A SEGURANÇA DA INFORMAÇÃO
COMO POLÍTICA INTERNA DE SEGURANÇA

A C S Magalhães[1]

A polêmica nos últimos dias com relação às denúncias feitas por Edward Snowden[2] sobre a espionagem desencadeada pelo governo americano em comunicações e tráfego de informações em vários países do mundo tem produzido desconfiança e medo em grande parte da população global, uma vez que, as conversações, publicações, postagens ou buscas de dados nos meios digitais são práticas muito constantes pela maioria das pessoas. O Ibope[3], conforme matéria publicada pela Folha de São Paulo[4] em 09 de julho de 2013 informa que 102,3 milhões de pessoas acessam internet no Brasil. Essa rede leva o individuo a um vasto mundo virtual com infinitos dados e informações disponíveis para uso conforme interesse da cada usuário. Programas e aplicativos criados com a ideia de proporcionar uma eficaz utilização das redes sociais acabam por expor informações sensíveis referentes aos usuários e aos locais de onde acessam para todo o mundo.

A presidente brasileira, em entrevista publicada pela Revista Veja On-line[5], em 08/07/2013 expressou claramente o descontentamento da Nação com tais atos, sendo peremptória na declaração de que seja um desrespeito aos direitos humanos e violação à soberania nacional, exigindo explicação do presidente americano sobre tais denúncias.

É notória a preocupação social com a segurança pública, muito em função dos altos índices de criminalidades evidenciados e muito difundidos pela imprensa escrita e televisada, porém no entendimento genérico de segurança pública quase ninguém se refere à segurança das informações como um ramo importante da segurança cidadã, ideia que tem sido mudada em razão das noticias veiculadas na imprensa sobre a espionagem e a invasão de privacidade americana. Em reportagem de Rubem Valente (apud Folha de São Paulo, loc.cit.), o governo brasileiro já reconheceu por duas vezes, em 2001 e em 2008, que os EUA comandavam um sistema de coleta de informações que tinha

[1] Policial Militar do Estado da Bahia, ex-comandante da unidade de operações especiais, especialista em operações especiais em áreas de Montanhas, Fronteiras e Limites por Carabineiros do Chile; em Táticas Especiais de Polícia e em Inteligência Estratégica; pós-graduado em Gestão Social e Cidadania pela Universidade do Estado do Pará e Mestre em Planejamento de Territórios pela Universidade Católica do Salvador.

[2] Edward Joseph Snowden, técnico em segurança da informação, ex-analista da Agencia de Segurança Nacional dos Estados Unidos da América, nascido em 1983, em Elizabeth City, Carolina do Norte, EUA.

[3] Ibope - Instituto Brasileiro de Opinião Pública e Estatística

[4] Disponível em http://f.i.uol.com.br/folha/mundo/images/13191513.jpeg

[5] http://veja.abril.com.br/noticia/brasil/dilma-quer-que-onu-discuta-monitoramento-feito-pelos-eua

capacidade de "intromissão eletrônica" em todo o mundo. Segundo ele, em depoimento prestado em 2001 à Câmara dos Deputados, o então ministro do Gabinete de Segurança Institucional (GSI) da Presidência da República, general Alberto Cardoso, disse aos parlamentares que os EUA desenvolveram um projeto, com o nome código de Echelon, em associação com o Reino unido, Irlanda, Austrália, Canadá e Alemanha, que tinha capacidade de interceptar comunicações por e-mail e fac-símile, o que já torna evidente a espionagem americana há muito tempo.

Essa vigilância adversa, entretanto está voltada principalmente para os metadados[6], ou seja informações uteis para identificar, localizar, compreender e gerenciar os dados. Essas informações são geradas quando uma pessoa usa um dispositivo tecnológico para comunicações, armazenamentos o transmissões de dados, expondo sem se dar conta informações tais como endereços de e-mail e IP do remetente e do destinatário, data, hora, tipo de conteúdo se texto, imagem, vídeo e devida codificação, assunto etc., bem como nas comunicações telefônicas o número de quem realiza e de quem recebe a chamada, hora, duração e localização dos equipamentos; para os sites de relacionamento do tipo facebook e twitter capta o perfil do usuário e os dados inerentes a ele, lançados por ocasião da criação da conta, bem assim status, assuntos pesquisados e resultados das pesquisas no caso do Google[7].

Diante de tais evidencias de invasão de privacidade noticiadas, inclusive pelo jornal O Globo na versão on-line de 07 de julho de 2013[8], surge a necessidade de que cada um, instituição ou indivíduo, tenha uma maior preocupação com uma política eficiente e eficaz de segurança das informações produzidas, capitadas ou disponibilizadas por meio do computador. Assim, busca-se aqui sugerir um padrão básico de política de segurança da informação que deve ser colocada em prática principalmente nos órgãos e instituições públicas, cuja preocupação com a segurança orgânica comumente passa despercebida.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Uma Política de Segurança da Informação é definida como documento que orienta e estabelece as diretrizes corporativas de uma Instituição (FERREIRA, 2008), pública ou privada, com a finalidade de proteger seus ativos de informação e prevenir sobre a responsabilidade legal para todos os usuários dessas informações. Representa

[6] Disponível em http://www.metadados.ibge.gov.br

[7] Multinacional americana de serviços online e software. Hospeda e desenvolve uma série de serviços e produtos baseados na internet. Informação disponível em: http://www.significados.com.br/google/

[8] Disponível em: http://m.g1.globo.com/mundo/noticia/2013/07/brasil-foi-alvo-de-espionagem-dos-eua-diz-o-globo.html

segundo Moreira (2001, p. 31) um conjunto de procedimentos a serem adotados com o intuito de reduzir probabilidades de ocorrências de ameaças ou riscos, uma vez que se o nível de segurança cresce, o nível de vulnerabilidade decai. Assim, deve ser cumprida e aplicada em todas as áreas do órgão.

Deve ter como base as recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005 reconhecida mundialmente como código de prática para a gestão da segurança da informação, e as leis em vigência no Estado Brasileiro.

Para efeito de aplicação de uma Política de Segurança da Informação, entende-se por:

- Segurança: sensação de bem-estar, de proteção a riscos, perigos e perdas.
- Segurança Orgânica: definida como aquela que objetiva minimizar riscos e ameaças ao bom desenvolvimento de uma instituição e visa à proteção do órgão, seja ele público ou privado, de ações adversas que possam dificultar ou impedir a consecução de seus objetivos[9].
- Informação: todo dado processado ou não, que pode ser utilizado para produção e transmissão de conhecimentos contidos em quaisquer meios, suporte ou formato (Lei 12.527 de 18 Nov. 2011, Art. 4º, Inciso I). É recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado.
- Segurança da Informação: conjunto de medidas, normas e procedimentos destinados a garantir a integridade, disponibilidade, confidencialidade e autenticidade da informação em todo o seu ciclo de vida.
- Arquitetura de Segurança da Informação: conjunto composto pelos elementos fundamentais de um sistema de segurança concebido para proteger informações e definido com base em criteriosa análise de riscos de uma organização. Dentre tais elementos destacam-se: a documentação normativa; as infraestruturas de gerência, auditoria e validação; as medidas contingenciais e um programa de

[9]http://www.webartigos.com/_resources/files/_modules/article/article_106872_201304131613180faa.pdf

conscientização dos recursos humanos[10].

- Medidas de contingências: ações que visam prover meios alternativos para tornar efetivo(s) e eficaz(es) o(s) processo(s) de produção, sem sofrer descontinuidade.
- Informação Sigilosa: aquela submetida temporariamente a restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado. São passíveis de restrição, dentre outras, as informações cuja divulgação ou acesso irrestrito possam comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações[11].
- Custodiante: aquele que detém a guarda da informação.
- Internet: rede mundial de computadores que possibilita o acesso a informações sobre e em qualquer lugar do mundo[12].
- Intranet: rede privada de computadores que assenta sobre protocolos da Internet, porém, de uso exclusivo de um determinado local, órgão ou instituição. É uma rede de computadores semelhante à Internet, porém de uso exclusivo de uma determinada organização[13].

[10] IG 20-19 disponível em: www.3cta.eb.mil.br/download/ig_20_19.pdf
[11] Lei 12.527 de 18 Nov 2011, Art 23, Inciso VII.
[12] http://www.significados.com.br/internet/

OBJETIVOS

Estabelecer diretrizes que permitam aos funcionários, colaboradores e público externo da instituição seguirem padrões de comportamento relacionados à segurança da informação, adequados às necessidades de proteção legal do órgão e dos indivíduos.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações do órgão quanto aos princípios essenciais da Autenticidade, Integridade, Confidencialidade e Disponibilidade.

APLICAÇÕES DE UMA POLITICA DE SEGURANÇA DA INFORMAÇÃO

As diretrizes estabelecidas deverão ser seguidas por todos os funcionários e colaboradores, bem como os prestadores de

[13] http://www.brunorusso.eti.br/documentacao/O_que_e_a_Intranet.pdf

serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política visa dá ciência a cada funcionário ou colaborador de que os ambientes, sistemas, computadores e redes do órgão poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada funcionário ou colaborador manter-se atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação de seu Encarregado, Coordenador, Chefe ou Diretor, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Toda informação produzida ou recebida pelos funcionários ou colaboradores como resultado da atividade profissional de uma instituição. Pertence ao referido órgão deverá está pautada nos princípios da:

- Autenticidade: garantia de que a mensagem é procedente da origem informada no seu conteúdo;
- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

As exceções devem ser comunicadas imediatamente ao Chefe correspondente e formalizadas explicitamente e por escrito ao Diretor da instituição ou órgão.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos funcionários ou colaboradores para a realização das atividades do órgão. O uso pessoal dos recursos somente será permitido se não houver prejuízo no desempenho dos sistemas, atividades e serviços, mediante autorização do Chefe responsável.

REQUISITOS DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para a uniformidade da informação, uma Política de Segurança da Informação deverá ser comunicada a todos os funcionários e colaboradores do órgão a fim de que seja cumprida dentro e fora dele.

Deverá haver um comitê multidisciplinar (com funcionários das mais diversas áreas da instituição ou órgão) responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação.

Tal política deverá ser revista e atualizada periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Para que haja o acesso às informações produzidas pelo órgão o interessado deverá assinar um Termo de Confidencialidade ou declarar conhecer a Cláusula de Confidencialidade intrínseca ao órgão.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de seleção do funcionário ou colaborador. Todos os funcionários e colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Chefia à qual estiver subordinado o funcionário e, após análise deste, à Direção para medidas protetivas julgadas convenientes.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo semestralmente, visando reduzir riscos de perda de autenticidade, confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que o órgão julgar necessário para reduzir os riscos dos seus ativos de informação, a exemplo das estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico e nos sistemas outros em exercício na instituição.

Os ambientes de produção de conhecimento devem ser separados e rigidamente controlados, garantindo a compartimentação necessária tanto em relação aos ambientes físicos como dos dados.

A instituição exonera-se da responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus funcionários e colaboradores, atribuindo toda ela ao respectivo funcionário ou colaborador que fez indevidamente uso destes, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos

processos investigatórios, bem como de adotar as medidas legais cabíveis.

A Política de Segurança da Informação será implementada no órgão ou instituição por meio de procedimentos específicos, obrigatórios para todos os funcionários e colaboradores, independentemente do nível hierárquico ou função no órgão, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos pela Política de Segurança acarretará violação às regras internas do órgão e sujeitará o funcionário ou colaborador às medidas administrativas e legais cabíveis.

RESPONSABILIDADES ESPECÍFICAS

Para Nakamura (2003, p. 178) toda política de segurança da informação deve definir as responsabilidades dos envolvidos, sejam indivíduos, chefias, direções ou órgãos de forma a estarem vigilantes às adversidades, planejando estratégias de ação sempre que a prevenção não tenha sido suficientemente observada. Todos devem conhecer as tecnologias de proteção em uso na instituição e estarem aptos a adotarem atitudes diante das ameaças detectadas, impedindo que se tornem ocorrências e prejudiquem o sucesso do órgão. Assim se sugere estabelecer atribuições dentro de uma política de segurança da informação como se segue:

1 - Dos Colaboradores em Geral

Entende-se por funcionário toda e qualquer pessoa física, contratada sob qualquer regime, mesmo os temporários, pela instituição ou órgão ou, ainda, prestadores de serviço.

Por colaborador entende-se funcionário outro vinculado temporariamente ou esporadicamente a alguma atividade desenvolvida pelo órgão ou instituição e que necessite tramitar relações de serviços.

Será de inteira responsabilidade de cada funcionário ou colaborador, todo prejuízo ou dano que vier a causar à instituição e/ou a terceiros, em decorrência da não obediência às diretrizes e normas preestabelecidas.

2 - Dos Funcionários do Órgão

Devem entender os riscos associados à segurança da informação e cumprir rigorosamente a política estabelecida no que diz respeito à prevenções e obstruções de toda e qualquer ameaça de vazamento ou perda de informação.

3 - Dos Diretores, Coordenadores ou Gestores de Pessoas e Atividades

Devem ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os

funcionários e colaboradores sob a sua gestão.

Cabem aos mesmos:

- Atribuir aos funcionários e colaboradores, na fase de seleção para prestação de serviços ou de parceria, a responsabilidade no cumprimento da Política de Segurança da Informação estabelecida pela instituição ou órgão;
- Exigir dos funcionários e/ou colaboradores sob sua responsabilidade, antes de acessá-los a qualquer tipo de informação processada no órgão ou instituição, a assinatura do Termo de Confidencialidade e de aceite das normas estabelecidas, bem como do compromisso de manter sigilo mesmo quando desligado sobre todos os ativos e informações acessadas;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a Política de Segurança da Informação e ao arcabouço legal vigente.

4 - Dos detentores da Custódia/Guarda da Informação

4.1 - Da Tecnologia da Informação (TI)

São atribuições da área de TI:

- Testar a eficácia dos mecanismos de controle utilizados e informar aos Chefes e Coordenadores os riscos e/ou ameaças porventura remanescentes;
- Acordar com os Chefes/Coordenadores o nível de serviço e os procedimentos de resposta aos eventuais incidentes;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos funcionários ou colaboradores com todos os controles necessários para cumprir os requisitos de segurança estabelecidos pela Política de Segurança da Informação estabelecida;
- Conscientizar os administradores e operadores dos sistemas computacionais de que, pela característica de seus privilégios como usuários técnicos de poderem acessar aos arquivos e dados de outros usuários, isso somente será permitido quando for necessário para a execução de atividades operacionais de sua responsabilidade, de extrema necessidade, como por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente;
- Assegurar as funções administrativas, operacionais e educacionais a fim de restringir

ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam alterar os logs, programas e trilhas de auditoria do sistema de TI;

- Garantir segurança especial para os sistemas com limitador de acesso, seja interno ou público, incluindo o ambiente físico, fazendo guarda de evidencias que permitam a rastreabilidade para fins de provas de auditoria ou investigação;
- Gerar e manter as trilhas para auditoria de TI, com nível de detalhe suficiente para rastrear possíveis falhas, vazamentos e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para órgão;
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;
- Informar ao Chefe ou gestor da informação previamente sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante;
- Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não sejam removidos de forma irrecuperável, antes de disponibilizá-las para outro usuário que possa utilizá-las;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pela atividade;
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, por matrícula, cadastro ou outro documento legal, de forma que:
  1) Os usuários (logins) individuais de funcionários sejam de responsabilidade do próprio funcionário;
  2) Os usuários (logins) de colaboradores ou terceiros sejam de responsabilidade do Chefe/gestor da área vinculada na instituição;
- Proteger continuamente todos os ativos de informação do órgão

contra códigos maliciosos, e garantir que todos os novos ativos só entrem para o sistema após estarem livres de código malicioso e/ou indesejado;

- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção do conhecimento do órgão em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso por terceiros outros;
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro do órgão;
- Realizar auditorias periódicas de configurações técnicas e análise de riscos;
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais;
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento do órgão, investigação ou outra atividade que exija medida restritiva para fins de proteger a informação;
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede do órgão operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro;
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
    1) Uso da capacidade instalada da rede e dos equipamentos;
    2) Tempo de resposta no acesso à internet e aos sistemas críticos do órgão;
    3) Períodos de indisponibilidade no acesso à internet e aos sistemas críticos;
    4) Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e outros);
    5) Atividade de todos os funcionários e colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

4.2 - Da Área de Segurança da Informação

- Propor as metodologias e os processos específicos para a segurança da informação, tais como avaliação de risco e sistema de classificação da informação;

- Propor e apoiar iniciativas que visem à segurança dos ativos de informação;
- Publicar e promover as versões das Políticas de Segurança da Informação e as Normas aprovadas pelo Comitê de Segurança da Informação;
- Promover a conscientização dos funcionários e colaboradores em relação a relevância da segurança da informação às atividades do órgão, mediante campanhas, palestras, treinamentos e outros meios de comunicação interna;
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;
- Analisar criticamente incidentes em conjunto com o Comitê de Segurança da informação;
- Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou das Chefias/Coordenações do órgão;
- Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a instituição;
- Buscar constantemente o alinhamento com as diretrizes internas do órgão.

4.3 - Do Comitê de Segurança da Informação

- Deve ser formalmente constituído por Funcionários Chefes, Coordenadores, e Encarregados, nomeados pela Direção para participar do Comitê pelo período de um ano, com possibilidade e renovação se conveniente para o órgão. A composição mínima desse grupo deve ser de um funcionário de cada Coordenação ou Chefia;
- Deverá reunir-se, pelo menos semestralmente, e sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o órgão, podendo, inclusive, utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico;
- Cabe ao Comitê:
  1) Propor investimentos relacionados à segurança da informação com o objetivo de reduzir riscos e ameaças;
  2) Propor alterações nas versões da Política de Segurança da Informação com inclusão,

eliminação ou mudança de normas complementares;

3) Avaliar os incidentes de segurança e propor ações corretivas;
4) Definir medidas corretivas cabíveis nos casos de descumprimento das normas estabelecidas pela Política de Segurança da Informação;

MONITORAMENTO AMBIENTE E AUDITORIA

Para garantir as regras mencionadas na Política de Segurança da Informação, o órgão poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas deverá ser usada para identificar usuários e respectivos acessos efetuados, bem como o material e o conteúdo manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação da Diretoria Geral, após dar conhecimento ao Comitê de Segurança da Informação;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

1 – Da Intranet (Correio eletrônico)

O objetivo das normas inerentes ao Correio Eletrônico (Intranet) é informar aos funcionários e colaboradores do órgão, quais são as atividades permitidas e proibidas quanto ao uso da Intranet.

O uso da intranet é exclusivamente para fins institucionais e relacionados às atividades do funcionário ou colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais não é recomendada, sendo permitida somente para situações extremamente necessárias e que não prejudiquem o órgão e não cause impacto no tráfego da rede. Entretanto é proibido aos funcionários ou colaboradores o uso da intranet para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo do órgão;
- Enviar mensagem usando o nome de outro usuário ou endereço

eletrônico que não esteja autorizado a utilizar;

- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a instituição vulnerável a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as sanções previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das Chefias/Coordenações estiverem sujeitas a algum tipo de investigação;
- Produzir, transmitir ou divulgar mensagem que:
    1) Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do órgão;
    2) Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
    3) Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança das informações;
    4) Vise obter acesso não autorizado a outro computador, servidor ou rede;
    5) Vise um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    6) Vise burlar qualquer sistema de segurança;
    7) Vise vigiar secretamente ou assediar outro usuário;
    8) Vise acessar informações confidenciais sem explícita autorização do proprietário;
    9) Vise acessar indevidamente informações que possam causar prejuízos a qualquer funcionário, colaborador ou pessoa outra;
    10) Inclua imagens criptografadas ou de qualquer forma mascaradas;
    11) Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet), bem como para recebimento (internet);

12) Tenha conteúdo considerado impróprio, obsceno ou ilegal;
13) Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
14) Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
15) Tenha fins políticos locais ou do país (propaganda política);
16) Inclua material protegido por direitos autorais sem a permissão do detentor desses direitos;

As mensagens na intranet sempre deverão incluir assinatura com o seguinte formato:

- Nome do funcionário ou colaborador;
- Função;
- Telefone(s);
- e-mail corporativo.

2 - Da Internet

Todas as regras em vigor visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional no uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre portas para riscos significativos para os ativos de informação. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a instituição, em conformidade com a legislação em vigor no país, reserva-se no direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do órgão, que pode analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação, ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O órgão, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer funcionário ou colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados aos mesmos e ao respectivo Chefe/Coordenador. O uso de qualquer recurso para atividades ilícitas poderá

acarretar sanções administrativas e outras decorrentes de processos civil e criminal, sendo que nesses casos o órgão cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus funcionários ou colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

Como é de interesse do órgão que seus funcionários ou colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede e não perturbe o bom andamento dos trabalhos, nem implique conflitos de interesse com os seus objetivos.

Os funcionários e colaboradores do órgão são proibidos de falar em nome do órgão, em meios de comunicação, exceto nos casos em que houver manifestação expressa do Diretor Geral e apenas os funcionários autorizados poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

Ademais é proibido ao funcionário ou colaborador:

- A divulgação e/ou o compartilhamento indevido de informações da área de produção do conhecimento ou administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet;
- Em hipótese alguma utilizar os recursos da instituição para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;
- Utilizar programas de entretenimento, jogos ou músicas (em qualquer formato). Em caso de real necessidade para o desenvolvimento de alguma atividade específica, estes devem ser solicitados à área técnica responsável para uso em regime de exceção, quando eles tiverem natureza intrínseca à atividade;
- Abrir, expor e armazenar material de cunho sexual. Caso seja extremamente necessário para fins investigativos, deverão ser criados grupos específicos de perfis de usuário especial e seus

integrantes definidos pelos respectivos Chefes;

- Efetuar upload (subida) de qualquer software licenciado pelo órgão ou de dados de sua propriedade a terceiros;
- Utilizar recursos do órgão para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

3 - Da Identificação e Controle de Acesso

Os dispositivos de identificação e senhas protegem a identidade do funcionário ou colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a instituição e/ou terceiros. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os funcionários e colaboradores.

Todos os dispositivos de identificação utilizados no órgão, como o número de registro, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante o órgão e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Havendo login de uso compartilhado por mais de um funcionário ou colaborador, a responsabilidade perante a instituição e a legislação (cível e criminal) será dos usuários que dele se utilizarem.

A Coordenação ou Chefia responsável pela emissão e controle dos documentos físicos de identificação dos funcionários responde pela criação da identidade lógica no órgão, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários, devendo identificar distintamente os visitantes, estagiários, empregados temporários e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

É recomendado que os usuários que não possuem perfil de administrador devam ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que

possível, enquanto que os usuários que possuem perfil de administrador ou acesso privilegiado devam utilizar uma senha de no mínimo 9 (nove) caracteres alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como o próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

Após três (3) tentativas de acesso, a conta do usuário será bloqueada e para o desbloqueio é necessário que o usuário entre em contato com o Núcleo de TI. Deverá ser estabelecido um processo para a renovação de senha (confirmação de identidade) e os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é noventa (90) dias, não podendo ser repetidas as três (3) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada sessenta (60) dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for afastado, seja por atos de ofício ou por solicitação, o Núcleo de TI deve ser informado a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários colaboradores cujo contrato ou prestação de serviços tenha se encerrado.

Caso o usuário esqueça sua senha, ele deverá requisitar formalmente a troca à área técnica correspondente para cadastrar uma nova.

4 - Dos Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos funcionários e colaboradores da instituição são de propriedade do órgão, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelo Núcleo de TI.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Núcleo

de TI, ou de quem este determinar. As Chefias/Coordenações que necessitarem fazer testes deverão solicitá-los previamente ao Núcleo de TI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instalados, ativados e atualizados permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o Núcleo de TI mediante registro de chamado disponível na intranet. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante e autorização, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes às atividades do órgão (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso seja identificada a existência de arquivos dessa natureza, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos funcionários ou colaboradores da instituição deverão ser salvos no drive da rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário. Os funcionários ou colaboradores não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do Núcleo de TI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas, dentre elas:

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pelo Núcleo de TI do órgão, que terá acesso a elas para manutenção dos equipamentos;
- Os funcionários e colaboradores devem informar ao Núcleo de TI qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de

reparo que não seja realizado por um técnico do Núcleo de TI ou por terceiros devidamente credenciados;

- Todos os modens internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas e vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização do Núcleo de TI;
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;
- O funcionário ou colaborador deverá manter a configuração do equipamento disponibilizado pelo órgão, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas do órgão, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pelo órgão devem ter imediatamente suas senhas padrões (default) alteradas;
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso;

Aos funcionários e colaboradores é proibido o uso de computadores e recursos tecnológicos do órgão para:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- Interromper um serviço, servidor ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

- Hospedar pornografia, material racista ou qualquer outro ato que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

5 - Dos Dispositivos Móveis

A instituição não permite a utilização de dispositivos móveis sem autorização prévia da Chefia/Coordenação pertinente ao funcionário que a necessite. Entende-se por "dispositivo móvel" qualquer equipamento eletrônico com atribuições de mobilidade de propriedade particular tais como: notebooks, smartphones, pendrives etc. Essa norma visa estabelecer critérios no manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os funcionários ou colaboradores que utilizem tais equipamentos. Em casos excepcionais de necessidade o órgão fornecerá o equipamento/dispositivo, reservando-se o direito de inspecioná-lo a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O funcionário ou colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de outros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão da função desempenhada no órgão, mesmo depois de terminado o vínculo contratual mantido com o órgão. Todo funcionário ou colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados do dispositivo móvel que, porventura, esteja sob sua responsabilidade, mantendo os backups separados do dispositivo, ou seja, não carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade do órgão deverá seguir o mesmo fluxo de suporte estabelecido pela instituição. Todo funcionário deverá utilizar senhas de bloqueio automático para os dispositivos sob sua carga e não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do Núcleo de TI.

Os funcionários e colaboradores deverão responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico do Núcleo de TI. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pelo órgão constituirá uso indevido do equipamento e, por consequência, infração legal às normas aqui estabelecidas e aos direitos autorais do fabricante.

É responsabilidade do funcionário ou colaborador, no caso de furto ou roubo de um

dispositivo móvel fornecido pelo órgão, notificar imediatamente seu Chefe/Coordenador direto, devendo também procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O funcionário deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venham causar ao órgão e a terceiros.

6 - Do Servidor Central

O acesso ao Servidor Central somente deverá ser feito por sistema forte de autenticação, por exemplo: biometria, cartão magnético entre outros e deverá ser registrado (usuário, data e hora) mediante software próprio, além de ser executada semanalmente uma auditoria nos acessos por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do Núcleo de TI, de acordo com o Procedimento de Controle de Contas Administrativas, quem deverá manter constantemente atualizada a lista de funções com direito de acesso.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um preposto do Núcleo de TI ou outro devidamente autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso, bem como assinar o Termo de Responsabilidade.

O acesso por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Servidor Central for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Deverão existir duas cópias de chaves da porta do Servidor, uma das quais ficará de posse do Núcleo de TI e outra na Coordenação ou Chefia de Segurança Interna ou similar, que deverá acompanhar a manutenção local quanto à limpeza e organização, atentando para retirar qualquer procedimento que gere lixo ou sujeira nesse ambiente.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos da área do Servidor Central somente se dará com o preenchimento da solicitação de liberação pelo funcionário solicitante e a autorização formal desse instrumento pelo Núcleo de TI, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

Em caso de desligamento de funcionários ou colaboradores que possuam acesso ao Servidor, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de funcionários autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso.

7 - Do Backup

Todos os backups devem ser automatizados por sistemas automáticos de agendamento para que sejam preferencialmente executados fora do horário de expediente administrativo, nas chamadas "janelas de backup" (períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática).

Os funcionários ou colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o

máximo possível do Servidor Central .

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional. O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial. Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas. Periodicamente deverá ser inserido dispositivo de limpeza nas unidades de backup nos termos procedentes de Controle de Mídias de Backup.

As mídias de backups de operações e atividades especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 10 quilômetros do Servidor Central. Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da instituição, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e

legais existentes no país. Na situação de erro de backup, o "restores" é necessário que seja feito no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e "Restore". Quaisquer atrasos na execução de backup ou "restore" deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração "restore" de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 dias, de acordo com a criticidade do backup. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo Núcleo de TI, nos termos do Procedimento de Controle de Backup e "Restore".

Conclusão

A segurança orgânica como meio essencial de proteção às instituições tem sido pouco explorada. É evidente que há um descaso das instituições e órgãos públicos com essa segurança, principalmente quando se trata da segurança da informação nela processada, e isso tem produzido danos muitas vezes despercebidos de pronto, mas que, com o tempo se tornam irreparáveis. A segurança orgânica deve primar pela segurança do pessoal, dos documentos, das áreas, das instalações, dos recursos tecnológicos e da informática; entretanto, alguns poucos órgãos que fazem uso dela, fazem de forma muito incipiente e limitam-se à instalação de alguma barreira física ou eletrônica ou ao controle de acesso. À segurança da informática especificamente nada ou quase nada tem sido feito.

Dessa forma, buscou-se neste ensaio estabelecer um padrão básico de política de segurança da informação que poderá ser aprimorado conforme o grau de sensibilidade das atividades e informações trabalhadas no órgão, tornando-as mais segura e menos vulneráveis às ações adversas e contrárias.

A política de segurança sugerida está voltada principalmente para o público interno do órgão ou instituição uma vez que de nada vale o investimento em diversas medidas mínimas de segurança se não houver o compromisso das pessoas e a consciência de sua importância. Medeiros (2012) cita que "o segredo para resultados imediatos está na conscientização, no treinamento e na educação, pois implementar medidas de segurança é uma questão, principalmente, de atitude".

O estabelecimento de medidas mínimas de segurança da informação visa, além da proteção do órgão, alertar e aguçar o interesse das pessoas pela própria segurança, tornando-se menos vulneráveis às ações que ameacem ou coloquem em risco a instituição.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna de uma instituição. Qualquer incidente subtende-se como alguém agindo contra a ética e os bons costumes regidos pelo órgão.

O descumprimento da política e normas de proteção da informação pode gerar sanções que variam de suspensão até a demissão do infrator, sem prejuízo das sanções penais e cíveis correspondentes ao dano causado à instituição e as atividades por ela desenvolvidas.

Referências

BRASIL, Lei 12.527 de 18 Nov. 2011. **Lei de acesso a informação.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

BRASIL, Ministério da Defesa, Exercito Brasileiro. Portaria 483 de 20 Set. 2001. Aprova a **IG 20-19 sobre segurança da informação.** Disponível em: www.3cta.eb.mil.br/download/ig_20_19.pdf Acessado em 18 Jul. 2013.

FERREIRA, Fernando Nicolau & ARAUJO, MARCIO. **Política de Seguranças da Informação**. Rio de Janeiro, Ed. Ciência Moderna, 2ª. edição, 2008.

MAGALHÃES, A C S.
Segurança Orgânica como ramo da Inteligência. Disponível.em: http://www.webartigos.com/_resources/files/_modules/article/article_106872_20130413161318 0faa.pdf Acessado em 14/07/2013.

MANDARINI, Marcos. **Segurança corporativa e estratégica: fundamentos**. Barueri, São Paulo, Ed. Mamole, 2005.

MOREIRA, N.S., **Segurança mínima, uma visão corporativa de informações**. Rio de Janeiro, Ed. Axcel Books do Brasil, 2001.

NAKAMURA, Emílio Tissato. **Segurança de Rede em ambientes corporativos**. São Paulo, Ed. Futura, 2003.

O GLOBO ON-LINE, **Brasil foi alvo de espionagem dos Estados Unidos**, disponível em: http://m.g1.globo.com/mundo/noticia/2013/07/brasil-foi-alvo-de-espionagem-dos-eua-diz-o-globo.html Acessado em 14/07/2013.

SÃO PAULO, SENAC. **Política de Segurança da Informação**: documento de diretrizes e normas administrativas. Disponível em: http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf Acessado em 14 Jul. 2013.

VEJA ON-LINE, **Dilma quer que ONU discuta monitoramento feito pelos EUA**. http://veja.abril.com.br/noticia/brasil/dilma-quer-que-onu-discuta-monitoramento-feito-pelos-eua Acessado em 14 Jul. 2013.