acesso** – Os mecanismos de controle de acesso têm o objetivo de implementar privilégios mínimos a usuários, a fim de que estes possam realizar suas atividades. O controle de acesso pode também evitar que usuários sem permissão possam criar/remover/alterar contas e instalar *software* danosos à organização.

Inicialmente, para definir o quê e como proteger, é necessário avaliar a importância do que se dispõe, em termos de informação, do que se sabe e o que precisa ser resguardado, protegido e disponibilizado.

A disponibilização deve levar em conta, também, a temporalidade da informação, pois uma informação pode ter muito valor em determinado momento e contexto, mas logo depois se torna algo trivial. Também pode se considerar a capacidade de uma informação ser útil para originar mais informações, daí a necessidade de assegurar que esteja disponível em tempo hábil a quem estiver autorizado a utilizá-la, estabelecendo níveis de acesso (amplo ou restrito), assim como identificar os casos em que não deveria estar disponível, de forma alguma, para pessoas não autorizadas.

Classificação e acesso à informação

Os gestores e responsáveis devem classificar os tipos de informação e gerenciar os acessos, de acordo com o grau de confidencialidade e de necessidade por parte dos clientes. Não significa sonegar informações, mas disponibilizar com segurança a quem dela necessita para fazer bom uso, atendendo aos interesses da empresa.

Na Embrapa Amazônia Ocidental, adotam-se termos de responsabilização ao lidar com informações, seja por parte de empregados, seja por parte de de estagiários e bolsistas, a saber:

- **Estagiários e bolsistas** – Termo de Compromisso, alínea "c": "Manter total reserva em relação a quaisquer dados ou informações a que venha ter acesso em razão de sua atuação no cumprimento do estágio, não repassando-as a terceiros sob qualquer forma ou pretexto, sem prévia autorização formal da Empresa, independente de se tratar ou não de informação reservada, confidencial ou sigilosa".
- **Empregados** – Cláusula Quinta do Contrato de Trabalho: "Toda produção do empregado, no cumprimento de seu contrato de trabalho, seja técnico-científica ou classificada como direitos de propriedade imaterial (direitos da propriedade industrial, do autor, ou sobre cultivar) será de propriedade exclusiva da Empresa".

Cuidados importantes no manuseio de informações

Informações em meio impresso

Dados e informações impressos em papel, de uso restrito, confidencial ou mesmo de uso público, mas que ainda não estão finalizados para divulgação, não devem ficar expostos sobre as mesas, em locais de livre circulação de pessoas. O mesmo vale para memorandos, cartas, relatórios e outros documentos relativos a informações internas. Sugere-se arquivá-los em pastas, separados por categoria.

Os documentos em papel a ser descartados devem passar por triagem, para separar o que pode ir para reciclagem e os que precisam ser destruídos. Documentos com dados confidenciais devem ser picados ou queimados, evita-se com isso que sejam utilizados por pessoas de má fé.

Seja cauteloso, também, se for responsável pelo transporte de bens ou de documentos da empresa. Procure não chamar a atenção e evite que outras pessoas tenham acesso a esse tipo de material.

Informações em meio eletrônico ou digital

Os arquivos compartilhados em redes internas na empresa devem servir para facilitar o trabalho em equipe e disseminar informações. Por isso, é importante que a versão disponibilizada de um documento esteja finalizada e disponível apenas aos que precisam tomar conhecimento ou dela fazer uso.

No caso de compartilhar um documento com pessoas que precisam dele quando ainda está em fase de elaboração, procure verificar qual a forma mais segura entre o grupo. Identifique que não é um documento finalizado (indicar a versão). O correio eletrônico (e-mail), por exemplo, permite direcionar apenas aos envolvidos, enquanto a opção de colocar o

documento na rede aberta representa mais riscos (vírus, modificações, eliminação, etc). Procure verificar também opções oferecidas pelos aplicativos, como, por exemplo, proteção de arquivo ou de pastas por senha, controle de alterações no texto, etc.

Conversas sobre o ambiente de trabalho

Tratando-se de Segurança da Informação, pequenas atitudes fazem toda a diferença. Não faça comentários em locais públicos sobre os aspectos da segurança da empresa. Conversas informais relacionadas ao tema podem ser úteis a terceiros com intenções escusas. Sem perceber, as pessoas podem estar dando dicas sobre as fragilidades do ambiente de trabalho. Há casos em que o colaborador de uma empresa pode ser envolvido, de forma aparentemente inofensiva, no repasse de informações a seu interlocutor, as quais poderão ser usadas contra a empresa ou contra a segurança pessoal do informante.

Seus dados pessoais e os da empresa onde trabalha não devem ser de fácil acesso. Os hábitos de trabalho também não devem ser comentados aleatoriamente, na frente de qualquer pessoa. Eles devem ser apenas do seu interesse. Seja cauteloso.

Evite fornecer o número de telefone celular ou residencial de colegas de trabalho para outra pessoa, sem o expresso consentimento deles.

Durante suas viagens (a passeio ou a trabalho), evite fazer comentários relacionados ao trabalho na frente de pessoas desconhecidas ou de quem possa distorcer suas informações e a imagem institucional da empresa.

Segurança Física ou Patrimonial

Geralmente atribui-se à Segurança da Informação o sinônimo de Segurança em Tecnologia da Informação (TI), porém essa é somente uma de suas partes, e acaba operando isoladamente na chamada Segurança Física ou Patrimonial. Ao entender a segurança como uma garantia de que a empresa está protegida contra ameaças que possam causar impacto ao bom funcionamento dos negócios, deixa-se de lado a visão pontual e centralizada para adotar uma visão mais abrangente sobre o assunto.

Considerando a informação em diversos formatos (digital, impressa, conversações pessoais ou por telefone), a Segurança da Informação envolve todos os segmentos da organização e se preocupa com três categorias básicas de riscos: administrativas, físicas e tecnológicas.

Portanto, não adianta ter uma excelente estrutura de proteção da informação eletrônica, se outros fatores não colaboram para que a informação esteja realmente protegida. Para tanto, Almeida (2005) estabelece alguns tópicos importantes que devem ser considerados e tratados para fins de uma Segurança da Informação mais efetiva:

- Guardar as informações impressas em local adequado e seguro, sem expô-las sobre as mesas.
- Classificar criteriosamente as informações e definir quem pode ter acesso a elas.
- Fazer uma análise de risco, vulnerabilidades, ameaças e impactos envolvidos.
- Estabelecer medidas efetivas para tratamento dos riscos.
- Elaborar um plano de segurança da informação.
- Estabelecer requisitos para admissão e demissão de funcionários e de terceiros.
- Formalizar acordos e contratos de confidencialidade de informações com funcionários, terceiros, fornecedores e clientes (sempre que a situação exigir).
- Realizar treinamentos específicos para os gestores das informações sigilosas, incluindo procedimentos em situações de crise e emergências.
- Promover seminários e campanhas de conscientização para todos os membros da organização, destacando a importância e os cuidados a ser tomados para a efetiva segurança da informação.
- Avaliar instalações e criar dispositivos, medidas e procedimentos de segurança para proteção de salas de reunião e salas que guardem informações sigilosas.
- Utilizar, sempre que necessário, aparelhos para detectar a interceptação eletrônica da comunicação (“grampos”) e nela interferir sempre que julgar necessário.
- Evitar comentar dados sigilosos por telefone, fixo ou celular, bem como por meios eletrônicos.
- Estabelecer critérios claros de descarte e destruição de documentos sigilosos (tratamento adequado do “lixo”).
- Estabelecer controle efetivo do acesso físico, das cópias de chaves (claviculário) e da troca periódica do segredo das fechaduras que dão acesso às informações sigilosas.
- Estabelecer auditorias periódicas dos dispositivos de segurança da informação para detectar e tratar as falhas encontradas.

Para que essas ações tenham eficácia, se faz necessário criar um trabalho de conscientização com a participação de todos os membros da organização.

Segurança em Tecnologia da Informação – TI

Segurança em Tecnologia da Informação tem cinco princípios fundamentais: integridade, disponibilidade, não repúdio (técnica usada para garantir que alguém, ao realizar uma ação em um computador, não possa falsamente negar que realizou aquela ação), autenticidade e confidencialidade. São todos essenciais para assegurar a integridade e a confiabilidade de sistemas, mas sempre em conjunto com mecanismos de defesa com poder de agregar capacidade de detecção, reação e prospecção de perigos iminentes.

Cada empresa define seu nível de tratamento de cada princípio, podendo ser determinado pela suscetibilidade das informações ou dos sistemas de informações ou ainda pelo nível de ameaças na qual a organização se encaixa, sendo que, para este último, entra também a sensibilidade e os fatores definidos dentro de um estudo de gestão de riscos da organização.

Ao pensar em segurança da informação, muitas organizações se concentram apenas na implementação de *firewall* e na autorização de acesso, porém essas iniciativas são apenas parte da solução.

A seguir, serão apresentadas diversas ações que o usuário de uma rede de dados pode realizar com sucesso, para auxiliar na prevenção de ataques de códigos maliciosos ou, ainda, da perda da informação.

Controle de senhas

Prefira senhas difíceis de ser descobertas e mude os códigos com frequência. No quesito senha, o ideal é complicar mesmo; pare alguns instantes para elaborar sua senha, misture números com caracteres alfanuméricos e especiais. Altere sua senha periodicamente, se não tiver essa opção disponível, solicite à administração do serviço. Apenas anote suas senhas em papel em casos extremos e, logo após o uso, destrua-o.

Manipulação de mídias

Atualmente existe uma infinidade de mídias disponíveis para uso, como: *CD-ROM*, *DVD*, *pen drives*. Não utilize mídias de fora da empresa; se for necessário, realize antes uma checagem com antivírus.

Mídias com dados sigilosos devem ser adequadamente armazenadas, de preferência em local que possibilite o uso de chaves, cadeados ou código de segurança, como cofres.

Utilização de um programa antivírus e *spyware*

Tenha um antivírus e um *antispyware* instalado em seu computador e mantenha-os sempre atualizados. Ainda é muito comum pessoas desconhecerem as ações de um vírus e de um *spyware*. O vírus atua de forma danosa diretamente no seu computador, seja apagando arquivos, seja alterando o funcionamento das aplicações, seja danificando o sistema operacional. Já o *spyware* atua de forma mais silenciosa, coletando informações do usuário sem ser percebido ou sem ter permissão. O vírus infecta seu computador através de arquivos executáveis, com extensões do tipo *.exe*, *.sys*, *.dat*, *.doc*, *.xls*, *.com*, etc. A invasão do *spyware* ocorre através do acesso a sites não confiáveis, programas de compartilhamento de arquivos ou de música, jogos gratuitos, dentre outros. Dispositivos de mídia como *pen drive* é a forma mais comum de transmissão de vírus e *spyware*. Faça um "*scan*" sempre que for utilizá-lo.

A maneira correta de evitar as duas "pragas" é, primeiramente, ter instalado no computador um bom *software* antivírus e um *antispyware*, mantendo-os sempre atualizados.

Atualização do sistema

Sempre que possível, instale as mais recentes atualizações e pacotes de segurança ao seu sistema operacional. Existem, no mercado, diversos sistemas operacionais para computadores *desktops*; os mais comuns são: o *Windows*, o *Linux* e o *Mac OS*. Quando uma falha no sistema operacional é descoberta, grande número de pragas digitais é criado para explorar a deficiência. O *Windows*, até por ser o mais comumente utilizado, é a vitima preferida. Mas para usuários do *Linux* e *Mac OS*, isso também é válido, pois falhas de segurança não são prerrogativas somente do *Windows*, e todos os desenvolvedores disponibilizam atualizações periodicamente, sendo ainda muito comuns ferramentas embutidas no sistema operacional para auxiliar nessa tarefa. Tente fazer atualização semanal.

Utilização do *firewall* pessoal

Uma barreira de proteção inicial para seu sistema. *Firewalls* são programas que têm por finalidade filtrar ou bloquear todos os acessos que entram ou que saem de uma rede através de regras pré-configuradas no computador que realiza a proteção. O *firewall* pode ser configurado em um servidor de uma rede de computadores e/ou em um computador pessoal.

No caso de um computador pessoal, é altamente recomendável deixar o *firewall* ativado, para fornecer um nível a mais de proteção.

Cuidados com uso de comunicadores instantâneos

Existem diversos comunicadores instantâneos disponíveis, como: *Windows Live Messenger*, *Google Talk*, *AIM*, *Yahoo Messenge*r. A melhor proteção é não utilizá-los em ambiente corporativo.

Todos eles disponibilizam formas de distribuição de arquivos e outros tipos de mídia, como som e imagem. Mesmo sem saber, o usuário pode estar distribuindo arquivos com vírus ou *spyware* para seus contatos.

É muito comum encontrar computadores infectados com um tipo de vírus que utiliza esse meio de comunicação para se propagar de forma silenciosa. Por isso, se durante uma conversa, receber um *link* ou arquivo inesperado, confirme com o contato se ele realmente enviou e qual o objetivo dele. O ideal é não receber arquivos ou clicar em *links*, mesmo de remetentes confiáveis.

Cuidados no uso do *e-mail*

Recebeu um *e-mail* dizendo que você tem uma dívida com uma empresa de telefonia ou afirmando que um de seus documentos está ilegal? Ou, ainda, a mensagem lhe oferece prêmios ou cartões virtuais de amor? Intima você a uma audiência judicial? Contém uma suposta notícia importante sobre uma personalidade famosa? É provável que se trate de um *spam*, ou seja, um falso *e-mail*. Se a mensagem tiver textos com erros ortográficos e gramaticais, se fizer ofertas tentadoras ou ter um *link* diferente do indicado (para verificar o *link* verdadeiro, basta passar o *mouse* por cima dele, mas sem clicar), desconfie imediatamente. Na dúvida, entre em contato com a empresa cujo nome foi envolvido no *e-mail.*

A seguir, são informadas outras dicas para *e-mail*:

- Não abra *e-mails* cujo remetente não seja conhecido.
- Verifique sempre o endereço do remetente antes de abrir qualquer *e-mail*.
- Não responda a *e-mails* não autorizados.
- Faça sempre um *scan* com antivírus no anexo.
- Ao enviar *e-mail* particular, não divulgue as suas informações pessoais em sua assinatura digital, ou seja, na seção no final de cada *e-mail* de saída.
- Quando enviar e-mail para mais de uma pessoa, utilize cópia oculta (CCo) para não disponibilizar mais endereços de *e-mail* sem necessidade.

Realização de *backup* de pastas e arquivos importantes

Faça *backup* de tudo. Todo computador tem algum nível de vulnerabilidade. Atualmente as possibilidades de mídias disponíveis para tal tarefa são muitas, entre CDs, DVDs, disco rígido removível ou até mesmo outra máquina segura na rede de dados. O importante é saber escolher o método mais apropriado e fazê-lo de modo seguro. Vale ainda salientar que um *backup* não é uma tarefa tão trivial, pois realizado de forma incorreta ou em mídia inapropriada, poderá não valer de nada seu esforço ao descobrir, na hora de restaurar os dados, que foi feito de maneira errada ou que a mídia está danificada. Por isso, no caso de dúvidas quanto à forma de gravação ou ao uso e manuseio dessas mídias, peça auxílio da equipe de suporte ou de um usuário mais experiente.

Não deixe seu *login* aberto

Um dos mandamentos básicos da segurança de sistemas de computador é nunca compartilhar senha com outras pessoas. A inobservância disso pode trazer muitos transtornos a quem comete tal deslize, pois como alguém poderá provar que não foi o responsável por realizar certa transação, como poderá provar que não enviou e-mail indevido ou mesmo que apagou arquivos ultraimportantes? Da mesma maneira que o problema anterior, estaremos repetindo os erros se também deixarmos o login aberto em qualquer serviço da internet (*Home Banking*, *e-mail*, etc.). Então, sempre tome o cuidado de se desconectar dos serviços, através de botões/*links* de Desconectar, Sair ou *Logoff*. O simples uso desse procedimento deixa a porta fechada para qualquer tentativa de invasão por parte de pessoas inescrupulosas.

Cuidado ao instalar programas baixados da *internet*

Muitos sites da internet oferecem arquivos para ser instalados em sua máquina. Cuidado! Não instale nada sem antes perguntar a alguém com mais conhecimento, pois muitos arquivos carregam vírus ou programas espiões. Só instale programas de fontes confiáveis, das quais conheça o funcionamento e que realmente sirva para os seus propósitos. Os sites que mais infectam computadores são aqueles voltados à pornografia, e que têm conteúdo *hacker* por tratarem de temas que despertam muito interesse das pessoas. Portanto, não acesse sites de conteúdos duvidosos e solicitados por pessoas desconhecidas.

Proteja-se contra *spyware*

O seu navegador da *Web* foi invadido por anúncios em forma de *pop-ups*? Há barras de ferramentas em seu computador que você não baixou? Você pode ser uma vítima de *spyware*, que é o *software* que coleta suas informações pessoais sem que você saiba ou sem pedir permissão para

isso. Você pode instalar *spyware* em seu computador inconscientemente ao baixar: programas de compartilhamento de arquivos ou de música, jogos gratuitos de sites não confiáveis ou outros programas de sites suspeitos.

Tome precauções ao usar conexão sem fio

Hoje, há diversos lugares com redes sem fio. Isso significa que você pode navegar pela *Web* na biblioteca, na cantina ou no shopping. Você pode já ter usado redes sem fio em casa, em aeroportos, cafés ou mesmo em parques públicos. Essas redes são convenientes, mas implicam um risco à sua segurança. Se você configurou sua própria rede sem fio em casa, no trabalho ou até na sua residência, proteja sua rede *Wi-Fi*, habilite o *WPA* com uma senha de, pelo menos, 20 caracteres. Em seu *notebook*, só acesse redes *Wi-Fi* que tenha proteção *WPA*.

Manutenção corretiva de equipamentos de TI

Os computadores *desktops*, *switches* de rede e os roteadores de uma rede também precisam receber manutenção preventiva, com atualização dos *softwares* (sistema operacional, antivírus, antispam, etc.), além disso o *hardware* também precisa de atenção especial, pois muitos equipamentos não podem funcionar com as versões dos sistemas mais atuais e seguros por terem periféricos que não suportam as últimas tecnologias do mercado, sendo obrigados a permanecerem com sistemas antigos cheios de falhas já conhecidas dos *hackers*.

Por isso, realizar manutenção corretiva, e quando necessário substituir os equipamentos defasados, ajuda a prevenir problemas com segurança da informação.

Segurança de servidores

Os servidores de dados de uma rede são aqueles que armazenam e/ou processam informações de toda uma rede corporativa, neles normalmente são centralizadas as informações que trafegam pela rede e dela para fora. Portanto, ter uma equipe de TI bem capacitada, com competência para atuar nesse segmento, é imprescindível, pois um servidor desatualizado ou mal configurado é uma porta de entrada para um *hacker*. Agora imagine, se a rede de computadores de sua organização, que talvez possua uma quantidade enorme de dados sigilosos e/ou críticos, for invadida por um *hacker*, e isso ocorrer justamente por meio de um dos servidores de rede, seria como colocar o bandido direto na sala do cofre de um banco, sem que ele tenha de passar por nenhum outro mecanismo de segurança.

Proteção à propriedade no contexto da segurança da informação

A importância da proteção dos ativos intangíveis das empresas

O atual ambiente de concorrência e liberalização comercial, o progresso científico e tecnológico e as estratégias adotadas pelas empresas de sucesso baseiam-se cada vez mais na proteção da propriedade intelectual e industrial. Hoje, muitas empresas de renome têm seu maior ativo financeiro na sua marca e no conhecimento técnico de sua equipe, o patrimônio intelectual, e não no seu patrimônio físico (máquinas e equipamentos). O conhecimento assumiu o papel de ativo intangível, bastante valorizado mundialmente, e, nesse contexto, a proteção da propriedade intelectual tornou-se um indicador de desempenho da apropriação econômica resultante do esforço inovador.

Portanto, assim como se protegem prédios e bens móveis com rígida segurança, ativos como marcas, conhecimento, técnicas e práticas devem ser protegidos, a fim de manter tais valores na empresa. Essa proteção não foca o cerceamento do conhecimento, mas sim a preservação dos bens intangíveis, como questão fundamental da Gestão do Conhecimento e da Segurança da Informação.

A propriedade intelectual trata da proteção concedida às criações resultantes do espírito humano, seja de caráter científico, industrial, literário ou artístico. Apresenta duas divisões:

- **Propriedade industrial:** patentes de invenção, patentes de modelos de utilidade, desenhos industriais, indicações geográficas, registro de marcas e proteção de cultivares;
- **Direito autoral:** obras literárias, artísticas e científicas, programas de computador, topografias de circuito integrado, domínios na Internet e cultura imaterial.

Orientações gerais para funcionários

- Não é permitido modificar, reproduzir, armazenar, transmitir, copiar, distribuir ou utilizar informações corporativas para fins comerciais, por qualquer que seja a forma, sem o prévio e formal consentimento da empresa.
- Não é permitido disponibilizar textos, imagens, sons e aplicativos exibidos em sites das empresas, por qualquer que seja a forma, sem o prévio e formal consentimento, pois estes são protegidos por direitos autorais.

- As marcas da empresa e de seus produtos e serviços, registradas no Instituto Nacional de Propriedade Industrial (INPI), são de propriedade dela e, portanto, é proibido adulterá-las e/ou copiá-las sem a autorização expressa da empresa proprietária.
- Tentativas de invasão nos sites das empresas, ou nos sites a elas relacionadas, poderão ser entendidas como atitudes ilícitas, sob o ponto de vista da legislação civil e penal em vigor.
- Os usuários/visitantes de sites das empresas não devem, sob pena da legislação em vigor, utilizar conteúdo desses sites com finalidade comercial de venda de serviços; modificar, alugar, vender, distribuir ou criar obras derivadas de aplicativos e de serviços, no todo ou em parte, disponíveis nos sites; reproduzir, duplicar, copiar ou explorar, com finalidade comercial, qualquer parte dos aplicativos, dos serviços ou dos produtos oferecidos nos sites.
- O funcionário deve comunicar imediatamente à empresa uma nova invenção no processo de trabalho.
- A invenção produzida pelo empregado no processo de trabalho pertence à empresa, portanto cabe a ela decidir sobre a oportunidade de investir em proteção ou divulgar a informação.
- O funcionário não deve transmitir a terceiros, sem o consentimento formal da empresa, informações sobre processos de trabalho, atividades que estejam sendo planejadas ou executadas, ou qualquer outra informação, evitando assim o risco de divulgar informações estratégicas para a empresa que venham a incorrer em prejuízos morais ou financeiros.
- Recomenda-se que o funcionário não cite a empresa ou informações internas em *sites* pessoais, *e-mails* pessoais, sites de relacionamento e até mesmo ao telefone.
- O uso do *e-mail* corporativo exige cautela, a fim de que informações sigilosas não caiam em domínio público.

Orientações gerais para as empresas

Objetivando garantir a segurança das informações, a empresa deve:

- Proteger as informações contidas em seus sites, em conformidade com leis e normas que regulamentam direitos autorais, marcas registradas e patentes.
- Realizar análises de idoneidade pessoal e profissional no processo de seleção de funcionários/colaboradores.

- Definir uma política onde os colaboradores/funcionários assinem contrato de confidencialidade/termo de sigilo no momento de sua contratação.
- Orientar os funcionários quanto à manutenção de registros das atividades, principalmente quando se tratar de trabalhos que envolvam experimentações, em laboratórios ou campos.
- Realizar treinamentos focados em segurança da informação para funcionários e terceiros.
- Estabelecer uma política de devolução de ativos e solicitação da remoção dos acessos no momento de desligamento de funcionários e de terceiros.
- Esclarecer formalmente aos empregados e gerentes o que pode ser compartilhado e o que deve ser protegido para garantir os negócios e evitar litígios.
- Criar normas internas referentes à Propriedade Intelectual e à Transferência de Tecnologia.
- Definir as condições para atribuição da titularidade das invenções, dos modelos de utilidade, dos desenhos industriais e de outras criações sujeitas à proteção.
- Proporcionar os contatos e a intermediação das cooperações entre funcionários e o setor interessado.
- Promover a proteção de invenções e modelos de utilidade, do registro de marcas, do registro de desenhos industriais e do registro de direitos autorais, em âmbitos nacional e internacional.
- Proteger tecnologias por segredos de negócios, assinaturas de termos de sigilo e patentes.
- Identificar os documentos sigilosos de forma clara e evidente, enumerar as cópias (se houver), e guardá-los em local seguro, trancado, em área de acesso restrito.
- Documentos importantes ou com informações estratégicas não devem ser jogados em lixo comum, e sim destruídos. Recomenda-se o uso de picotadoras de papel ou incineração.
- A empresa deve adotar sistemas de trabalho em que o menor número de pessoas possível tenha acesso a informações sigilosas. Deve-se aplicar marca temporal aos registros eletrônicos, em servidor de acesso restrito.

- Nos sistemas informatizados, recomenda-se o uso de sistema de registro e armazenagem que não permita alteração posterior dos registros realizados.
- Monitorar os casos de uso não autorizado por terceiros dos direitos de Propriedade Intelectual da instituição, com previsão de pronta repressão a essas ações.
- Promover o marketing, a negociação e a exploração econômica da Propriedade Intelectual.
- As ações de transferência de tecnologia, bem como as de cooperação entre a empresa e seus parceiros, devem ser precedidas de celebração de instrumentos contratuais, que estabeleçam claramente questões sobre o direito de posse das tecnologias/conhecimentos em questão, bem como cláusulas sobre distribuição dos recursos auferidos e previsão de penalidades para caso de infração contratual.
- Distribuir, com os inventores, os proventos obtidos com a exploração econômica da Propriedade Intelectual.
- Disseminar os conceitos do sistema de Propriedade Intelectual na empresa.
- Gerir os processos relativos à proteção de direito, instituindo um setor de Propriedade Intelectual, com Agentes de Propriedade Industrial, com formação técnica em Engenharia, Física, Química, Ciências Biomédicas ou Direito. Essa profissão é regulamentada pelo Decreto-Lei nº 8.933, de 26/1/46 e pela Portaria nº 32, de 19/4/98.
- Dar suporte aos funcionários/pesquisadores nos processos de patenteamento ou registro de produtos e processos decorrentes de pesquisas.
- Implementar políticas e diretrizes relativas à propriedade intelectual e à inovação tecnológica.
- Decidir quanto à conveniência de divulgação das criações desenvolvidas na empresa, passíveis de proteção intelectual.
- Assegurar proteção ao seu patrimônio intelectual.

Visão geral sobre contratos: proteção do conhecimento e segurança da informação

No texto abaixo, estão listados os principais instrumentos jurídicos que devem ser estabelecidos pelas empresas nas contratações de pessoal e ações de parceria/transferência de tecnologias, com vistas ao resguardo do conhecimento e das tecnologias geradas pela organização. Além das cláusulas habituais (preâmbulo, identificação das partes, objeto do contrato,

vigências, obrigações, penalidades, foro), é de suma importância a inserção de cláusulas referentes à segurança da informação e propriedade intelectual, descritas para cada tipo de contrato.

- **Acordos de Estágio** – Contrato estabelecido para a empresa receber estudantes na categoria de estagiários, visando à complementação da formação educacional dos estudantes. Devem constar as cláusulas de acesso às instalações e uso dos resultados.
- **Acordo de Confidencialidade** – Utilizado quando a empresa necessita informar detalhes de tecnologias para terceiro, interessado no licenciamento. Previne a empresa contra o risco de apropriação do conhecimento por parte do terceiro envolvido.
- **Acordo de Transferência de Material Biológico** – O acordo permite controlar o uso do material biológico transferido de uma instituição à outra.
- **Contratos de Direitos de Co-titularidade** – Objetiva que as partes estabeleçam as condições sobre os procedimentos acerca dos resultados protegidos oriundos de pesquisas realizadas em conjunto. Devem constar cláusulas sobre: o percentual de co-participação, obrigações e deveres de cada uma das partes.
- **Contratos de Pesquisa e Desenvolvimento** – Tem por objetivo a execução conjunta de projetos para o desenvolvimento de novos produtos/processos. Também chamados de contratos de cooperação técnica.
- **Contratos de Transferência de Know-How** – Instrumento formalizado quando uma pessoa, física ou jurídica, concede ao contratante a fruição do direito que ela possui sobre certos conhecimentos, secretos ou não, durante um período de tempo estabelecido, sob a condição de pagamento.
- **Contratos de Licenciamentos** – Objetiva o licenciamento de patente requerida ou concedida junto aos órgãos competentes do País (INPI) ou do exterior. Deve estabelecer se a licença será do tipo cessão (venda) ou concessão de licença a terceiro, para que este explore o objeto desta. Ainda, cláusula sobre a exploração do privilégio, ou seja, se a licença será exclusiva ou não exclusiva e se a subcontratação é admitida.
- **Contrato de Uso de Marca** – Autoriza o uso, por terceiros, de marca regularmente depositada ou registrada no País, respeitando-se o disposto nos Artigos 139 e 140 da Lei n° 9.279/96. Deve constar a caracterização completa da marca, cláusula sobre a exclusividade ou não da licença e da permissão ou não para sublicenciar.

- **Contrato de Fornecimento de Tecnologia** – Utilizado quando a empresa vai adquirir conhecimentos e/ou técnicas não amparados por direitos de Propriedade Industrial depositados ou concedidos no Brasil. Importante mencionar no contrato a identificação completa do produto e do setor em que será aplicada a tecnologia.

- **Contrato de Franquia** – São contratos amplos, que estabelecem as condições para a empresa ceder a terceiros o direito de utilizar seus procedimentos operacionais padrão, sua marca e demais aspectos relacionados a um produto ou serviço. É um tipo de contrato de transferência de tecnologia. Deve especificar as taxas de franquia, *royalties* e de publicidade. Especificar também se a franquia será exclusiva ou se é permitido subfranquear.

- **Termo de Compromisso de Confidencialidade e Outras Avenças** – Contrato firmado, no ato da contratação de funcionários e estagiários, visando a estabelecer regras claras para atuação do contratado na empresa. Deve constar uma lista de obrigações que o contratado deverá respeitar enquanto da vigência do contrato de trabalho/estágio.

A seguir, exemplos de cláusulas contratuais voltadas para a proteção do conhecimento da empresa:

Do acesso às instalações
O acesso à infraestrutura e às instalações da empresa pelo(a) estudante/funcionário/colaborador será o estritamente necessário à execução das atividades objeto do estágio, observada a regulamentação interna da empresa.

Dos resultados
A exploração, a qualquer título, dos resultados dos trabalhos realizados pelo(a) estudante, privilegiáveis ou não, pertencerá automática e exclusivamente à empresa.

Propriedade Intelectual
Qualquer invento, aperfeiçoamento ou inovação tecnológica, obtenção de produto ou processo, privilegiável ou não, adquirido, produzido, transformado ou construído ou em construção, oriundos da execução deste Convênio, inclusive direito de exploração econômica de obras científicas ou literárias, pertencerão à empresa.

Obrigações do contratado
Observar a regulamentação interna da empresa sobre ingresso e permanência em suas dependências; utilizar a infraestrutura da empresa

estrita e exclusivamente para fins de complementação das condições indispensáveis para a condução do seu trabalho; não acessar quaisquer arquivos ou bases de dados de informações da empresa, sob qualquer pretexto, sem expressa autorização.

Confidencialidade
O contratado/cooperante compromete-se a manter total reserva em relação a quaisquer dados ou informações da empresa que venha porventura ter acesso em razão de seu trabalho, não utilizando-os para interesse próprio ou de terceiros, nem repassando-os a terceiros sob qualquer forma ou pretexto, independentemente de se tratar ou não de informação reservada, confidencial ou sigilosa, mesmo após a extinção do presente Termo.

As partes responsabilizam-se, por si e por seus empregados ou prepostos a qualquer título, quanto à manutenção de absoluto sigilo sobre qualquer dado ou informação técnica – pertinente à utilização da tecnologia ora negociada – bem como sobre demais informações reservadas, referentes à execução deste Contrato.

Aplicações de uso

O material aqui apresentado foi elaborado com o objetivo de auxiliar gestores e colaboradores na implementação das boas práticas em segurança da informação dentro de uma organização.

A segurança da informação precisa ser um processo contínuo e fazer parte da rotina de todos os colaboradores, no qual exista a preocupação com o acompanhamento das ações, através de auditorias rotineiras aplicando avaliações objetivas e subjetivas com base em modelos de controle de qualidade.

Mas, além de aplicar bons conceitos em prática, é preciso institucionalizar a questão da segurança da informação. A melhor forma de se fazer isso é implantando uma política de segurança da informação.
A política de segurança da informação é um processo interno que deve ser pensado e discutido por um grupo bem representativo das mais diversas áreas da empresa, com participação ativa da direção e apoiada nas normas atuais e legislações vigentes. Nesse contexto, é indispensável a leitura das seguintes normas:

- **ABNT NBR ISO/IEC 27002:2005** – Código de prática para a gestão da segurança da informação;
- **ABNT NBR ISO/IEC 27001:2006** – Sistemas de gestão de segurança da informação – Requisitos;

- **BBS 7779** – British Standart 7799 – Norma padrão de segurança da informação, desenvolvida em 1995 na Inglaterra.

Considerações finais

Para pensar em Segurança da Informação é preciso ter mente aberta a novos preceitos e à quebra de paradigmas. O conceito de Segurança da Informação é muito amplo e abrange, mesmo que de forma implícita, todos os segmentos de uma organização.

Percebe-se que só é possível a implantação dos conceitos e cuidados descritos neste trabalho com a participação e o engajamento de todos os colaboradores de uma organização, abrangendo as mais diversas áreas da empresa desde a alta direção até a escala mais baixa do organograma, incluindo os prestadores de serviços e estagiários.

A Segurança da Informação deve ser realizada de forma completa, levando em consideração todos os controles descritos pela norma ABNT ISSO/IEC 27001:2006, pois qualquer descuido pode afetar a cadeia por completo.

Quando inicia-se um processo de implantação de Segurança da Informação, não é viável que se faça de forma parcial, pois, assim, deixaria de pertencer ao conceito de Segurança da Informação e passaria a atuar isoladamente.

O processo de implantação de Segurança da Informação deve ser gerenciado por grupos de pessoas com as mais diversas competências e linhas de atuação. O grupo deve ser democrático e ao mesmo tempo firme, destemido em suas decisões, com capacidade para realizar um processo de melhoria contínuo, e que todos entendam ser parte do modelo de gestão e segurança da empresa.

Este trabalho aborda uma gama relativamente grande de áreas de atuação de Segurança da Informação, mas não é completo, faltam outras áreas também importantes como: análise de risco, gestão de comunicação, gerenciamento de serviços terceirizados, manutenção em sistemas de informação, gestão de continuidade do negócio, e, ainda, leis e normas internacionais.

Almeja-se que os tópicos abordados neste trabalho possam auxiliar todos os que objetivem iniciar um trabalho em Segurança da Informação, com noções gerais nas áreas de atuação aqui abordadas.

Referências

ALMEIDA, A. E. de G. **A importância da segurança patrimonial na segurança da informação. 2005**. Disponível em: <http://www.help-info.com.br/news_artigo_esdras.htm>. Acesso em: 17 abril 2009.

ARAÚJO, E. E de. A vulnerabilidade humana na segurança da informação. Uniminas, Uberlândia -MG, 2005, 95 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2006**: Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação – requisitos. Rio de Janeiro, 2006. 34 p.

ATHENIENSE, A. **Conheça os 8 erros de segurança que os usuários mais cometem nas empresas**. Disponível em: <http://www.dnt.adv.br/noticias/dicas/conheca-os-8-erros-de-seguranca-que-os-usuarios-mais-cometem-nas-empresas/>. Acesso em: 10 abril 2009.

BANCO SANTANDER. **Segurança**: principais itens. Disponível em: <http://www.santander.com.br/document/gsb/seguranca_parceiros_principais_itens.pdf>. Acesso em: 28 abril de 2009**.**

COELHO, F. E. S. **SEG-005**: Gestão da segurança da informação. Rio de Janeiro: Escola Superior de Redes RNP, 2007. 276 p.

EMBRAPA. Assessoria de Inovação Tecnológica. **Parecer nº 018/09**. Estratégias para proteger o direito de propriedade intelectual da Embrapa sobre as criações intelectuais geradas no âmbito de seus projetos de pesquisa. Brasília, DF, 11 de fevereiro de 2009. 41 p.

EXPORTAÇÃO de informações deixa as empresas vulneráveis. Segurança Gestão. Disponível em: <http://www.computerworld.com.pt/site/content/view/6337/40/>. Acesso em: 28 abril de 2009.

POLÍTICA de privacidade e condições de uso dos sites da Embrapa. Disponível em: <http://www.cppse.embrapa.br/politica#5>. Acesso em: 28 de abril 2009.

POLÍTICA de propriedade intelectual e transferência de tecnologia. Disponível em: <http://www.prppg.ufpr.br/documentos/pesquisa/npi/Politica%20de%20PI%20e%20TT.pdf>. Acesso em: 28 abril de 2009.

RESOLUÇÃO Univ. nº 27 de junho de 2008. Disponível em: <https://sistemas.uepg.br/producao/reitoria/documentos/1272008-06-20.pdf>. Acesso em: 28 abril de 2009.

SÊMOLA, M. **Conheça os 10 erros fatais em projetos de segurança**. Disponível em: <http://74.125.47.132/search?q=cache:213cKIA7MEUJ:pucrs.campus2.br/~annes/projetos_segur.doc+seguran%C3%A7a+da+informa%C3%A7%C3%A3o+erros&cd=9&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 10 abril 2009.

SÊMOLA, M. **Estratégia de segurança: o jogo dos 7 erros**. Coluna Firewall IDGNow, 29 fev. 2001. Disponível em: <http://198.106.31.168/disco/Coluna_IDGNow_29.pdf>. Acesso em: 10 abril 2009.

SILVA FILHO, A.M. **Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações.** Revista Espaço Acadêmico nº 43 Dez 2004, mensal, ano IV. Disponível em <http://www.espacoacademico.com.br/arquivo/silvafilho.htm> Acesso em: 08 de maio 2009.

UNIVERSIDADE FEDERAL DO PARANÁ. Pró-Reitoria de Pesquisa e Pós-Graduação. **Manual de contratos de propriedade industrial e de transferência de tecnologia.** Curitiba, 2005. 35 p. Disponível em: http://www.prppg.ufpr.br/documentos/pesquisa/npi/Manual%20Propriedade%20Industrial.pdf. Acesso em: 28 abril de 2009.

Embrapa
Amazônia Ocidental

Ministério da
Agricultura, Pecuária
e Abastecimento

BRASIL
UM PAÍS DE TODOS
GOVERNO FEDERAL