FUNDAÇÃO JOÃO PINHEIRO
Governo de Minas Gerais

Curso de Especialização em Contabilidade e Finanças Públicas

# POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES NA SECRETARIA DE ESTADO DE FAZENDA DE MINAS GERAIS: UMA QUESTÃO DE GOVERNANÇA CORPORATIVA

**REGINA CELIA MOREIRA DA SILVA**

Belo Horizonte
2009

REGINA CELIA MOREIRA DA SILVA

# POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES NA SECRETARIA DE ESTADO DE FAZENDA DE MINAS GERAIS: UMA QUESTÃO DE GOVERNANÇA CORPORATIVA

Dissertação apresentada a Escola de Governo de Minas Gerais (EGMG) da Fundação João Pinheiro (FJP), como parte das exigências para obtenção do título de especialista em Contabilidade e Finanças Públicas.

Orientadora: Profª Drª Sulamita Crespo Carrilho Machado

Belo Horizonte
Fundação João Pinheiro
2009

Ficha Catalográfica

**Silva, Regina Celia Moreira da**
*Política de Segurança da Informação na Secretaria de Estado de Fazenda: uma questão de governança corporativa*. 2009.
81f.

Orientador: Profª Drª Sulamita Crespo Carrilho Machado
Monografia (Especialização) – Escola de Governo Professor Paulo Neves de Carvalho da Fundação João Pinheiro, Curso de Especialização em Contabilidade e Finanças Públicas

1. Governança Corporativa. 2. Administração Pública. 3. Segurança das Informações. 4. Política de Segurança da Informação.

REGINA CELIA MOREIRA DA SILVA

# POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES NA SECRETARIA DE ESTADO DE FAZENDA DE MINAS GERAIS: UMA QUESTÃO DE GOVERNANÇA CORPORATIVA

Dissertação apresentada a Escola de Governo de Minas Gerais (EGMG) da Fundação João Pinheiro (FJP), como parte das exigências para obtenção do título de especialista em Contabilidade e Finanças Públicas

Aprovada em 29 de junho de 2009

Banca Examinadora:

_____

Orientadora Profª Drª Sulamita Crespo Carrilho Machado - FJP

_____

Prof. Dr. Ronaldo Ronan Oleto – FJP

DEDICATÓRIA

Aos que acreditam que nossas vidas, assim como nossas ações, estão interligadas. Qualquer ação que realizamos, sejam elas boas ou más, influencia diretamente em nossa e nas demais vidas que nos rodeiam.

# A G R A D E C I M E N T O S

Sobretudo e primeiramente a Deus, Pai paciente, amigo, o Tudo a quem estou aprendendo a conhecer e amar, que me guiou pelas pontas dos dedos pelos caminhos que me trouxeram ao final desta jornada, me iluminando para traçar as linhas.

À minha família que silenciosa e pacientemente aguardou a conclusão do trabalho, em especial à Letícia, querida irmã, companheira inseparável e parceira em todos os meus projetos de vida.

A Geraldo Pedro grande amigo e responsável por eu estar concluindo essa especialização, uma vez que abriu mão da vaga que havia sido destinada a ele.

A Lindenberg Naffah e Alessandro Zebral pela compreensão e disponibilidade em auxiliar no que fosse necessário, grandes incentivadores, colaboradores e crédulos no importante trabalho do profissional da segurança da informação, cujos resultados são alcançados somente com muito esforço e dedicação.

Aos colegas, profissionais da Tecnologia de Informação, que atuam na Gerência de Redes e Segurança da Informação da Secretaria de Estado de Fazenda, sempre disponíveis aos questionamentos de uma leiga.

Aos colegas da Diretoria de Administração e Finanças da Secretaria de Estado da Fazenda que confiaram na minha capacidade.

Aos professores da Fundação João Pinheiro que ministraram o curso de Especialização em Contabilidade e Finanças Públicas aos servidores da SEF, cujas aulas acrescentaram em muito em meu conhecimento sobre administração pública, em especial à minha orientadora pelo conhecimento, sabedoria e paciência sempre presentes em palavras objetivas.

"*Antes do compromisso*

*Há a hesitação, a oportunidade de recuar,*

*Uma ineficácia permanente.*

*Em todo ato de iniciativa (e de criação),*

*Há uma verdade elementar*

*Cujo desconhecimento destrói muitas idéias*

*E planos esplêndidos.*

*No momento em que nos comprometemos*

*De fato, a Providência também age.*

*Ocorre toda espécie de coisas para nos ajudar,*

*Coisas que de outro modo nunca ocorreriam.*

*Toda uma cadeia de eventos emana da decisão,*

*Fazendo vir em nosso favor todo tipo*

*De encontros, de incidentes*

*E de apoio material imprevistos, que ninguém*

*Poderia sonhar que surgiriam em seu caminho.*

*Começa tudo o que possas fazer*

*Ou que sonhas poder fazer.*

*A ousadia traz em si o gênio, o poder e a magia*".

(Goethe)

# POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES NA SECRETARIA DE ESTADO DE FAZENDA DE MINAS GERAIS: UMA QUESTÃO DE GOVERNANÇA CORPORATIVA


## RESUMO

Este trabalho objetiva realizar um estudo sobre a Política de Segurança da Informação na Secretaria de Estado de Fazenda de Minas Gerais como uma ferramenta de apoio no processo de governança corporativa. Apresentando algumas considerações acerca do "*e-governance*" como uma ferramenta de gestão e transparência dos atos governamentais, e as discussões do direito eletrônico referentes às infrações cometidas no meio virtual bem como as respectivas penalidades a serem aplicadas. Realizou-se uma pesquisa bibliográfica, com revisão analítica da literatura e consultas em revistas e *sites* especializados sobre os assuntos: segurança da informação, governança corporativa, política de segurança, direito eletrônico, direitos humanos. Com o estudo foi possível constatar que as organizações estão mais conscientes sobre a importância de uma gestão embasada em boas práticas em governança e com postura ética que permita ser reconhecido seu valor no mercado. Foi possível constatar também que possuir uma Política de Segurança da Informação possibilita uma melhor gestão sobre os recursos tecnológicos e informacionais. Concluiu-se, portanto, que uma gestão embasada nos princípios fundamentais de governança, na postura ética por parte de todos os envolvidos e do contínuo processo de conscientização de todos os usuários dos sistemas e serviços, não há o que falar em penalidades. A conscientização dos usuários é a maior aliada em qualquer organização, uma vez que a Política de Segurança das Informações deve ser um recurso de gestão preventiva, não tendo como finalidade primária definir punições.



Palavras Chaves: Governança Corporativa, Administração Pública; Segurança das Informações; Política de Segurança

# LISTA DE ILUSTRAÇÕES

# LISTA DE SIGLAS

**CGSINS** – Conselho Gestor de Segurança Institucional da Secretaria de Estado de Fazenda

**CVM** – Comissão de Valores Imobiliários

**IBGC** – Instituto Brasileiro de Governança Corporativa

**PRODEMGE** – Companhia de Tecnologia da Informação de Minas Gerais

**PSI** – Política de Segurança da Informação

**PSI/SEF-MG** – Política de Segurança da Informação da Secretaria de Estado de Fazenda do Estado de Minas Gerais

**SEF/MG** – Secretaria de Estado de Fazenda de Minas Gerais

**SEPLAG/MG** – Secretaria de Estado de Planejamento e Gestão do Estado de Minas Gerais

**SGSI** – Sistema de Gestão de Segurança da Informação

**SI** – Segurança da Informação

**TI** – Tecnologia da Informação

**TIC** – Tecnologia da Informação e Comunicação

# S U M Á R I O

# 1. APRESENTAÇÃO

O mundo está interligado por meio de sistemas, tramitando e guardando todas as informações no meio digital. Esse detalhe, que há uns poucos 10 anos idos era inimaginável aos nossos pensamentos, hoje é possível verificar que a maioria da população mundial utiliza algum aparelho eletrônico.

Pesquisa realizada sobre telefonia celular no Brasil apresentou um espantoso resultado de quase um aparelho por habitante. Também resultado de pesquisa que a população brasileira procura alimentos mais baratos de acordo com a época, mas prefere comprar automóveis e celulares de último modelo.

Mas de que forma e quais são os recursos utilizados para proteger as informações que são trafegadas em meios virtuais? Mal podemos acompanhar as mudanças tecnológicas, tal a agilidade como a evolução acontece. As empresas de produtos de telecomunicações oferecem recursos de proteção para as informações, e já é possível ter contratos com empresas que se especializam em resguardar as informações críticas. Mas onde são guardadas e quais são as ferramentas? Em meios virtuais, com recursos tecnológicos em constante evolução, cujo principal objetivo é proteger as informações críticas das organizações.

E assim, o tráfego de informações no ambiente virtual tem agilidade semelhante aos impulsos elétricos do sistema nervoso humano. Um simples comando em um equipamento eletrônico e é possível disponibilizar qualquer informação para todo o mundo.

Nosso cérebro é um ambiente que contém toda uma gama de células, mas se não forem bem cuidadas certamente perecerão já que muito provavelmente não serão restabelecidas, embora a ciência já encontre alternativas de estimulação que permite o restabelecimento de alguns tipos. Assim são também as informações no ambiente virtual, se perdidas dificilmente serão recuperadas se não forem observados os cuidados básicos de segurança.

A perda dessas informações pode ocorrer: por ameaças internas ou externas, naturais ou intencionais, por usuários rancorosos ou usuários desavisados e despreparados. A maneira como a organização faz a gestão das informações, a sua política de segurança, os investimentos nas tecnologias, seus planos de continuidade e, acima de tudo, como mantém a conformidade de sua política de segurança, é que irá definir a permanência ou não dessa organização no mercado.

Um exemplo bem concreto de que é necessário ter uma gestão sobre as informações armazenadas em meio virtual, foi o atentado terrorista contra o *Word Trade Center* – "as torres gêmeas" – ocorrido em 11 de setembro de 2001 nos Estados Unidos da America que exterminou por completo as empresas que não possuíam qualquer recurso de proteção às informações. Somente as empresas que resguardaram suas informações conseguiram restabelecer as atividades.

Prejuízos causados pelos crimes em meio eletrônico são maiores a cada dia. Roubos de informações estratégicas crescem assustadoramente. Os celulares são novos alvos de ataque porque a cada dia se parecem mais com computadores e um percentual considerável de pessoas utilizam dispositivos móveis pessoais para armazenamento de informações que, na maioria das vezes, são informações organizacionais.

Este trabalho teve como objetivo apresentar a relevância da instituição da política de segurança da informação na Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG), implementada pela Deliberação CGSINS nº 003 (SEF/MG, 2006), sendo uma importante ferramenta de subsídio à gestão administrativa de governança eletrônica voltada para apresentação de resultados.

Buscando embasamento nas literaturas consultadas objetivou-se verificar se é viável para a SEF/MG, implementar a governança corporativa sustentada simplesmente pelos princípios de gestão, ou se é necessário elaborar normas específicas que permitam um maior controle sobre seus ativos, visando à proteção de suas informações, e com um nível de detalhamento que permita especificar as infrações que porventura coloquem em risco as informações sensíveis, bem como instituir penalidades referentes às possíveis infrações cometidas.

Foi realizada uma pesquisa em artigos científicos, teses e livros referentes aos temas segurança da informação, políticas de segurança da informação, governança corporativa, direitos humanos, direito eletrônico e penalidades no contexto dos códigos civil e penal, visando buscar nas fontes consultadas subsídios que sustentem a necessidade de alteração da redação das normas com a inclusão de quais condutas são inaceitáveis no ambiente da SEF/MG, sendo as mesmas passiveis de punições.

A relevância deste projeto está na discussão se é necessário detalhar as penalidades permitindo que as mesmas possam ser aplicadas de maneira mais pontuais. As penalidades cometidas serão analisadas sob a ótica das normas internas da SEF/MG? Pelo Código Civil? Pelo Código Penal, ou observando todos os códigos mais as normas internas? Os códigos de conduta ética são suficientes para coibir e também punir as práticas que contrariam os princípios éticos e que lesam a administração pública? Ou será que eles estão sendo ignorados e assim facilitando as ações contraventoras dos usuários?

Este trabalho foi estruturado em cinco partes. Na primeira ousou-se apresentar o cenário na governança corporativa, a governança na administração pública, governança em Tecnologia da Informação (TI), e a gestão e a ética. A segunda parte apresenta o cenário da evolução da sociedade da informação no contexto dos direitos humanos. Na terceira parte os princípios, objetivos e importância da segurança da informação para as organizações. A quarta parte discorre sobre o Plano Corporativo de Segurança da Informação no contexto do governo de Minas Gerais. A quinta parte discorre sobre a Política de Segurança da Informação e seu papel na organização, a sexta parte apresenta a Política de Segurança da Informação no âmbito da SEF/MG e, por fim, as considerações realizadas acerca dos estudos feitos.

# 2. A GOVERNANÇA CORPORATIVA

O termo governança corporativa é mais comumente utilizado nas áreas de atividades econômicas. Porém, atualmente vem se tornando conhecido em vários outros seguimentos da sociedade, mas todos com o mesmo objetivo, garantir uma relação satisfatória entre acionistas e dirigentes.

De acordo com Houaiss (2001), o termo governança significa "*ato de governar(-se)"* e o termo corporativo significa *"relativo a ou próprio de uma corporação"*.

Para a Comissão de Valores Imobiliários (2002, p.1) significa um conjunto de práticas que objetiva otimizar o desempenho da organização e proteger os interesses das partes interessadas, tais como investidores, empregados e credores.

Pela teoria econômica a governança corporativa objetiva administrar o processo de superação do conflito existente entre a propriedade e a gestão sobre a mesma, pois nem sempre o interesse de quem administra a propriedade está alinhado com os interesses de seus titulares. É conhecido como conflito de agência. (GRÜN, 2005)

A teoria da agência busca criar mecanismos que garantam aos acionistas a proteção de seus investimentos por meio do comportamento ilibado dos executivos que gerenciam a organização, conduzindo a uma gestão estratégica e resultando nas práticas de governança. (GRÜN, 2005)

A idéia da boa governança originou-se nos Estados Unidos da América onde tradicionalmente a população realiza investimento no mercado de ações, o que favorece a uma disputa mais leal pelo controle das empresas.

Mas foi também nesse país que ocorreram os primeiros indícios de abalo à confiança na governança corporativa, face aos escândalos financeiros de grandes empresas, o que indicava que a gestão das mesmas não havia se comportado com ética, ignorando um ou alguns dos princípios que regem a governança corporativa.

Foi constatado também que a legislação norte-americana não conseguiu dar sustentabilidade necessária aos investidores, sendo necessário elaborar uma legislação especifica para proteção ao acionista.

Grün (2005, p. 74), relata que a legislação norte-americana de então não era suficiente para atingir os objetivos que se esperava dela. A principal consequência foi a edição da Lei Sarbanes-Oxley considerada um avanço em relação ao estado anterior da proteção legal que o acionista do mercado norte-americano tinha em relação ao comportamento dos responsáveis pelas empresas que ele investiu.

Conforme Marques (2007, p. 15) inicialmente três princípios básicos da governança corporativa eram mais conhecidos. São eles: o respeito aos acionistas, a transparência das ações e a possibilidade de adquirir o controle da empresa através da compra de ações no mercado.

A evolução destes princípios trouxe novos temas a serem observados como métodos alternativos de solução de conflitos, responsabilidade social, dentre outros, sendo que os princípios são apenas referências para uma gestão ética. Cada organização deve desenvolver os seus próprios e de acordo com suas particularidades.

A união ou a observação aos princípios da governança corporativa permite leal concorrência no mercado de ações para os acionistas minoritários reforçada por uma legislação que oferece sustentabilidade às garantias oferecidas aos investidores, sendo um código igualmente adotado em todo o mundo.

A criação desse código proporcionou mudanças nas práticas de governança oferecendo, principalmente, maior transparência nas ações das organizações, bem como uma conduta ética por parte dos administradores.

Esses códigos visam mais do que penalizar os gestores no não cumprimento de suas obrigações. São constituídos por regras para uma gestão ética, com base em dispositivos legais e instruções específicas, para nortear as organizações a

alcançarem resultados favoráveis a novos investimentos, ampla concorrência e permitindo que possam se solidificar no mercado.

No Brasil a organização exclusivamente dedicada à promoção da governança corporativa é o Instituto Brasileiro de Governança Corporativa (IBGC), que fornece fundamentos da efetiva aplicação das boas práticas de governança corporativa.

Visando a orientar as empresas sobre o assunto, o IBGC (2003) elaborou o *Código das Melhores Práticas em Governança Corporativa*, que tem como princípio básico ser um instrumento de gestão para todas as organizações, públicas ou privadas, no que tange à governança corporativa.

Embora a Governança Corporativa tenha surgido visando organizações de capital aberto que desejam consolidar-se no mercado mundial, ela pode e deve ser vista como importante instrumento de gestão das organizações em geral, sejam elas públicas ou privadas, deste ou daquele segmento da economia, pequenas ou grandes.

Nas literaturas consultadas é possível encontrar diversas definições para governança corporativa. Seguem apresentação de algumas delas. Para o IBGC governança corporativa é definida como:

> (...) sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade. (IBGC, 2003, p.6)

De acordo com Chagas (2004, p.3) governança corporativa é a tradução da expressão inglesa *"corporate governance"* ou o sistema pelo qual os acionistas de uma empresa “governam”, ou seja, tomam conta, de sua empresa. Conceito esse que pode ser ampliado para:

> (...) conjunto de princípios, procedimentos, métodos e rotinas que, aplicados numa entidade, propiciam resultados eficientes e eficazes e promovem a harmonia das partes interessadas na condução ordenada da organização. As partes interessadas são os acionistas, cotistas, dirigentes, gerentes, empregados, fornecedores, clientes, financiadores e a comunidade afetada diretamente pelos negócios e/ou atividades. CHAGAS (2004, p.3)

Para Monteiro (2003, p. D-2) *apud* Chagas (2004, p. 3), governança corporativa é um "*conjunto de práticas adotadas na gestão de uma empresa que afetam as relações entre acionistas (majoritários e minoritários), diretoria e conselho de administração*".

Portanto, governança corporativa, pode ser compreendida como um sistema que visa otimizar o desempenho da organização, bem como proteger os interesses de todos os envolvidos sendo regido por um código de práticas organizacionais para orientar o comportamento ético das organizações diante da sociedade e do mercado.

O processo da governança corporativa no Brasil, também teve início com a preocupação em estabelecer confiança nos investimentos no mercado de ações, e, através dos meios legais, proteger e atrair investidores uma vez que a disputa ocorria entre a elite brasileira, que era uma minoria e detinha o controle das empresas, também conhecido como governança familiar, ficando na contra mão dos direitos dos acionistas minoritários. (GRÜN, 2005)

## 2.1 Os princípios fundamentais à Governança Corporativa

De acordo com autores consultados a governança corporativa é norteada por cinco princípios básicos. São eles: transparência, equidade, prestação de contas ou *accountability, compliance* e eficácia. Chagas (2004) define esses princípios como:

> (...) um conjunto de valores e regras que orientam a gestão empresarial e o comportamento dos administradores de uma organização no sentido de atenderem os interesses das partes interessadas nos negócios e atividades desenvolvidos. (CHAGAS, 2004, p. 8)

Esses princípios são fundamentais na gestão e trazem em si a finalidade de exercer o papel de ferramentas de controle visando uma gestão por resultados, não sendo desconhecidos para a administração pública.

O princípio da transparência deve ser o principal objetivo a ser alcançado por qualquer administração. Deve ser interpretado como a forma pela qual a organização deve realizar seu papel assumindo seus compromissos com a sociedade. Os resultados devem ser apresentados de forma que qualquer leigo no assunto possa compreendê-los.

O despertar para a cidadania e para um mundo ecologicamente correto, já é um item considerado importante pelos cidadãos que estão a cada dia mais atentos ao tipo e à qualidade dos produtos e serviços ofertados.

O princípio da equidade é saber tratar justo e igualmente todos os acionistas. Atitudes ou políticas discriminatórias, sob qualquer pretexto, são totalmente inaceitáveis. (IBGC, 2003, p.10)

O prestar contas é atestar de forma clara que os atos praticados estão em conformidade legal, sendo que a forma para a apresentação dos resultados deve atender aos padrões estabelecidos pelos órgãos competentes. É poder dizer pelos relatórios gerados se, e quais, foram os investimentos feitos, se o planejamento foi cumprido, o que foi feito com os recursos disponibilizados.

Estar em "*compliance*" significa aquiescência, é o mesmo que estar em conformidade com as normas vigentes.

E, finalmente, a eficácia, que é a gestão efetivada do cumprimento das obrigações, que, por meio de ferramentas específicas as organizações podem apresentar os resultados alcançados e garantir a continuidade no mercado.

Para qualquer organização, estar competitiva no mercado é saber que precisa estar atenta aos riscos aos quais está exposta e a quais riscos expõe seus investidores e também a sociedade em geral.

Reconhecidos estes riscos e gerado o comprometimento social que objetiva zelar pelo bem coletivo, um novo valor é agregando aos princípios da governança corporativa: o da responsabilidade social, que visa evitar o enriquecimento de alguns por manipulações contábeis.

Esse novo valor estimula que empregados e dirigentes sejam dotados de boa moral e é também um caminho para que a empresa adquira a legitimidade no mercado financeiro e diante à sociedade.

Assim mais um valor passa a ser observado: a sustentabilidade das empresas. Para se manter no mercado tem que haver preocupação com o que se produz e seus efeitos para a sociedade. De acordo com Grün (2005, p. 77) o índice de sustentabilidade funciona como uma métrica para indicar os riscos aos quais a organização está exposta bem como os custos necessários para mitigá-los.

Para gerir uma organização com fins de garantir os investimentos considerando o bem estar de todos os envolvidos, bem como da sociedade, faz-se necessário uma boa gestão embasada em uma postura ética que perpasse por toda a estrutura organizacional envolvendo desde a direção até o último colaborador.

Estudos revelam que organizações que possuem alto padrão em governança tendem a possuir maiores investimentos[1], uma vez que os acionistas optam por investir o capital em organizações que lhes permitam acompanhar toda a evolução dos negócios, bem como ofereçam garantias do investimento feito, proporcionando também bons retornos.

A governança corporativa está para as organizações assim como os indicadores financeiros estão para os economistas. São sinalizadores sensíveis utilizados para indicar a real condição administrativa e financeira da organização nos quais os investidores se baseiam para a tomada de decisões.

Uma administração que vise a atender aos princípios da gestão corporativa de forma a se manter ética, lícita e competitiva no mercado, deve ter também um bom sistema de indicadores que permita mensurar sua evolução e desempenho no mercado.

O exercício da governança corporativa depende da qualidade das informações disponíveis e na agilidade que se pode ter acesso às mesmas. Para isso é necessário que a organização esteja bem estruturada para alcançar seus objetivos. Analisar os riscos e tomar decisões no momento certo depende diretamente de informações precisas e imediatas.

[1] De acordo com Ribeiro (2007, p. 2). a discussão sobre esse assunto no Brasil (...) foi motivada por fenômenos econômicos e sociais, ganhando mais força após as crises da Ásia e da Rússia, quando os investidores institucionais, especialmente os fundos de pensão americanos, passaram a priorizar os investimentos em empresas que tivessem maior transparência e respeito para com os acionistas e demais *stakeholders*.

## 2.2 Governança Corporativa na Administração Pública

A governança corporativa na administração pública tem a mesma representatividade que no mundo empresarial, ressalvadas suas proporções e características. Os governos devem realizar uma gestão responsável dos recursos, entregando as obras em cumprimento aos planejamentos, garantindo assim, o retorno do investimento da população. Esta, por sua vez, deve conscientizar-se de seu papel como auditora uma vez que ao pagar os impostos eles devem ser aplicados nas necessidades primordiais da população.

Para a administração pública a governança corporativa tornou-se uma ferramenta gerencial para apresentação de resultados, onde um dos princípios básicos é a transparência nas ações do governo.

Sendo a governança corporativa uma evolução natural da sociedade na busca de maior controle e transparência, para que o governo transforme em realidade suas decisões devem ser observadas as condições financeiras e administrativas ressaltando que essas ações não são meramente altruísticas, mas uma necessidade de mercado[2], uma vez que a administração pública, em detrimento aos princípios da governança corporativa, deve cumprir seu papel social retornando à sociedade obras e serviços aos quais foi designada a realizar.

O processo de governança permitiu à administração pública fazer uma releitura de sua atuação no mercado, assim como perceber que a gestão dos processos realizada de forma manual não favorece a uma apresentação satisfatória de resultados. É como ter uma caixa d'água de grande capacidade de armazenamento que possui um vazamento não detectado e não se sabe qual a melhor alternativa para contê-lo.

[2] De acordo com Ribeiro (2007, p. 1) a governança corporativa pretende contribuir para a superação de um grande desafio que é a atração de investidores, porém respeitando os diversos interessados na companhia, sem impactar os lucros. Portanto, a discussão acerca da governança corporativa não se deu por altruísmo ou benevolência das empresas e de seus controladores, mas pela necessidade mercadológica.

Agia Neto (2007, p. 5) considera extremamente pertinente que existam na administração pública práticas de governança corporativa, semelhantes às do setor privado que permita combater fraudes e corrupções, tão comum no setor público.[3]

Quem gerencia os recursos é também responsável por apresentar resultados. O que foi feito e com quê, o que precisa ser melhor administrado, fazendo a gestão do orçamento com autonomia para redistribuir os recursos conforme as necessidades da comunidade.

Sendo o processo de governança a capacidade de governar-se, as ações que cada indivíduo exercer conscientemente enquanto administrador público será uma resposta ao cumprimento ético do seu papel como gestor dos recursos públicos em prol do fim a que se destina, ou seja, realizar ações que beneficie a coletividade e não aos próprios interesses ou a de um pequeno grupo.

Por sua vez a sociedade deve ter consciência da importância de sua participação nas decisões das políticas públicas, a exemplo do orçamento participativo, onde tem poder de escolher quais obras e serviços que irão ser realizados.

O que é possível perceber na administração pública nos últimos anos é que os benefícios que não foram recebidos pela população não são justificados pela falta de recursos, mas sim na incapacidade de gestão do administrador. Conforme dito por Almeida (2004, p. 2):

> *(...) os maiores problemas que se apresentam, nos dias de hoje, no processo de melhoria nas condições de vida e bem-estar das populações, em países ricos ou pobres, não são aqueles derivados da falta de recursos ou de meios técnicos para sua solução, mas provêm, tão simplesmente, da incompetência institucional.*

Portanto, administrar os recursos, ter conhecimento dos riscos e poder optar por um caminho de gestão que não lese a sociedade, é um processo complexo. Vários

[3] Agia Neto (2007) considera interessante que o setor público obtenha resultados e métodos semelhantes ao do setor privado em termos de eficiência, custos, produtividade e de administração. Também não existem razões para que não possam ser implantadas, no setor público, práticas que objetivam reduzir sensivelmente as fraudes e a corrupção interna e externa. Medidas como: *a) rotatividade e compartilhamento de funções de decisão ou sensíveis; b) auditorias freqüentes e independentes; c) identificação e eliminação ou monitoramento dos pontos de risco; e d) comparação de dados de produtividade, e custos do mercado com os alcançados.*

modelos de gestão são colocados no mercado a cada dia. Cabe aos dirigentes escolher qual é o modelo mais adequado para atender as necessidades da organização.

A estrutura da administração pública, em respeito à segregação de funções, já possui uma parte específica que planeja, dirige, controla, executa e outra para realizar a análise dos resultados bem como as auditorias.

Os relatórios contábeis gerados pela administração pública são elaborados com base em orientações específicas, oriundas dos órgãos competentes, que por sua vez irão realizar a auditoria nas contas públicas. Embora essas demonstrações ainda não representem os resultados de forma satisfatória aos leigos no assunto, já é um grande passo dado que é a obrigatoriedade de publicá-los

A boa governança é um processo de amadurecimento da sociedade para uma gestão com visão de que algumas ações políticas precisam de garantias para sua continuidade em outros governos para atingir os resultados esperados. É importante que o governo opte por uma gestão com fins de apresentação de resultados, ao invés de realizar disputas políticas partidárias que ocorrem a cada eleição.

Da mesma forma que as empresas, orientadas pelos códigos de boas práticas em governança corporativa apresentam os resultados dos investimentos de forma a ser interpretado e utilizado pelos investidores como informações vitais, assim devem ser as demonstrações geradas pela administração pública.

Os dados deixam de ser meramente estatísticos, para ser parte do negócio, ou seja, informações estratégicas, que devem ser protegidas conforme critérios de criticidade. A informação crítica[4] é tratada como patrimônio da organização e deve ser devidamente protegida.

Tanto nas empresas estatais quanto na administração pública o item primordial é a informação, que deve ser extraída, tratada objetivando a elaboração das

[4] Na tecnologia da informação o termo informação crítica ou informações sensíveis, são todas as informações relevantes para o negócio, sendo consideradas como um ativo da organização. Por sua vez devem ser tratadas conforme o grau de criticidade das mesmas.

demonstrações de resultados e apresentada aos interessados para a realização da tomada de decisões, mantendo a integridade dos dados originais.

## 2.3 O governo eletrônico (e-governance)

Para Pinheiro (2008, p. 238) o Governo Eletrônico pode ser entendido com o conjunto de serviços e acessos a informações que o governo oferece à sociedade civil por meios eletrônicos.

É um conceito que representa para a administração pública um avanço no uso dos recursos tecnológicos tornando-se um canal de comunicação com cidadãos e contribuintes, cuja redução no custo das transações, propicia também colocar em prática o princípio governamental da transparência, disponibilizando para a sociedade, em meio eletrônico, os resultados das ações e procedimentos governamentais tais como: projetos de lei em andamento, obras realizadas, relatórios de gestão, dentre outros.

Além da visibilidade que as transações oferecem é também um meio de combate a fraudes, a exemplo da entrega das Declarações de Imposto de Renda em meio magnético, impedindo que as declarações sejam emitidas e entregues em nome de outra pessoa.

As possibilidades que a internet pode oferecer são inúmeras. É um veículo de comunicação em massa muito eficiente, permite a interação entre as pessoas de todo o mundo. Basta apenas estar conectado à rede mundial de computadores, para que qualquer pessoa possa acessar, de qualquer lugar do mundo, um assunto ou serviço de seu interesse, uma vez que é vasto teor de materiais publicados. O ponto mais relevante, e também o mais debatido, é que para ter acesso a essas informações e serviços o cidadão precisa saber como utilizar.

Para os estudiosos no assunto a internet pode ser um meio de comunicação capaz de atingir toda a sociedade, mas também pode ser uma forma de exclusão social tendo em vista que boa parte da população não tem acesso às novas tecnologias e por sua vez não sabe utilizá-la. Por outro lado pode ser também um veículo para

renovar as formas de participação política e tomada de decisões. (FREY, 2000, p. 37).

Frey (2000)[5] apresenta extremos na discussão do tema. Por um lado as novas tendências de administração pública que apresenta uma gestão de políticas públicas objetivando uma governança participativa com fins a mitigar os problemas sociais e econômicos, levando em conta a complexidade e o dinamismo do ambiente urbano. De outro aflora apenas as tendências ideológicas de mudança dos sistemas políticos, mas que não resultam em reformulações profundas.

O conceito *e-gov* traz o entendimento de que o uso da internet pode proporcionar alternativas para a disponibilização de informações e ser também um recurso de controle democrático, uma vez que permite ampliar a participação social. Porém se essa participação for realçada além do necessário poderá maquiar o objetivo primordial, que é a transparência dos atos governamentais. É também importante considerar que a rápida evolução da tecnologia digital, solicita investimentos para as ferramentas utilizadas, na capacitação dos operadores e desenvolvedores dos sistemas, e para a população que irá utilizar os serviços. (FREY, 2000, p. 41)

É inquestionável que a internet trouxe novas formas de relacionar, transformando substancialmente as dimensões de tempo e espaço. Observado os cuidados necessários a não exclusão digital, cabe às agências, governamentais ou não, estimular o uso investindo de forma que a propagação das redes chegue para todas as comunidades. Assim todas elas terão a oportunidade de participar da nova forma de participação democrática, bem como de interação social.

O Brasil vem atuando no combate à exclusão digital trabalhando a educação, oferecendo equipamentos de custos mais acessíveis e disponibilizando terminais de acesso em repartições públicas. Como exemplo de caso de sucesso, Pinheiro (2008, p. 238) cita o Projeto Rede Fácil [6] da prefeitura de Santo André em São Paulo, que

[5] Artigo publicado na I Conferência Eletrônica do Centro Virtual de estudos Políticos (CEVEP), com o tema Internet, Democracia e Bens Públicos, promovida pelo Departamento de Ciência Política da UFMG e pela empresa de Informática e Informação do Município de Belo Horizonte (Prodabel) entre 01 e 30 de novembro de 2000.

[6] Este projeto foi avaliado pelo *Habitat*, Centro das Nações Unidas para Assentamentos Humanos, sendo considerado uma das 100 melhores experiências mundiais no combate à exclusão digital,

oferece 180 diferentes tipos de serviços. O Brasil é referência entre os países emergentes nas ações de combate a exclusão digital e no uso do ambiente digital visando o aumento da eficiência administrativa, sendo importante ressaltar que o Brasil é o único país no mundo que tem votação eletrônica em todo o território nacional.

Porém os estudiosos no assunto não são unânimes na afirmação de que o uso da internet seja vantajoso. O cenário é de que nem só de vantagens é composto esse ambiente. Benefícios como a restauração da legitimidade do sistema político, a criação de novos canais de comunicação, permanente intercâmbio de conhecimento, valorização da pesquisa acadêmica, gerenciamento urbano, participação da população na história política, podem dar uma falsa idéia de nova forma de participação democrática, bem como a concretização da transparência das ações governamentais.

## 2.4 A Governança e a Ética

A governança corporativa ou a autogestão da organização, tem um super-olhar em si própria vigilante sobre tudo o que faz. Desde como administrar visando lucros até como será vista pelos clientes e concorrentes. Neste sentido a gestão ética da organização passa ser um item a mais, ou o mais importante da lista de itens requisitados pelos investidores.

O comportamento ético dos indivíduos em sociedade é objeto de estudos no campo da filosofia, antropologia, dentre outras, que buscam explicação para tão diferentes comportamentos. Conflitos como os de interesses financeiros ou ideológicos, podem colocar em crise a estrutura administrativa e, por sua vez, colocar em risco a missão da organização.

É possível conceber uma organização que tenha princípios éticos e não ter boa governança, mas não o inverso, pois, não basta seguir regras. O comportamento

---

porque além do serviço *online* foram criados postos de atendimento e serviços por telefone. Vide Pinheiro (2008, p. 238).

das pessoas influencia diretamente, uma vez que a adoção de boas práticas de governança significa também adoção de princípios éticos.

Todo o contexto organizacional tende a seguir os parâmetros e princípios éticos propostos, desde que gerentes e colaboradores, exerçam suas funções pautados nessas definições.

Organizações cuja direção preza o comportamento ético como item primordial ao atendimento aos clientes, cientes que essa atuação garante bons retornos dos investimentos e no fortalecimento de participação social, certamente exercerão uma forte influência no comportamento de seus profissionais sob pena de que, quem não se adequar aos princípios da organização, ser convidado a se retirar da equipe.

Já é comum encontrar organizações que realizam consultas sobre a conduta ética do profissional que está selecionando, sendo esse um dos quesitos de peso na escolha.

No momento onde a fidedignidade com clientes e com os investimentos é um importante diferencial que a organização procura apresentar, assim também tem comportado o mercado que recebe a organização e seus serviços solicitando a cada dia novas garantias. Um bom exemplo são as certificações oferecidas para as organizações que se destacam em determinado segmento, na qualidade dos serviços oferecidos, e na garantia oferecida aos clientes.

Os escândalos decorrentes dos desfalques, tanto no âmbito da administração pública quanto das empresas privadas, induzem os investidores e a sociedade em geral a cobrarem mais qualidade pelos serviços que estão sendo oferecidos.

As transformações que sofreram as estruturas governamentais, em termos mundiais, decorrentes da insatisfação com a conduta ética dos dirigentes, convergem para o estabelecimento de uma gestão administrativa que vise padrões de conduta voltados para o consenso organizacional permeados pela modernização e o fortalecimento

institucional da organização, que no Brasil tornou-se conhecida como gestão da ética[7]. Carneiro et al. (2002, p.17).

Esta linha de raciocínio conduz a interpretação de que não há como ter governança sem condução ética, uma vez que essa enseja um restabelecimento da confiança da sociedade no caráter dos agentes públicos, esses, por sua vez, devem ter claro o que pode e o que não pode ser feito no âmbito da administração pública.

A gestão ética requer que se estabeleça conjunto de regras levando em conta as especificidades de cada organização. É extremamente importante que haja um processo educativo consistente e contínuo que divulgue a todos os colaboradores as diretrizes e normas criadas, bem como seus objetivos, e sistemas de monitoramento que permita identificar a não observância das regras e a aplicação de sanções.

## 2.5 Governança em Tecnologia da Informação

No contexto da sociedade da informação, a governança em Tecnologia da Informação (TI) vem ocupar um lugar representativo nas organizações. Uma vez que não há como conter a evolução tecnológica, não é possível manter as informações em manuais e os processos sem automatização.

Com o avanço das tecnologias ultrapassamos o mundo material para o imaterial, do meio físico, para o meio virtual. Institui-se uma nova forma de registro, escrito, mas não em papel.

De acordo com Laia e Lara (2007, p. 63) a década de 80 trouxe grandes transformações para a administração pública mudando radicalmente o papel e a gestão dessas organizações.

[7] Palestra apresentada no VII Congresso Internacional do Centro Latino-Americano de Administração para o Desenvolvimento, referente à experiência da Comissão de Ética Pública, realizado em outubro de 2002.

A *Nextgeneration Center* (2006)[8] apresenta uma definição não muito complexa do que é a governança de TI, ou governança em Tecnologia da Informação:

> "... *governança de TI nada mais é do que uma estrutura bem definida de relações e processos que controla e dirige uma organização no atual cenário de forças econômicas em extrema competição. O foco é permitir que as perspectivas de negócios, de infra-estrutura de pessoas e de operações sejam levadas em consideração no momento da definição do que mais interessa à empresa, alinhando a tecnologia da informação à sua estratégia*." (NEXTGE, 2006, p. 2)

Ao mesmo tempo em que existe a preocupação com a segurança dos dados, também é fato de as informações que definem a existência das pessoas, seus documentos, seus dados, estão disponíveis no meio virtual. Com o apertar numa simples tecla ou a execução de um simples programa, podendo ser ou não intencional, a repercussão pode não causar grandes transtornos, mas também pode resultar em danos irreversíveis, como por exemplo: apagar o histórico de um indivíduo ou documentos de alta relevância para a organização.

Numa sociedade a cada dia mais digital, cuidar para que ninguém tenha acesso a seus segredos ou informações também é uma armadilha, porque é necessário conhecer e implementar ferramentas tecnológicas para gestão das informações levando em conta que a evolução é contínua, a tecnologia tende a ficar obsoleta e sem a manutenção devida os sistemas podem ser invadidos. É um mundo que busca insistentemente um ambiente seguro e é inseguro ao mesmo tempo, porque não há como garantir que não ocorrerá perda de informações. Não existem ambientes ou sistemas 100% seguros.

Certamente que lidar com um mundo intangível requer uma série de cuidados. Mas não resta dúvida que não há como ficar à margem da modernização. É necessário haver uma harmonia, encontrar um equilíbrio, entre o avanço das tecnologias e a necessidade de proteção das informações, cuidando para não se tornar refém dos recursos tecnológicos.

Porém, quem não acompanhar a evolução poderá se tornar "jurássico". É como navegar guiando-se apenas pelas estrelas num meio onde os demais utilizam todo e

[8] Ambiente de educação a distância que disponibiliza cursos na área de tecnologia da informação.

qualquer recurso tecnológico disponível. Neste ambiente intangível é necessário discernir o que é e o que não é realmente representativo, saber o que deve ser guardado e disponibilizado.

Quem tem o conhecimento acerca dos recursos tecnológicos disponíveis no mercado e utiliza a tecnologia adequada, consegue gerir melhor os recursos disponíveis. Na sociedade da informação, novas tecnologias e definições sempre surgirão, mas o princípio é o mesmo: quem tem a informação detém o poder. Daí a importância de cuidar do que lhe é importante.

Apenas deter esse poder não basta é necessário saber resguardá-lo. A evolução tecnológica é muito rápida tornando-se também um fator de risco para a organização. O exemplo disso são as mídias eletrônicas que estão cada vez menores e com capacidade de guardar cada vez mais um volume maior de informações.

A governança por si somente não existe, é devido à necessidade de ter controle sobre os ativos[9] da empresa que se tornou fundamental a gerência dos bens, do seu patrimônio. Quanto maior a organização, mais complexa se torna sua gestão devido à interface a ser feita. Em uma organização são encontrados vários tipos de ativos.

De acordo com Lopes (2006, p.1) são seis tipos:

1. Ativos humanos: pessoas, habilidades, planos de carreira, treinamento, relatório, *mentoring*, competências etc.
2. Ativos financeiros: dinheiro, investimentos, passivo, fluxo de caixa, contas a receber etc.
3. Ativos físicos: prédios, fábricas, equipamentos, manutenção, segurança, utilização etc.
4. Ativos de PI: Propriedade Intelectual (PI), incluindo o *know-how* de produtos, serviços e processos devidamente patenteado, registrando ou embutindo nas pessoas e nos sistemas da empresa.
5. Ativos de informação e TI: dados digitalizados, informações e conhecimentos sobre clientes, desempenho de processos, finanças, sistemas de informação e assim por diante.
6. Ativos de relacionamento: relacionamentos dentro da empresa, bem como relacionamentos, marca e reputação junto a clientes, fornecedores, unidades de negócio, órgãos reguladores, concorrentes, revendas autorizadas etc.

[9] Qualquer coisa que tenha valor para a instituição – ABNT NBRI SO/IEC 17799:2005

Gerenciar esses ativos e a interface que os mesmos possuem entre si, não é uma tarefa simples e requer ferramentas específicas. "*A governança destes ativos ocorre por meio de um grande número de mecanismos organizacionais*" (LOPES, 2006). Todavia uma boa gestão desses ativos requer uma direção atenta, mas principalmente que esteja envolvida e interessada em investir, uma vez que na área da Tecnologia da Informação (TI), o investimento não é pequeno.

E não pouco comum observar que as organizações possuem maior gestão sobre os ativos financeiros e físicos do que os de informação.

> A maturidade na governança desses ativos varia significativamente na maioria das empresas de hoje, com os ativos financeiros e físicos sendo tipicamente os mais bem governados, e os ativos de informação figurando entre os piores. (LOPES, 2006, p.1).

Gerir uma organização é também lembrar que cada uma é única e tem sua representatividade nos mercados interno e externo, uma vez que os investimentos tendem a ultrapassar as fronteiras. Para alcançarem seus objetivos estas organizações precisam ser eficientes e possuírem estruturas tecnológicas que favoreçam a comunicação umas com as outras, bem como competitividade no mercado.

Estar atuante no mercado ou cumprindo seu papel como gestora de recursos públicos requer que a organização esteja atualizada com os recursos tecnológicos. No mercado existem várias ferramentas para apoiar a gestão da organização. O que leva a conclusão de que as organizações, por menor que seja sua estrutura ou representatividade no mercado, consegue encontrar recursos tecnológicos que sustentem seus processos de negócios.

Para tanto é necessário que haja um forte apoio da direção da organização, investimento financeiro, trabalho em conjunto e o entendimento quanto ao importante trabalho que será realizado pelas áreas de TI, uma vez que os controles, procedimentos e métricas que viabilizarão a gestão dos processo de negócio partirão delas.

> (...) é fundamental o papel desempenhado pela Tecnologia da Informação para a efetiva implementação da governança como habilitadora dos controles e demonstrações de conformidade aos princípios contábeis, legais e de administração responsável e ética das organizações (GAJANIGO, 2006, p. 1)

Para a administração pública o desenvolvimento das tecnologias e comunicações trouxe grandes desafios, uma vez que todo o trabalho era feito manualmente, mas foi também um importante diferencial para automatizar os processos possibilitando também um maior controle sobre os ativos.

A SEF/MG iniciou em 2005, em parceria com a Secretaria de Estado de Planejamento e Gestão (SEPLAG) e Companhia de Tecnologia da Informação de Minas Gerais (PRODEMGE), o Plano Corporativo de Segurança da Informação que, além de proteção às informações, objetiva adequar a instituição com os recursos tecnológicos mais modernos e que atendam às boas práticas de segurança e pelas Leis Internacionais de Segurança, sendo uma delas a NBR/ISO 17799/2005.

A elaboração deste projeto é o reflexo da mudança de conceitos e criação de novos procedimentos na gestão pública, o que faz com que a SEF/MG esteja apenas iniciando a sua gestão de risco, para ter o controle de suas informações, objetivando melhorar seu processo de governança.

A estruturação desse projeto está embasada em uma política de segurança da informação sustentável, que visa à proteção das informações, a gestão dos sistemas, a conformidade, a continuidade do negócio, resultando na gestão da segurança das informações.

# 3. DIREITOS HUMANOS, GOVERNANÇA CORPORATIVA E A INFORMAÇÃO

O volume, sempre crescente de informações disponibilizadas, contrasta com a característica do espaço virtual e na necessidade de se estabelecer padrões internacionais de Direitos Humanos para as interações, considerando que a almejada governança global é um longo caminho a ser percorrido.

A importância do produto informação, suas interfaces e nuances no contexto da história da humanidade pode ter várias representações. A informação como: suporte a serviços sociais, referência para as atividades econômicas, transações comerciais e financeiras, como troca de informações culturais, de cunho social, político e cultural, informação que alcança determinados grupos sociais, informações históricas, informações rápidas e sem fronteiras.

Na discussão acerca dos direitos humanos na sociedade da informação, as pessoas são afetadas por esse novo padrão de interação o qual certamente será a forma como as pessoas conduzirão suas vidas, seu trabalho, seus relacionamentos afetivos, momentos de lazer, dentre outras. E a discussão no campo dos direitos humanos converge ao entendimento de que é uma forma legítima de abordagem, avançando a discussão para um futuro próximo, é necessário estabelecer a defesa de um padrão popular universalmente aceito, uma vez que os Direitos Humanos formam o único conjunto universalmente disponível de padrões para a dignidade e a integridade de todos os seres humanos. (HAMELINK, 2005, p. 105)

As sociedades vão se adaptando aos movimentos da informação, das idas e vindas dos fatos e notícias. E assim percebe-se que o espaço intangível passou a ter valores significativos. Chegar ao trabalho e perceber que não há mensagens a serem lidas, os telefones não tocam, a internet está fora do ar, jornais e revistas não chegaram, ninguém procura por você. É um bom exemplo de como estamos dependentes da informação e mais ainda dos equipamentos tecnológicos que a suportam. (PINHEIRO, 2005)

A sociedade da informação como é conhecido o momento em que vivemos, é uma forma de expressar o contexto social atual onde o item de maior valor é a

informação, e quem a detém, detém também um grande poder. De acordo com Sathler (2005, p. 1) o termo sociedade da informação é uma forma de expressar o poder da atualidade, da mesma forma em que foi na época das sociedades, agrária que o poder era baseado na terra, e industrial, que o poder pertencia às indústrias.

A informação é, portanto, um item de disputa entre as empresas de maior poder econômico para ter acesso à matéria prima: a informação. Motivo esse que levou à convocação da Organização das Nações Unidas (ONU) para discutir sobre o assunto e encontrar meios de não permitir que houvesse a concentração de poder na mão de alguns poucos países.

Constatou-se que dos 13 equipamentos que controlam a disponibilização de domínios macro[10] e de todo o tráfego de informações pela rede mundial, 10 estão localizados nos EUA. Caso decidam por bloquear a disponibilização de informações de um referido domínio, pode fazer com que um país fique totalmente sem comunicação, o que na atual sociedade da informação, não é concebível.

A convocação feita pela ONU resultou na Cúpula Mundial sobre Sociedade da Informação (*World Summit on the Information Society* – ***WSIS***) onde foram discutidas as questões que envolvem o controle monopolista das informações. Sathler (2005, p. 2) ressalta que o assunto é tão abrangente que se tornou prioridade para vários órgãos intergovernamentais, conduzindo a uma gestão por governança global considerando a facilidade com que extrapola as fronteiras nacionais.

As possibilidades permitidas pelas tecnologias de informação e comunicação são inimagináveis e tendem tanto para atividades que beneficiam a sociedade, como também pode ocorrer ao contrário. A grande dificuldade é encontrar mecanismos de controle, uma vez que os interesses variam.

A WSIS como ficou conhecida a Cúpula Mundial, dada a abrangência do assunto, focalizou em dois itens de discussão que foi a governança na internet e

[10] São as abreviações que compõem os endereços eletrônicos que identificam de onde são os domínios. Exemplo: fazenda.mg.gov.br, onde significando: MG que é do estado de Minas gerais, gov que é um ambiente do governo e BR que informa de qual país, neste caso o Brasil.

financiamento das telecomunicações para atender às nações mais pobres. Muitos outros temas foram debatidos: exclusão digital, direitos de propriedade, software livre, diversidade, direitos à comunicação multiculturalismo, dentre outros.

Como resultado do encontro foi possível perceber que os países estão mais informados e mais conscientes sobre o uso da internet e as Organizações da Sociedade Civil (OSCs) obtiveram nesse encontro um amadurecimento sobre o assunto e um alcance maior para agir e expressar em áreas restritas dos governos. Mas considerando os desafios, a governança global ainda tem um longo e árduo caminho a percorrer.

Em meio a essa indefinição, os diversos campos da ciência continuam a debater o então ambíguo conceito sociedade da informação e o ambiente virtual, meio intangível, no qual se pode dizer que quase tudo está inserido e qual sua representatividade para o cidadão.

A Declaração Universal dos Direitos Humanos (ONU, 1948) discute em seu artigo 27 o direito do cidadão de ter acesso ao avanço científico e a seus benefícios, mas os avanços ocorridos exigem atenção por parte da ONU, porque pode colocar em risco os direitos e liberdades dos indivíduos e assuntos focados em respeito à privacidade dos indivíduos, como o uso dos satélites para observação, integridade e soberania das nações, dentre outras.

Assim, a grande discussão é o que realmente é considerado como informação e o papel que a comunicação representa no contexto da sociedade da informação, considerando que o direito à comunicação, enquanto direito fundamental. Perpassa pelo processo de diálogo entre os participantes, uma vez que, apenas receber a informação ou ser comunicado de sua existência, não produz sentido, considerando que é necessário ter acesso à mesma.

Os direitos de comunicação baseiam-se nos princípios da liberdade de expressar e manifestar suas opiniões e idéias, de ser incluído em processos que conduzam à construção de sentidos e no contexto social ao qual faz parte, de respeito à diversidade, uma vez que cada indivíduo é único, de utilizar dos recursos para

capacitar-se cultural e profissionalmente, estar inserido no contexto social ao qual pertence.

No que tange a governança, a comunicação pode ser percebida de duas formas. O uso do ambiente virtualizado para a disponibilização de informações de forma que o cidadão possa acessar o governo. Neste caso a prática da governança eletrônica é percebida como uma forma de manter uma interlocução entre governo e o cidadão por meio dos portais governamentais onde são disponibilizados os serviços, informações, notícia, dentre outros. Essa forma de estabelecer a comunicação vai além da idéia de manter contato apenas pela internet, utilizando também outros canais de comunicação como centrais de atendimento telefônico, postos de atendimento, quiosques de auto-atendimento, dentro outros.

Nesta interface a simples publicação de relatórios ou a disponibilização de informações necessárias ao cidadão não garante que será um meio onde será exercido o direito de cidadania e nem que a transparência de atos do governo foi alcançada.

Há também a discussão acerca do corporativismo informacional, quando torna-se necessário, seja por questões econômicas ou por disponibilidade de recursos imprescindíveis à prestação do serviço, concentrar a informação a ser disponibilizada aos cidadãos, sob os cuidados de algumas poucas empresas privadas ou setores do governo. Neste sentido pode ocorrer que a informação publicada atenda a objetivos estritamente comerciais, que forma que apenas o interesse da minoria seja atendido.

Há o grande interesse comercial em manter os bancos de dados contendo as informações dos usuários que fazem uso da internet ao utilizar o e-mail, fazer compras online, acessar jornais ou *site* de relacionamentos. Coletar e utilizar esses dados tornou-se uma indústria, pois correm o risco de ser utilizados para publicidade ou vendidos. Embora já exista legislação que regulamenta a manutenção dos logs registram o acesso dos usuários por parte dos provedores de acesso à internet para fins de possível auditoria, ainda há o que legislar sobre o correto uso destes dados.

Em ambos os casos se o objetivo social é desvirtuado, o risco à desinformação é alto, considerando que não há uma preocupação quanto aos direitos de comunicação. Situações como essas contribuem para a apropriação de conhecimento técnico por corporações privadas e a recusa dos detentores da tecnologia em concordar com padrões internacionais para transferência da tecnologia; controle corporativo sobre a produção e distribuição de bens e serviços informacionais e comunicacionais; proliferação mundial de subinformação no tocante às questões de interesse público; aumento das corporações transnacionais sem se preocupar com suas responsabilidades de contexto social e ético, dentre outras.

Ainda é necessário que ocorram movimentos que visem a assegurar que as informações possam ser acessadas por todos indiscriminadamente com fins a obter o conhecimento e desenvolvimento humano, e que esse acesso seja garantido mediante investimentos públicos, visando a extinguir o monopólio sobre o uso dos recursos tecnológicos e de comunicação.

Nas transações online a privacidade e confidencialidade das comunicações é um fator crucial, porque existem interesses conflitantes nessa discussão, de um lado as empresas desejam proteção para comunicações seguras, de outro em virtude da ampliação do comércio eletrônico as organizações estão se interessando por coletar e negociar dados pessoais dos consumidores.

É importante encontrar alternativas para assegurar comunicações seguras, mantendo a privacidade dos usuários, porém de uma forma padronizada para não incentivar o uso do recurso para atividades criminosas deixando o cidadão comum mais vulnerável aos ataques criminosos.

A evolução da governança requer mudanças de padrões comportamentais visando adotar códigos que atendam à maioria e métodos de gestão que concilie os diversos anseios, buscando um equilíbrio que resultará na geração de riquezas e valores para a sociedade.

# 4. A SEGURANÇA DAS INFORMAÇÕES

A importância dada ao trato das informações, não é uma preocupação da modernidade. O homem pré-histórico já utilizava o recurso dos desenhos para se comunicar, e, por conseguinte, registrar seu cotidiano.

Ao longo da história da humanidade é possível verificar registros de diversas formas de comunicação utilizadas. Vão desde a emissão de sinais de fumaça, toque de tambores, perpassando pelo telégrafo, até os modernos meios de comunicação da atualidade.

A agilidade no processo de comunicação, e, conseqüentemente de seus métodos, se deveu à utilização da eletricidade. A invenção do telégrafo elétrico de Samuel Morse em 1832 é um grande exemplo de evolução. Barreto (1993, p. 3) *apud* Machado (1996, p. 106) compara a mudança das várias formas de comunicação a um ritual de passagem da cultura tribal para a cultura escrita/tipográfica e para a cultura eletrônica.

Com os recursos tecnológicos a cada dia mais desenvolvidos, a informação torna-se o mais importante ativo da organização, sendo altamente relevante sua proteção, estando ela em meio físico ou magnético.

A sistematização dos processos, diminuindo consideravelmente os fluxos de documentos em papel, a, necessidade de agilizar a comunicação para atender às demandas urgentes do mercado, a necessidade de que as informações trafeguem de maneira rápida, que estejam disponíveis para serem acessadas a qualquer tempo e de qualquer lugar, a preocupação com as questões ambientais, são apenas alguns exemplos que evidenciam o porquê das informações trafegarem em ambiente virtual.

Uma vez que trafegando estas informações em meios virtuais, os equipamentos, *software*, ambientes, enfim todos os recursos tecnológicos que propiciam a disponibilização no meio virtual também evoluem com muita rapidez.

O Quadro 1 a seguir é um resumo comparativo feito por Pinheiro (2005a, p. 8) referente à evolução dos recursos tecnológicos antigos com os atualmente disponíveis e utilizados pela maioria dos usuários. Esse comparativo recebeu o título de *Paradigmas do mundo novo*:

Quadro 1 – Evolução dos recursos tecnológicos

| **O VELHO** | **O NOVO - Aonde já estamos!** |
|---|---|
| Analógico | Digital |
| Físico | Virtual |
| Átomos | Bits |
| Serviços Fixos | Serviços Móveis |
| Coletivos | Pessoais |
| Banda estreita | Banda Larga |
| Equipamentos dedicados | Equipamentos Multifuncionais |
| Baixa velocidade de transmissão | Alta velocidade transmissão |
| Comunicação por fio | Comunicação sem fio |
| Monopólio | Competição |
| Propriedade Estatal | Propriedade Privada |
| Protocolos Fechados | Protocolos Abertos |
| Unidirecionais | Interativos |
| Comutação de circuitos | Comutação de pacotes |

Fonte: Pinheiro, (2005a, p. 8)

Mas a que realmente chamamos de informações? De acordo com o Aurélio (1995), informação é um dado acerca de alguém ou algo; o conhecimento.

De acordo com Machado (1996, p.15) informação é uma palavra de definição difícil. Seu uso está sempre presente em nossa vida como elemento imprescindível. O conceito de informação está ligado ao significado e é usado como sinônimo de mensagem, notícia, fatos e idéias que são adquiridos e passados adiante como conhecimento[11].

De acordo com Pinheiro (2008, p. 363 e 349), informação é um ativo composto por um conjunto de dados ou elementos que tem valor para a organização necessitando ser adequadamente protegido. Seu conjunto compõe os ativos de informação da organização que são constituídos por todas as informações, base de dados,

[11] Yuexiao (1998), apud Machado (2003, p. 17), refere-se ao assunto informação ressaltando que "... há mais de quatrocentas definições apresentadas por estudiosos de distintos campos do saber e de distintas culturas, situação que torna inevitável o surgimento de interpretações errôneas. Informação não é ainda um conceito singular; ao contrário, caracteriza-se como um conceito controverso e, às vezes enganoso."

arquivos, documentação de sistemas, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, dentre outros.

A cada dia as informações sensíveis das instituições estão à mercê dos equipamentos tecnológicos que dispõem e dos profissionais responsáveis no trato e tráfego das mesmas.

Tanto os sistemas como as pessoas possuem vulnerabilidades que podem ser exploradas tornando-se um risco para a organização. É importante ressaltar que não existe 0% de risco para organização e em algum momento os equipamentos e *software* podem ser corrompidos por falhas tecnológicas. As pessoas podem ser seduzidas pelas fraquezas humanas: curiosidade, vaidade, interesse, egoísmos, dentre outras.

Embora haja a necessidade de acompanhar os avanços tecnológicos, adquirindo equipamentos compatíveis, não quer dizer que os mesmos não precisam estar condizentes com controles de segurança que permitam que as informações trafeguem seguramente.

Também não adianta ter equipamentos modernos para se resguardar de possíveis ameaças, sem que haja treinamento e conscientização de todos os usuários que fazem uso dos recursos tecnológicos e que tenham acesso às informações.

Dada a necessidade e relevância em se resguardar esse importante bem da instituição, é necessário encontrar alternativas que garantam os princípios básicos da informação conhecidos pela sigla CID: Confidencialidade, Integridade, Disponibilidade.

A confidencialidade é a garantia que somente as pessoas autorizadas terão acesso à informação; Integridade é a garantia da salvaguarda da exatidão e completeza da informação e dos métodos de processamento; Disponibilidade é a garantia de que os usuários autorizados terão acesso às informações, sistemas e serviços sempre que precisarem; Autenticidade é a garantia de que uma informação, produto ou

documento é do autor quem se atribui, certificada por instrumento ou testemunho público. A legalidade é a garantia do não repudio da informação.

A diversidade de tipos de ameaças que sofrem as organizações "... *têm influenciado para que a segurança da informação seja considerada uma real necessidade e um requisito estratégico, que interfere na capacidade das organizações de realizarem suas atividades com eficiência e eficácia.*" (LAIA e LARA, 2007, p. 63)

Considerando que a informação para a organização é vital, assim também o é um sistema de gestão de segurança, Sêmola (2003, p. 7 e 8) faz uma comparação da situação vivida pelas organizações no contexto de evolução das tecnologias e das informações. Por meio de fatos evidenciados dessa evolução ele construiu um cenário que ele chamou de "*receita explosiva*" composta por:

*a) Crescimento sistemático da digitalização de informações.*
*b) Crescimento exponencial da conectividade da empresa.*
*c) Crescimento das relações eletrônicas entre empresas.*
*d) Crescimento exponencial do compartilhamento de informações.*
*e) Barateamento do computador, facilitando sua aquisição.*
*f) Gratuidade do acesso à Internet.*
*g) Baixo nível de identificação do usuário no acesso gratuito à Internet.*
*h) Acesso a conexões Internet em banda larga.*
*i) Alto compartilhamento de técnicas de ataque e invasão.*
*j) Disponibilidade de grande diversidade de ferramentas de ataque e invasão.*
*k) Facilidade de uso de ferramentas de ataque e invasão.*
*l) Carência de mecanismos legais de responsabilização em ambiente virtual.*
*m) Carência de conscientização da similaridade entre o crime real e o virtual*
*n) Carência de jurisprudência que tenha regulado sobre atos ilícitos em meio eletrônico.*
*o) Comunicação de massa exaltando o jovem invasor pelo mérito da invasão.*
*p) Criação do estereótipo do gênio e herói que obteve êxito em invasão.*
*q) Associação equivocada entre Inteligência Competitiva e Espionagem Eletrônica.*
*r) Diversificação dos perfis da ameaça: concorrente, sabotador, especulador, adolescente, hacker, funcionário insatisfeito etc.*
*s) Crescente valorização da informação como principal ativo de gestão das empresas.*

A mistura desses ingredientes resulta no que ele considerou como "*um bolo amargo, difícil de digerir e que nos reserva um cenário de grande risco,* (...)". (SÊMOLA, 2003, p. 8). Cenário esse que toda organização deve evitar, já que nenhuma está livre dele.

Para qualquer da organização é de suma importância seu desempenho no mercado, sem perder a credibilidade, o que faz da informação o ativo mais importante. Tendo

como referencial que as informações que dispõe pertencem a duas categorias: as que já foram perdidas ou as que um dia serão perdidas. Agindo assim é possível ter cuidado redobrado uma vez que a qualquer momento algum incidente pode ocorrer.

O grande desafio do profissional de segurança da informação é convencer a alta gerência sobre a importância da implantação de um sistema de segurança dentro da organização. É um investimento muito caro cujo retorno não é imediato e nem sempre visível.

Somente quando a organização sofre o impacto em seus negócios é que ela passa a considerar a possibilidade de investir e, mesmo assim, ainda considera que pode manter-se competitiva mantendo os olhos fechados à realidade da evolução tecnológica.

Nakamura e Geus (2002, p. 34) apresentam uma lista de desculpas dadas pelos executivos para não investirem em sistemas de segurança:

a) Isso não acontecerá conosco.
b) Já estamos seguros com o *firewall*
c) Utilizamos os melhores sistemas, então, eles devem ser seguros.
d) Utilizamos as últimas versões dos sistemas dos melhores fabricantes.
e) Nossos fornecedores irão nos avisar, caso alguma vulnerabilidade seja encontrada.
f) Ninguém vai descobrir essa “brecha” em nossa segurança.
g) Tomamos todas as precauções, de modo que os testes não são necessários.
h) Vamos deixar funcionando e depois resolveremos os problemas de segurança
i) Os problemas de segurança são de responsabilidade do departamento de TI.
j) Luís, depois de instalar o *Word* para a Cláudia, você pode instalar o *firewall*?
k) A companhia de TI que foi contratada irá cuidar da segurança.
l) O nosso parceiro é confiável, podemos liberar o acesso para ele.
m) Não precisamos nos preocupar com a segurança, pois segurança é um luxo para quem tem dinheiro.

Diante deste cenário, que se torna a cada dia mais crítico em virtude dos avanços tecnológicos e dos interesses pelas informações, as organizações estão cada vez mais expostas às inúmeras ameaças.

Ameaças para a segurança da informação, de acordo com Sêmola (2003, p. 47) é:

> Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, conseqüentemente, causando impacto aos negócios de uma organização.

Ainda de acordo com Sêmola (2003, p. 47 e 48) as ameaças são classificadas conforme a intencionalidade:

> "NATURAIS – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição, etc.
>
> INVOLUNTÁRIAS – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia, etc.
>
> VOLUNTÁRIAS – Ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários."

Quanto às ameaças, elas podem surgir de qualquer lugar, basta que a organização esteja vulnerável e que o infrator que tem interesse na informação descubra essa falha ou então consiga burlar os recursos de segurança implementados pela organização.

Os maiores problemas de segurança para os quais os resultados das pesquisas apontam são causados porque as organizações se consideram imunes às ameaças ou porque não conseguem perceber o valor que suas informações possuem.

A cada dia são disponibilizados no mercado equipamentos mais sofisticados e acessíveis à população. A internet tornou-se a mais valiosa ferramenta de trabalho, largamente utilizada no ambiente corporativo e também no doméstico. Embora recomendações de segurança sejam propagadas incessantemente no ambiente virtual, de nada servem quando os usuários são pouco precavidos, muito ousados e pior que tudo, acreditam que eventos que colocam em risco os equipamentos, bem como as informações, não irão acontecer com ele.

Pinheiro (2005b, p. 32) fez uma lista contendo algumas ameaças, consideradas as mais comuns, às quais estão sujeitas qualquer organização:

a) Acesso Indevido;
b) Furto de informações;
c) Fraude Eletrônica e Falsificação de Identidade;
d) Dano aos dados e informações arquivadas;
e) Espionagem para Obtenção de segredos industriais/comerciais;
f) Cópia de programa;
g) Violação do Direito Autoral;
h) Interceptação indevida de informação;
i) Violação de bases de dados pessoais;
j) Uso Indevido de marca em *Search Engine* para gerar tráfego;
*k)* Exposição da Marca associada a Conteúdo Ofensivo ou falso em *Chat, Newsgroup, Messaging, Peer-To-Peer Network, Streaming Midia, e-mail, Website, Hotsite;*
*l)* *"Sucks" Sites* – frustração do consumidor – atualmente também em Comunidades, *Blogs, Fotologs, Forums*
*m)* Pirataria – de marca, texto, áudio, vídeo, música, *software*
*n)* Pornografia – 300.000 domínios mais visitados da *web* no mundo contém pornografia *(case Nintendo, Zippo, Sexdisney.com)*

Sabendo que a informação é valiosa e que precisa ser resguardada, é importante conhecer sua trajetória na organização, bem como sua interface com todos os sistemas. Gerir adequadamente uma organização é o caminho para mitigar riscos e não comprometer o negócio, por isso é importante conhecer como funciona a organização, atribuir competências e responsabilidades.

Estruturada a gestão do fluxo da informação, o esperado é que tudo funcione adequadamente. O usuário deseja que suas informações estejam protegidas e disponíveis; toda a organização espera que o departamento de informática desempenhe suas funções a contento; por sua vez o departamento de informática espera que os ambientes estejam controlados e protegidos e os sistemas funcionem adequadamente para atender as necessidades dos usuários e que esses últimos sejam constantemente esclarecidos sobre as vulnerabilidades às quais estão expostos.

Se ameaças se concretizam e as informações forem perdidas o usuário não vai querer saber se foram apagadas por um ex-funcionário insatisfeito, por um vírus, falha de hardware ou sobrecarga elétrica. A informação foi adulterada ou perdida e bem provável que não haverá como recuperá-la. (DIAS, 2000)

Cientes da relevância das informações para a organização, elas devem ser tratadas como o patrimônio mais representativo devido seu valor no mercado, portanto, necessitam de proteção contra as possíveis ameaças, independente de onde se originarem.

No contexto das organizações já não deve existir o pensamento de que a responsabilidade pela proteção das informações compete exclusivamente ao departamento de informática. Os gestores das informações também precisam se precaver, através de cuidados simples como, por exemplo: desligar ou bloquear o acesso ao computador em momentos de ausência, fazer cópia de segurança, não divulgar as senhas, dentre outras. Schneier *apud* Camargos (2005, p.14) deixa claro que os problemas de segurança da organização não são de exclusiva responsabilidade da tecnologia. "*Se você acredita que a tecnologia pode resolver seus problemas de segurança, então você não conhece os problemas e nem a tecnologia"*.

Para que a segurança da informação esteja presente em toda a estrutura organizacional causando o mínimo de impacto nas rotinas faz-se necessário a instituição de uma gestão de segurança para manter os riscos dentro dos patamares aceitáveis, uma vez que esta gestão segue normas e padrões que permitem uma unificação de procedimentos entre as organizações no mercado.

De acordo com Sêmola (2003, p. 139) as normas sugerem bases comuns de interação visando à proteção das organizações e competitividade no mercado. Assim as normas *"São exemplos de critérios, padrões e instrumentos de controle, aplicáveis parcialmente ou totalmente em função da natureza de cada negócio,* (...)". A gestão de SI é regulamentada pela ISO/IEC 17999, norma internacional que estabelece diretrizes e princípios para a gestão de segurança da informação nas organizações. No Brasil essa norma é conhecida como ABNT NBR ISO/IEC 17799:2005.

A norma é um guia de melhores práticas, objetivando sistematizar o trabalho e criar ambientes seguros. A norma por si só não resolve os problemas da segurança. Ela indica o que deve ser feito sem dizer como fazer, em virtude das peculiaridades de

cada organização. Para tanto faz-se necessário um sistema de gestão que auxilie e garanta sua conformidade.

Ainda de acordo com Sêmola (2003) as organizações podem conduzir as ações de segurança sob a orientação da norma, além de se prepararem indiretamente para o reconhecimento de conformidade aferido por órgãos credenciados. Procedendo assim a organização adquire o reconhecimento no mercado em que atua, uma vez que "(...) *Nem todos os controles e diretrizes contidos nesta Norma podem ser aplicados. Além disto, controles adicionais e recomendações não incluídos nesta Norma podem ser necessários.*" (ABNT NBR ISO/IEC 17799:2005, p. xii).

A ABNT NBR ISO/IEC 17799:2005, (p. ix) define segurança da informação como "(...) *proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.*"

O Decreto Federal nº 3.505 (BRASIL, 2000), definiu a segurança da informação como:

> *(...) proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.*

Sêmola (2003, p. 43) utiliza a base de conhecimento empresa da Módulo *Security Solutions* para definir segurança da informação como "*área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.*"

A Resolução SEF/MG nº 3.839, (SEF/MG, 2006), em seu artigo 4º define Segurança da Informação como:

> *Conjunto de medidas que tem como objetivo o estabelecimento dos controles necessários à proteção das informações durante sua criação, aquisição, uso, transporte, guarda e descarte, contra destruição, modificação, comercialização ou divulgação indevidas e acessos não autorizados, acidentais ou intencionais, garantindo a continuidade dos serviços, e a preservação de seus aspectos básicos, a saber: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.*

A segurança da informação é, portanto, o resultado da implantação de controles adequados, políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

Toda e qualquer informação é importante e deve ser protegida. Não importa em qual meio esteja: papel, meio magnético, nos equipamentos e sistemas, ou trafegando na rede. Basta apenas que um usuário não autorizado tenha acesso a algum sistema ou serviço para comprometer a segurança das informações da organização.

Independente de qual seja a natureza da organização, uma das recomendações propostas da norma para gestão de segurança é realizar a classificação das informações conforme os graus de sigilo. Assim será possível definir ações de proteção de acordo com os princípios básicos da segurança: confidencialidade, integridade e disponibilidade cujo grau de prioridade deve ser de acordo com o tipo de negócio e com os serviços que são oferecidos.

É o que Dias (2000, p. 44) quis dizer com "*Sistemas com necessidades de segurança diferentes devem ser tratados e protegidos também de forma diferente.*" Por exemplo, se um sistema não contém dados confidenciais, mas precisa estar disponível 24 horas por dia, o que deve ser considerado relevante é o princípio da disponibilidade, e assim sucessivamente.

Para criar um ambiente com base num sistema que permita uma gestão de segurança a ABNT NBR ISO/IEC 17799:2005, (p. 4), apresenta os domínios de segurança a serem implementados:

a) Política de Segurança da Informação;
b) Organizando a Segurança da Informação;
c) Gestão de Ativos;
d) Segurança em Recursos Humanos;
e) Segurança Física e do Ambiente;
f) Gestão das Operações e Comunicações;
g) Controle de Acesso;
h) Aquisição, desenvolvimento e Manutenção de Sistemas de Informação;
i) Gestão de Incidentes de Segurança da Informação;
j) Gestão da Continuidade do Negócio;
k) Conformidade.

A Norma recomenda a implementação de todos esses domínios, porém a ordem e o grau de importância serão definidos pela organização.

> A ordem das seções nesta Norma não significa o seu grau de importância. Dependendo das circunstâncias todas as seções podem ser importantes. Portanto, convém que cada organização que utilize esta Norma identifique quais são os itens aplicáveis, quão importantes eles são e a sua aplicação para os processos específicos do negócio. (...) (ABNT NBR ISO/IEC 17799:2005, p. 4)

A implementação de qualquer sistema de segurança precisa atender aos interesses da organização. Para tanto é necessário fazer uma análise do que se pretende fazer e de que maneira. Dias (2000, p. 44) ainda coloca que:

> Antes de implementar qualquer programa de segurança de informações, é aconselhável responder às seguintes questões: O que se quer proteger? Contra que ou quem? Quais as ameaças mais prováveis? Qual a importância de cada recurso? Qual o grau de proteção desejado? Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados? Quais as expectativas dos usuários e clientes em relação à segurança de informações? Quais as conseqüências para a instituição se seus sistemas e informações forem corrompidos ou roubados?

Quando a organização passa a visualizar o ambiente organizacional numa perspectiva de conformidade legal, se questionando sobre as conseqüências de possível perda das informações que estão sob sua custódia ou se deparando com processos judiciais, caso seja constatada a negligência administrativa por causa de problemas com a segurança das informações, o nível de importância dado à necessidade de possuir uma política de segurança da informação, passa ser altamente relevante. "*(...) Os serviços ou medidas preventivas devem ser definidos de forma a atender os requerimentos de segurança da política, levando em consideração o equilíbrio entre necessidades de segurança e custos.*" (DIAS, 2000, p. 44).

A elaboração e a implementação de uma Política de Segurança das Informações serve como uma maneira de tomar ações preventivas antes que os problemas com a segurança das informações venham a ocorrer, levando em conta a estrutura da organização, a gestão de riscos e a conformidade com a legislação.

# 5. PLANO CORPORATIVO DE SEGURANÇA DO ESTADO DE MINAS GERAIS

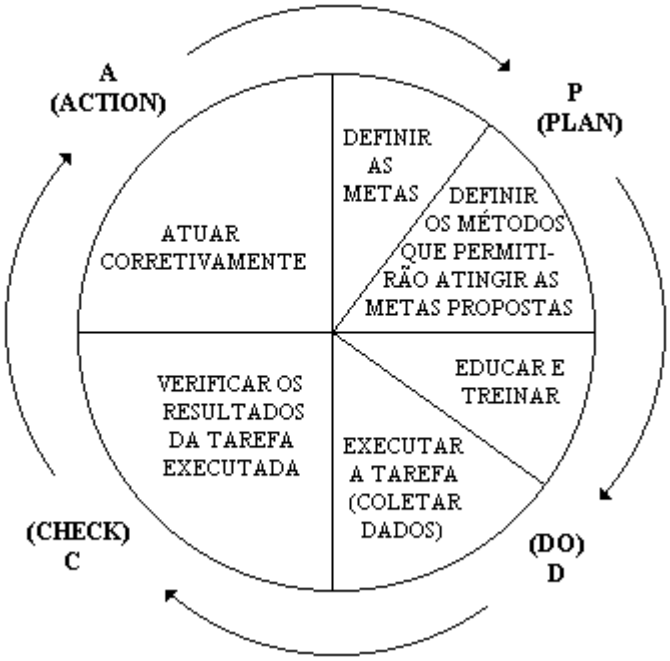
O Governo do Estado de Minas Gerais em consonância com o Programa de Governança Eletrônica elaborou e implementou em 2005 o Plano Corporativo de Segurança da Informação do Governo do Estado de Minas Gerais, com a participação das Secretarias de Estado de Fazenda (SEF/MG), de Planejamento e Gestão (SEPLAG) e a Companhia de Tecnologia da Informação de Minas Gerais (PRODEMGE).

O objetivo era que esses órgãos alcançassem o nível desejado de segurança adotando novas tecnologias como recurso estratégico para disseminação de informações sendo ainda um canal de comunicação junto a outros órgãos do governo, fornecedores e cidadão, considerando os princípios básicos de segurança da informação. (LAIA e LARA, 2007, p. 63-64)

No primeiro momento o objetivo era “Estabelecer a política, objetivos, processos e procedimentos do Sistema de Gestão de Segurança da Informação (SGSI), relevantes para a gestão de riscos e a melhoria da segurança da informação...” (LAIA e LARA, 2007, p. 65).

Para isso era necessária a utilização de um sistema de gestão que permitisse o gerenciamento dos processos organizacionais. A figura 1 exemplifica o modelo de gestão conhecido como “Ciclo PDCA” adotado para implementação do Plano Corporativo de Segurança.

Figura 1 – Ciclo PDCA




Fonte: http://www.pmportal.com.br/2008/03/ciclo-pdca-ou-ciclo-de-deming/.

Este modelo objetiva organizar a gestão de segurança em quatro fases, iniciando em P= *Plan* momento do planejamento e onde são estabelecidos: objetivos (metas), e procedimentos (metodologias), processo necessário para atingir os resultados. Na fase D = *Do* ocorre a execução das atividades definidas no planejamento. Na fase C = *Check* ocorrem as verificações e acompanhamento sistematizado do que foi planejado e finalmente na fase A = *Act* verifica se o resultado esperado foi alcançado, corrige-se as falhas e novos planos de ação, se necessários, são elaborados e postos em prática.

Em detrimento ao modelo adotado foram realizadas ações visando: a elaboração do Plano Diretor de Segurança (PDS) com a definição de atividades que seriam executadas a curto, médio e longo prazos para o período de três anos; a elaboração do Plano de Continuidade de Negócios (PCN) para os Ativos de TI; foi realizada a Análise de Risco em processos, pessoas, sistemas e tecnologia; foram elaboradas as Políticas de Segurança da Informação (PSI); e, finalmente, foi realizada a campanha de divulgação da segurança da informação no âmbito da SEF, envolvendo todos os servidores públicos e prestadores de serviço.

Este foi apenas o início do trabalho para se elevar o nível de segurança das informações nos órgãos estaduais, uma vez que, iniciada a gestão de segurança da informação é contínua e permanente.

O objetivo é que este projeto seja expandido para os demais órgãos e entidades da administração pública de Minas Gerais, bem como seja publicada uma Política Corporativa de Segurança da Informação, e consolidado um modelo de Gestão em Segurança da Informação já visando a Cidade Administrativa, obra do governo de Minas Gerais, proposta para estar em atividade em 2010, onde funcionarão todas as unidades da administração pública.

# 6. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Em qualquer organização a pré-disposição às ameaças é igual, a relevância é ainda maior se as informações trafegam em meio virtual sem os devidos cuidados de proteção. Coloca a organização em exposição total a qualquer tipo de incidente, podendo ser irreversível.

Em ambientes controlados, a organização define se é possível, ou não, conviver com o risco ao qual está exposta e toma as devidas providências para colocar o ambiente em patamares de segurança gerenciáveis.

A gestão das vulnerabilidades e ameaças às quais estão sujeitas as organizações é feita por ferramentas tecnológicas específicas disponíveis no mercado e oferecerá subsídios para avaliar quais são os processos mais críticos na estrutura organizacional, os que precisam ser melhorados quais são os riscos com os quais se pode conviver sem comprometer os negócios da instituição.

Nakamura e Geus (2002, p. 96) apresentam quatro importantes elementos a serem observados no combate às ameaças: "*vigilância, atitude, estratégia e tecnologia".* A vigilância serve para toda a organização que precisa entender a importância da segurança; a atitude solicita a cumplicidade por parte de todos os usuários; a estratégia diz que as definições da política precisa de um plano de defesa e não causar impacto ao ambiente; a tecnologia, onde a solução ideal para a organização é aquela que melhor supre as necessidades estratégicas da organização.

Conhecer as vulnerabilidades, possuir ferramentas tecnológicas que permitam combater as ameaças, modernizar o parque tecnológico, investir em capacitação dos profissionais são medidas importantes, mas apenas parte da gestão. É necessário que a organização possua normas visando a orientar todos os usuários para a segurança da informação observando os requisitos do negócio, bem como as leis e regulamentações relevantes.

Essas normas constituem a Política de Segurança da Informação (PSI) que é um conjunto de documentos que contêm os princípios de segurança da informação da

organização. Esses documentos constituirão o eixo norteador das atividades realizadas, observando os "... *aspectos humanos, culturais e tecnológicos de uma organização, levando também em consideração os processos de negócios.* Nakamura e Geus (2002, p. 94)

Deve existir de maneira formal elaborada conforme os objetivos da organização, resumindo "... *os princípios de SI que a organização reconhece como sendo importantes e que devem estar presentes no dia-a-dia de suas atividades.*" (RAMOS, 2006, p. 87)

A PSI deve conter detalhamentos do que pode e do que não pode ser acessado pelos usuários dos sistemas e serviços, considerando que a melhor política é a que é construída em conjunto, considerando as sugestões e peculiaridades da instituição.

Nakamura e Geus (2002, p. 98) elencam algumas considerações pertinentes à segurança da informação que podem auxiliar os responsáveis pela elaboração dos documentos com níveis de detalhamento que permita cercar domínios que a organização considerou relevante ser tratado:

a) Conheça seus possíveis inimigos;
b) Contabilize os valores,
c) Identifique, examine e justifique suas hipóteses;
d) Controle seus segredos;
e) Avalie os serviços estritamente necessários para o andamento dos negócios da organização;
f) Considere os fatores humanos;
g) Conheça seus pontos fracos;
h) Limite a abrangência do acesso;
i) Entenda o ambiente;
j) Limite a confiança;
k) Nunca se esqueça da segurança física;
l) A segurança é complexa;
m) A segurança deve ser aplicada de acordo com os negócios da organização;
n) "As atividades de segurança formam um processo constante, como carpir a grama do jardim. Se isso não for feito regularmente, a grama (ou os *hackers*) cobrirá seu jardim."

Considerando também que indistintamente todos os usuários serão guiados por esta norma é importante que os responsáveis pela criação conheçam todo o contexto organizacional e as questões culturais que envolvem as pessoas elaborando um documento simples, claro, objetivo, de forma que não haja interpretações errôneas.

Podemos pegar como exemplo Pignatari (p.33) *apud* Machado (2003, p.117) nesta pequena história:

> Um garoto recém-alfabetizado costumava passar, em companhia da irmã, já ginasiana, em frente a um edifício onde se lia “Escola de arte... onde se ensina arte”. “Escola de arte... que é isso?” E a irmã: “Escola de arte... onde se ensina arte”. E ele: “Puxa!... Deve ser uma bagunça!” Para ele, “arte” significava “molecagem”, “peraltice”, de acordo com o repertório que lhe forneciam os ralhos da mãe (“Esse menino vive fazendo arte”)

Com esse relato é possível perceber que uma PSI deve conter normas e procedimentos claros, que não dê margem para subjetividade, uma vez que a diversidade de origens culturais das pessoas que compõem a organização fará com que cada um faça a leitura e a contextualize conforme sua vivência. Por isso um dos grandes aliados na divulgação da PSI no âmbito da organização é o processo de conscientização, bem como a discussão acerca dos documentos que a compõem.

A PSI não está determinada em apenas um único documento. Dada a abrangência que assume dentro da organização é uma composição de diretrizes, normas, procedimentos e instruções de trabalho que serão os norteadores da organização, e serão seguidos por todos os usuários dos sistemas e serviços, uma vez que esse conjunto de normas:

> Estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa; portanto a política deve ser personalizada.” (SÊMOLA, 2003, p. 105)

Será esse conjunto de normas que irá proporcionar proteção às informações, organização do ambiente tecnológico, maior controle sobre os recursos e garantir a finalização dos negócios da instituição.

Muitos obstáculos precisam ser ultrapassados para a implementação da PSI na organização. É imprescindível o apoio gerencial. Sem ele, mesmo que toda a política esteja devidamente estruturada, tanto em documentos, quanto em recursos materiais e tecnológicos que lhe sustentem, não haverá sucesso.

Nakamura e Geus (2002, p. 101) citam alguns obstáculos que os gerentes podem apontar quando da preparação para a implementação da PSI na organização:

a) Desculpe, não existem recursos financeiros suficientes, e as prioridades são outras.
b) Por que você continua falando sobre a implementação da política?
c) Foram feitos todos os esforços para o desenvolvimento da política, isso e tudo?
d) Temos realmente que fazer tudo isso?
e) O que você quer dizer com existem dependências?
f) O que você quer dizer com ninguém sabe o que fazer depois?
g) Desculpe isso é muito complexo.
h) A política de segurança vai fazer com que eu perca meu poder?
i) Por que eu tenho que me preocupar com isso? Esse não é o meu trabalho.
j) Não podemos lidar com isso, pois não temos um processo disciplinar.

É importante salientar que a implementação de uma PSI tem como um dos principais objetivos diminuir custos e não o contrário, conforme Dias (2000, p.101):

> (...) seu desenvolvimento ajuda a diminuir, e não a aumentar, os custos operacionais. Isso porque a especificação dos recursos a serem protegidos, dos controles e das tecnologias necessárias e de seus respectivos valores resulta em um melhor controle e no gerenciamento da segurança em nível organizacional, em oposição à dificuldade de gerenciamento de soluções isoladas (...) (DIAS, 2000, p. 101)

Segundo a ABNT ISO/IEC 17799:2005, (p. 8), o objetivo da PSI é "*Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes*." A Norma ainda reforça que o documento da política precisa ser "... *aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes*."

A implementação da PSI na organização visa à proteção do negócio. Alguns dos objetivos a serem atingidos são: "*proteção da imagem da organização; proteção de segredos corporativos ou industriais; minimizar os problemas de indisponibilidade de sistemas.*" ARAÚJO (2006, p. 89).

A Norma ABNT NBR ISO/IEC 17799:2005: (p. 9) recomenda que a política de segurança seja revisada de tempos em tempos, seja por intervalos planejados ou quando ocorrerem mudanças relevantes. Isso irá garantir "*sua contínua pertinência, adequação e eficácia*."

Em pesquisa feita pelo Comitê Gestor da Internet no Brasil (2008), o número de organizações que adotam Política de Segurança passou de 25,61% dos entrevistados em 2006 para 40% em 2007. Mesmo considerando a significância do resultado, ainda está muito longe do esperado, uma vez que é a Política de Segurança da Informação é uma importante aliada aos recursos tecnológicos adquiridos pela organização. É um código de orientação aos colaboradores, que, seguida corretamente, permite a organização diminuir o nível de risco para seu negócio. Verificar o ano e inserir na referência bibliográfica

## 6.1 A Política de Segurança da Informação da SEF/MG

É bem nova a idéia de segurança das informações na administração pública. Embora já existam algumas leis e alguns decretos legislando sobre procedimentos para tratar as informações, estejam elas em meio material ou magnético.

Governo Federal, reconhecendo a importância de tratar a segurança das informações, publicou o Decreto nº 3.505 (BRASIL, 2000) que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

A SEF/MG foi um dos primeiros órgãos estaduais a publicar a norma de segurança da informação, o que aconteceu em 2006.

A elaboração da Política de Segurança da Informação da SEF/MG (PSI – SEF/MG) teve início com o trabalho em conjunto desenvolvido com a SEPLAG e PRODEMGE, onde foram elaboradas normas que visassem à proteção das informações, que de acordo com Laia e Lara (2007, p. 66) a PSI elaborada foi considerada como "... *um exemplo exitoso de política realizada de forma corporativa*."

Considerando que a PSI das organizações devam ser elaboradas conforme as características de cada organização, a SEF/MG deu continuidade a esta atividade elaborando outras normas e procedimentos de acordo com as peculiaridades, ou seja, considerando a criticidade de suas informações, seu parque tecnológico, estrutura organizacional, dentre outras.

Uma vez elaborada a PSI a mesma precisava ser aprovada pelo Conselho Gestor de Segurança Institucional da SEF/MG – CGSINS, conselho este criado com a publicação da Resolução nº 3.700 (SEF/MG, 2005), cujas competências foram definidas no artigo 1º:

> "Fica instituído o Conselho Gestor de Segurança Institucional - CGSINS, o qual incumbe deliberar sobre as diretrizes de elaboração, implantação, acompanhamento e aperfeiçoamento da execução da política de segurança institucional, no âmbito da SEF/MG."

Em 22 de dezembro de 2006 foi publicada a Resolução nº 3.839, (SEF/MG, 2006) que veio instituir as diretrizes da PSI no âmbito da SEF/MG. No § 1º do Art. 1º estatui que:

> "A Política de Segurança da Informação da SEF/MG é constituída por um conjunto de diretrizes e normas que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas por suas unidades administrativas."

Estabelece a Resolução nº 3.839, (SEF/MG, 2006) no artigo 4º que as diretrizes da PSI da SEF/MG são:

I) Proteção da Informação
II) Classificação da Informação
III) Controle de acesso às informações
IV) Educação em Segurança da Informação
V) Responsabilidade pela Segurança da Informação
VI) Gestão de Continuidade do Negócio

Uma vez publicada a Resolução nº 3.839 (SEF/MG, 2006), em 26 de dezembro do mesmo ano o CGSINS regulamentou a PSI da SEF/MG, por meio da Deliberação CGSINS nº 003 (SEF/MG, 2006).

Ambas as legislações visam que a SEF/MG proteja as informações em uso estabelecendo salvaguardas contra ações não autorizadas envolvendo os processos e os recursos humanos, tecnológicos e físicos da instituição.

# 7. PENALIDADES NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA SEF/MG

A elaboração da Política de Segurança da Informação não tem uma receita pronta. As orientações referentes às penalidades são vinculadas à elaboração de um documento que preveja possíveis ilícitos e conforme o negócio da organização. Via de regra este documento deve ser claro o suficiente para não haver duplas interpretações.

Para dar conformidade à norma, é pré-requisito que sejam criados mecanismos de gestão sobre todos os ativos de tecnologia. É unânime o entendimento de que a implementação da PSI em qualquer organização precisa contar com vários fatores, porém dois ressaltam: é imprescindível o apoio institucional e o processo educativo dos usuários dos sistemas e serviços disponibilizados deve ser constante.

Posteriormente à implementação da PSI deve ser feita, em períodos regulares, a auditoria na política verificando sua conformidade e propondo ajustes, se necessário. Um fator extremamente relevante para auditar uma política de segurança da informação é ter recursos necessários, tanto de profissionais capacitados quanto de ferramentas tecnológicas específicas. Isso permitirá uma maior eficiência na coleta de informações ou levantamento de dados referentes a uma possível infração tendo a chance de analisar o contexto antes de penalizar o usuário.

Para Nakamura e Geus (2002, p. 100):

> A política de segurança deve definir também, do modo mais claro possível as punições e os procedimentos a serem tomados, no caso do ao cumprimento da política definida. Esse é um aspecto importante que precisa ser definido para que os abusos sejam evitados e para que os usuários tenham consciência de que a política de segurança é importante para o sucesso da organização.

Em algumas políticas de segurança é possível verificar que existe uma norma específica para infrações com suas respectivas penalidades, conforme citado por Peck (2005b)

> A Política de Segurança da Informação costuma vir acompanhada de uma série de normas específicas que detalham o aspecto operacional, de execução da mesma. Como exemplo destas normas temos:
>
> .....
>
> • Norma de Infrações e Penalidades
> .....

Em algumas literaturas pesquisadas as normas já trazem um capítulo específico para tratar as infrações instituindo as penalidades ou são elaboradas normas específicas para tratar o tema. Os governos federal e estadual já elaboraram algumas normas específicas, conforme exemplificado a seguir:

> Lei nº 6.437 (BRASIL, 1977) Configura infrações à legislação sanitária federal, estabelece as sanções respectivas, e dá outras providências.
>
> LEI Complementar nº 083 (RORAIMA, 2004) Define as infrações e penalidades a serem aplicadas no caso de descumprimento das normas referentes à segurança contra incêndio e pânico no âmbito do Estado de Roraima e dá outras providências.

Para não penalizar injustamente um usuário e provocar animosidades por parte do corpo organizacional é preciso ter como comprovar que a ação foi cometida e que a mesma foi intencional. Para tanto é necessário que a organização possua ferramentas específicas de controles de acesso aos sistemas e serviços disponibilizados, cujo uso esteja expresso na PSI.

A instituição de penalidades numa organização deve ser pensada como recurso em segunda instância, uma vez que é importante criar uma política preventiva e, em primeiro momento, a maior interessada na segurança é a organização. Isso gera menos animosidades por parte dos usuários e favorece a colaboração de todos.

> A política de segurança é um mecanismo preventivo de proteção de dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos e externos. (DIAS, 2000, p. 48)

Para o sucesso da implementação da PSI na organização, o setor competente já deve ter definido de antemão, conforme as características de cada atividade, quais os privilégios a serem dados ao colaborador para a realização de suas tarefas.

Deve ser dada ao usuário permissão de acesso ao que é estritamente necessário para a realização das atividades e essas permissões só devem ser alteradas se comprovada a real necessidade. Tratamentos especiais devem ser dados aos que forem fundamentadamente justificados, devendo ser criadas normas específicas para acesso a sistemas, serviços e áreas sensíveis.

Atualmente as empresas já adotam o procedimento de capacitar seus novos funcionários nas primeiras horas em que o mesmo ingressa, onde é cientificado das normas internas, da política de segurança das informações e assinando contrato de sigilo, quando for lidar diretamente com informações críticas[12] da organização.

Na administração pública é pouco comum ação punitiva embasada nas legislações criminal ou penal, uma vez que a administração pública tem seus próprios códigos de conduta ética. Mesmo assim todo servidor público já responde administrativa, e também penal e criminalmente por faltas cometidas. Mas são bem poucos os casos que resultam em processos administrativos.

Em sistemas corporativos, como é o caso da administração pública, qualquer pessoa também já responde civil e penalmente. Isso, aliado ao fato de mudanças ocorridas na legislação quanto ao direito eletrônico, já resulta num número expressivo, e cada dia mais crescente, de jurisprudências sobre o uso indevido dos recursos das organizações, devido aos crimes cometidos neste ambiente causando grandes transtornos e prejuízos para as organizações. Prejuízos esses, que, de acordo com as estatísticas, são causados, em sua maioria, por ex-funcionários ou por funcionários insatisfeitos.

Atualmente as questões legais acerca do uso indevido dos recursos tecnológicos disponibilizados pela empresa ao empregado geram polêmicas. Não só no Brasil, mas também em outros países. A utilização e disponibilização dos recursos ao

[12] Informações críticas são aquelas cuja perda poderá causar impacto aos negócios da organização.

empregado são necessárias, porém o risco também é igualmente alto. Um simples e-mail pode resultar em grandes problemas.

Blum e Jimene (2007, p. 40), em seus estudos referentes ao uso indevido dos sistemas corporativos, apresentaram uma sentença da Corte de Recursos da Califórnia, onde foi julgada improcedente a ação de responsabilizar o empregador por e-mail ilícito enviado pelo empregado:

> (...) a Corte entendeu que a conduta indevida praticada pelo empregado foge por completo do escopo da empresa, devendo a mesma ser imunizada em relação à má utilização de seus sistemas informáticos... afastando assim a responsabilidade pelo ilícito.

Apresentam também Blum e Jimene (2007, p. 40) no mesmo estudo, um julgamento de caso semelhante em tribunal brasileiro que resultou em ação penalizando a empresa a indenizar por danos morais o reclamante porque deixou *"... de tomar as providências para apuração de e-mail de conteúdo ofensivo à honra do empregado é responsável pela indenização dos danos morais sofridos por este."*

Uma vez que ainda não há uma legislação específica para o caso é recomendado que as organizações adotem medidas de proteção às suas informações por meio de instrumento jurídico *"... através deles é possível adotar monitoração de e-mail e limitar o uso das máquinas para fins estritamente profissionais."*

Em ambos os casos a intervenção da justiça foi conforme as provas apresentadas. Embora o julgamento tivesse sido por envio de mensagens com conteúdo ilícito ou ofensivo, cada corte aplicou sentença diferente inocentando a empresa ou culpando-a por não gerir devidamente seus recursos.

As organizações, para se resguardar de possíveis ilícitos que porventura venham a ser cometidos pelos colaboradores, vêm elaborando contratos de trabalho contendo cláusulas de confidencialidade.

De acordo com o IDG*Now* (2008) um levantamento feito pelo Superior Tribunal de Justiça identificou que o número de decisões judiciais envolvendo crimes eletrônicos passou de 400, em 2002, para mais de 17.000 atualmente. De acordo com grande parte dos magistrados, advogados e consultores jurídicos, 95% dos delitos

cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizar crimes comuns praticados por meio da internet. Os 5% abrangem transgressões que só existem no mundo virtual, como a distribuição de ameaças digitais[13].

A Deliberação CGSINS nº 003, (SEF/MG, 2006) é o documento que contém a deliberação do Conselho Gestor de Segurança SEF/MG acerca dos procedimentos para boa gestão dos recursos tecnológicos e informacionais disponibilizados visando a garantir ao usuário o direito de ter à sua disposição os recursos necessários à devida realização de suas atividades. Isso que dizer que a SEF/MG deve proporcionar aos usuários um ambiente seguro, orientando-os devidamente sobre os corretos usos e trato às informações, sistemas e serviços, tendo também ferramentas que permitam realizar o controle de acesso.

O corpo organizacional da SEF/MG é composto por servidores públicos e por profissionais que prestam serviços específicos, como é o caso da administração dos ambientes tecnológicos cujas equipes são compostas por servidores públicos e profissionais contratados.

Considerando que ambos acessam a rede fazendária, são considerados, portanto usuários dos serviços e sistemas da SEF/MG, ambos orientados pela mesma PSI, ressalvadas as atribuições e privilégios de acesso.

Resolução nº 3.839 (SEF/MG, 2006) que instituiu as diretrizes da PSI/SEF e estabeleceu em artigo 3º estabelece princípios e conceitos, definiu no inciso VII que Usuário é *toda pessoa à qual se aplica a Política de Segurança da Informação.*

O artigo 2º da citada Resolução define que a PSI/SEF se aplica a todo e qualquer usuário dos sistemas e serviços da SEF/MG.

> *A Política de Segurança da Informação da SEF/MG se aplica a todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em suas unidades administrativas, ou fora delas, em razão do acesso às informações da SEF/MG.*

[13] Vírus, worms, cavalos de tróia, dentre outros

Portanto, todos que acessam a rede fazendária são usuários e a PSI/SEF se aplica a todos indistintamente, podendo ser auditados de igual forma, uma vez que o acesso aos serviços e sistemas disponibilizados na rede fazendária é orientado por normas específicas e caso venham a violá-las poderão responder aos dispositivos legais definidos.

Neste sentido, dois capítulos da Deliberação CGSINS nº 003 (SEF/MG, 2006) merecem destaque: *Capítulo XII – VEDAÇÕES*, contendo quais ações não são permitidas na rede fazendária e *Capítulo XIV – PENALIDADES* composto unicamente pelo Artigo 108: que define: *"O não cumprimento deste normativo está sujeito às penalidades previstas em lei."*

No âmbito da organização, a lei pode ser entendida como o conjunto de normas existentes que devem ser seguidas por todos, sendo que já respondem administrativa, civil e penalmente.

De acordo com as normas internas instituídas (políticas, códigos de conduta, estatutos, dentre outros) na SEF/MG, os prestadores de serviços especializados também estão submetidos às mesmas. O Código de Conduta Ética do Servidor Público e da Alta Administração Estadual, instituído pelo Decreto nº 43.885 (Governo de Minas Gerais, 2004) no Artigo 29 define que:

> Está também sujeito ao Código de que dispõe este Decreto todo aquele que exerça, ainda que transitoriamente e sem remuneração, por eleição nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em órgão ou entidade da Administração Pública Direta e Indireta do Estado, conforme o disposto no parágrafo único do art. 4º do Decreto nº. 43.673, de 2003.

Portanto, aos profissionais contratados também podem ser aplicadas as penalidades previstas no referido código, assim como foi instituído na PSI/SEF-MG, quando da definição de quem são os usuários dos serviços e sistemas disponibilizados

Como em qualquer local de trabalho os usuários dos recursos tecnológicos da SEF/MG têm direitos, mas também têm obrigações.

O Capítulo I – Dos princípios e Valores Fundamentais, do Código da Conduta Ética do Servidor Público, define quais são os deveres e o que é vedado ao servidor:

> Art. 1º - A conduta do servidor público reger-se-á, especialmente, pelos seguintes princípios e valores:
> I - boa-fé;
> II - honestidade;
> III - fidelidade ao interesse público;
> IV - impessoalidade;
> V - dignidade e decoro no exercício de suas funções;
> VI - lealdade às instituições;
> VII - cortesia;
> VIII - transparência;
> IX - eficiência;
> X - presteza e tempestividade;
> XI - respeito à hierarquia administrativa;
> XII - assiduidade; e
> XIII - pontualidade.

Artigo 5º - Dos deveres éticos fundamentais do servidor.

> I – agir com lealdade e boa-fé;
> II – ser justo e honesto no desempenho de suas funções e em suas relações com demais servidores, superiores hierárquicos, e com os usuários dos serviços;
> ...
> XII – comunicar imediatamente a seus superiores todo e qualquer ato ou fato contrário ao interesse público, exigindo as providências cabíveis;
> ...
> XVI – manter-se atualizado com as instruções, as normas de serviço e a legislação pertinentes ao órgão onde exerce suas funções;
> ...
> XVIII – exercer sua função, poder ou autoridade visando exclusivamente à finalidade pública da qual são instrumentos de concretização, ficando vedado o exercício com finalidade estranha ao interesse público, mesmo que observadas as formalidades legais;
> ...
> XIX – observar os princípios e valores da ética pública;
> ...

Artigo 6º - É vedado ao Servidor Público.

> ...
> IX – alterar ou deturpar o teor de documentos que deva encaminhar para providências;
> ...
> XII – retirar da repartição pública, sem estar legalmente autorizado, qualquer documento, livro ou bem pertencente ao patrimônio público;
> XIII – fazer uso de informações privilegiadas obtidas no âmbito interno de seu serviço, em benefício próprio, de parentes, de amigos ou de terceiros;
> ...

Pelo Código de Conduta Ética, a violação das normas acarretará as seguintes providências por parte da Comissão de Ética:

> I – advertência verbal, aplicável nos casos de menor gravidade; ou
>
> II – censura ética, nos casos de maior gravidade ou de reincidência no inciso anterior.
>
> § 1º A censura de que trata o inciso II deste artigo consistirá em um documento escrito, fundamentado em parecer com ciência do faltoso.
>
> § 2º Configurada a gravidade da conduta do servidor público ou sua reincidência, deverá a Comissão de Ética encaminhar a sua decisão e respectivo expediente para a Superintendência Central de Correição Administrativa da Auditoria-Geral do Estado.

Assim, todos os usuários dos sistemas e serviços da SEF/MG que porventura venham a cometer alguma infração também podem ser enquadrados nos dispositivos de penalidades constantes no Código de Conduta Ética.

Já no caso da Lei Estadual nº 869 (Governo de Minas Gerais, 1952), dispõe sobre o Estatuto dos Servidores Públicos Civis do Estado de Minas Gerais, as orientações e os dispositivos de penalidades cabem apenas aos servidores públicos civis, não sendo parâmetro para o conceito de usuário dos sistemas e serviços da SEF.

> ...
>
> Artigo 79 – O funcionário efetivo preso preventivamente, pronunciado por crime comum ou funcional, ou condenado por crime inafiançável em processo no qual não haja pronúncia, será considerado afastado do exercício, até condenação ou absolvição, passada em julgamento.
>
> ...
>
> Artigo 107 – a demissão será aplicada como penalidade.
>
> ...
>
> Artigo 208 – pelo irregular exercício de suas atribuições, o funcionário responde civil, penal e administrativamente.
>
> ...
>
> Artigo 218 – A autoridade que tiver ciência ou notícia da ocorrência de irregularidade no serviço público é obrigada a promover-lhe a apuração imediata, por meios sumários, inquérito ou processo administrativo.
>
> Parágrafo Único – o processo administrativo precederá sempre à demissão do funcionário.
>
> ...
>
> Artigo 232 – quando o funcionário se imputar crime praticado na esfera administrativa, a autoridade que determinar a instauração do processo administrativo providenciará para que se instaure simultaneamente o inquérito policial.
>
> Artigo 233 – Quando a infração estiver capitulada na lei penal, será remetido o processo à autoridade competente, ficando traslado na repartição.
>
> ...

> Artigo 244 – São penas disciplinares:
>
> I – Repreensão;
>
> II – Multa;
>
> III – Suspensão;
>
> IV – destituição de função;
>
> V – Demissão;
>
> VI – Demissão a bem do serviço público.
>
> Artigo 245 – A pena de repreensão será aplicada por escrito em caso de desobediência ou falta de cumprimento de deveres.
>
> Parágrafo Único – Havendo dolo ou má-fé, a falta de cumprimento de deveres será punida com a pena de suspensão.
>
> Artigo 246 – A pena de suspensão será aplicada em caso de:
>
> I – falta grave;
>
> ...
>
> III – desrespeito às proibições consignadas neste estatuto;
>
> ...
>
> Artigo 247 – A pena de multa será aplicada na forma e nos casos expressamente previstos em lei ou regulamento
>
> ...
>
> Artigo 250 – Será aplicada a pena de demissão a bem do serviço ao funcionário que:
>
> III – revelar segredos de que tenha conhecimento em razão ou função, desde que o faça dolosamente e com prejuízo para o Estado ou particulares;
>
> ...
>
> ...
>
> Artigo 273 – A responsabilidade administrativa não exime o funcionário da responsabilidade civil ou criminal, que no caso couber, nem o pagamento da indenização a que ficar obrigado o exime da pena disciplinar em que incorrer.
>
> ...

Caso ocorra algum evento que necessite da atuação da Comissão de Ética ou do Conselho Gestor de Segurança Institucional, a chefia imediata deve atuar tomando as providências necessárias e encaminhando formalmente a solicitação de apuração do fato ao órgão competente.

A falta de orientação e esclarecimentos ao usuário referentes às normas existentes e sobre o uso dos recursos disponibilizados aumenta a possibilidade da ocorrência de incidentes de segurança, demonstrando que nem toda infração é voluntária e necessariamente não requer punição e sim orientação. Neste caso é necessário que a organização intervenha e oriente ao usuário qual o caminho correto a ser seguido informando que as sanções serão aplicadas numa reincidência.

A sensibilização do usuário quanto aos corretos usos dos recursos disponibilizados, é o primeiro passo para ter aliados no processo de conscientização da PSI, pois *"Na verdade, nenhuma empresa quer punir: o ideal é educar e evitar riscos e responsabilidades legais para o funcionário e a empresa."* (PINHEIRO, 2008, p. 136).

Num processo de gestão por governança o objetivo é verificar também porque o ato foi cometido. Isso permite que se reveja o próprio processo para verificar as falhas, que se cometidas conscientemente, podem não ser voluntárias.

Os governos tomam iniciativas para manter a vigilância sobre as informações que trafegam na rede. Uma das medidas é elaborar legislações específicas (quadro 2) que tratam sobre segurança da informação e que permitam traçar um caminho juridicamente viável e que permita a proteção ao cidadão. No Brasil existem alguns projetos de leis e algumas leis que já estão em vigor.

Quadro 2 – Dispositivos legais na legislação brasileira

| Legislação | Data | Assunto |
|---|---|---|
| Instrução Normativa nº 001 | 18.06.2008 | Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta. |
| Projeto de Lei nº 2.196 | 09.10.2003 | Dispõe sobre a divulgação de mensagens pelos usuários de provedores na Internet e demais redes de computadores abertas ao uso do público. |
| Projeto de Lei nº 123 | 21.02.2003 | Veda a transmissão a terceiros de dados relativos a pessoas naturais e jurídicas. |
| Projeto de Lei nº 18 | 18.02.2003 | Veda o anonimato dos responsáveis por páginas na Internet e endereços eletrônicos registrados no país. |
| Decreto nº 4.553 | 27.12.2002 | Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal e dá outras providências. |
| Projeto de Lei nº 7.093 | 06.08.2002 | Dispõe sobre a correspondência eletrônica comercial, e dá outras providências. |
| Projeto de Lei nº 6.210 | 05.03.2002 | Limita o envio de mensagem eletrônica não solicitada ("spam") por meio da Internet. |
| Lei nº 9.983 | 14.07.2000 | Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. |
| Projeto de Lei nº 3.356 | 28.06.2000 | Dispõe sobre a oferta de serviços através de redes de informação. |
| Projeto de Lei nº 3.303 | 27.06.2000 | Dispõe sobre normas de operação e uso da Internet no Brasil |
| Decreto Federal nº 3.505 | 13.06.2000 | Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal |
| Projeto de Lei nº 3.016 | 16.05.2000 | Dispõe sobre o registro de transações de aceso a redes de computadores destinados ao uso público, inclusive a Internet |
| Projeto de Lei nº 76 | 27.03.2000 | Define e tipifica os delitos informáticos. |

| Legislação | Data | Assunto |
|---|---|---|
| Projeto de Lei nº 1.589 | Set./1999 | Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital e dá outras providências. |
| Projeto de Lei nº 84 | 24.02.1999 | Dispõe sobre os crimes cometidos na área de informática e suas penalidades. |
| Lei nº 9.609 | 19.02.1999 | Dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no país. |
| Decreto nº 2.910 | 29.12.1998 | (revogado pelo Decreto nº 4.553, de 27 de dezembro de 2002) – Estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e sistemas de informação de natureza sigilosa. |
| Lei nº 9.610 | 19.02.1998 | Altera, atualiza e consolida a legislação sobre direitos autorais. |
| Lei nº 9.296 | 24.07.1996 | Regulamenta o inciso XII, parte final, do art. 5º, da Constituição Federal. O disposto nessa lei aplica-se a interceptação do fluxo de comunicações em sistemas de informática e telemática. |
| Projeto de Lei do Senado nº 234 | 1996 | Dispõe sobre crimes contra a inviolabilidade de comunicação de dados de computador. |
| Projeto de Lei da Câmara dos Deputados nº 1.713 | 1996 | Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores. |
| Decreto nº 96.036 | 12.05.1988 | Regulamenta a Lei nº 7.646, de 18 de dezembro de 1987, revogada pela Lei nº 9.609, de 19 de fevereiro de 1998. |
| Decreto nº 79.099 | 06.01.1977 | Aprova o regulamento para salvaguarda de assuntos sigilosos. |

Fonte: Pinheiro (2008)

A grande discussão, e que reforça que a aplicabilidade das penalidades é necessária, decorre da impunidade vislumbrada na Administração Pública, onde só seria coibida se realmente fossem instituídas penas para as faltas cometidas.

Embora contenha na PSI/SEF *que "o não cumprimento deste normativo está sujeito às penalidades previstas em Lei."* a Política de Segurança da Informação da SEF objetiva prover tanto ao usuário quanto à instituição, de recursos com os quais possam ambos exercer suas atribuições de maneira orientada sem a necessidade de aplicação de penalidades, uma vez que o objetivo é ser preventivo e não punitivo. Um processo educativo e constante é o caminho para que o ambiente esteja sempre seguro e o usuário exercendo suas atribuições devidamente.

No cenário mundial o Brasil já configura a lista dos 5 maiores emissores de spam[14] do mundo. Saltou do quinto lugar em dezembro de 2008 para ocupar o segundo lugar em fevereiro de 2009. No primeiro posto estão os Estados Unidos, responsáveis por 23% do spam mundial. O terceiro lugar é da China, com 7%, seguida pela Índia (4%) e pela Coréia do Sul (3%).

[14] SPAM é um termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

A mudança da tecnologia resulta na mudança comportamental e social. A sociedade muda, o direito também precisa mudar. Assim, o direito eletrônico tem se especializado a cada dia. De acordo com Pinheiro (2008, p. XXX ):

> O direito digital consiste na evolução do próprio direito abrangendo todos os princípios fundamentais vigentes introduzindo novos institutos e elementos para o pensamento jurídico em todas as áreas: direito constitucional, civil, autoral, comercial, contratual, econômico, financeiro, tributário, penal, internacional, etc.

É grande a dificuldade na investigação de crimes digitais pela natureza das provas, as pistas são muitas vezes voláteis, tem ainda as discussões acerca da territorialidade reforçando a importância da cooperação internacional para garantir os direitos soberanos e compatibilidade nas decisões jurídicas.

Os crimes virtuais já tipificados pelas legislações brasileiras apresentam penas que vão, desde pagamento de multas, até 12 anos de reclusão. No quadro 3 a seguir, estão apresentados os crimes virtuais mais comumente cometidos.

Quadro 3 – Conseqüências legais para as infrações digitais mais comuns

| Infração praticada | Enquadramento nos códigos | Artigo | Pena |
|---|---|---|---|
| Falar em um chat que alguém cometeu algum crime (ex. - ele é um ladrão...) | Calúnia | 138 do C.P. | Detenção de seis meses a dois anos e multa |
| Dar *forward* para várias pessoas de um boato eletrônico | Difamação | 139 do C.P. | Detenção de três meses a um ano e multa |
| Enviar um email para a pessoa dizendo sobre características dela (gorda, feia, vaca ...) | Injúria | 140 do C.P. | Detenção de um a seis meses ou multa |
| Enviar um email dizendo que "vai pegar" a pessoa | Ameaça | 147 do C.P. | Detenção de um a seis meses ou multa |
| Enviar um email para terceiros com informação considerada confidencial | Divulgação de segredo | 153 do C.P. | Detenção de um a seis meses ou multa |
| Enviar um vírus que destrua equipamentos ou conteúdos | Dano | 163 do C.P. | Detenção de um a seis meses ou multa |
| Copiar conteúdo e não mencionar a fonte, baixar MP3 | Violação ao direito autoral | 184 do C.P. | Detenção de três meses a um ano e multa |
| Criar comunidade online que fale sobre pessoas e religiões | Escárnio por motivo de religião | 208 do C.P. | Detenção de um mês a um ano ou multa |
| Acessar sites pornográficos | Favorecimento da prostituição | 228 do C.P. | Reclusão de dois a cinco anos |
| Criar uma comunidade para ensinar como fazer "um gato" | Apologia de crime ou criminoso | 287 do C.P. | Detenção de três a seis meses ou multa |
| Enviar email com remetente falso (caso comum de *spam*) | Falsa identidade | 307 do C.P. | Detenção de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave |

| Infração praticada | Enquadramento nos códigos | Artigo | Pena |
|---|---|---|---|
| Inserir dados falsos em sistema da administração pública | Adulterar dados em sistema | 313-A do C.P. | Reclusão de dois a doze anos e multa |
| Entrar na rede administração pública e mudar informações (mesmo que com uso de um *software*) | Adulterar dados em sistema de informações | 313-B do C.P. | Detenção de três meses a dois anos e multa |
| Receber spam e devolver com vírus ou com mais spam | Exercício arbitrário das próprias razões | 345 do C.P. | Detenção de quinze dias a um mês ou multa, além da pena correspondente à violência |
| Participar de cassino online | Jogo de azar | 50 da L.C.P. | Prisão simples, de três meses a um ano e multa, estendendo-se os efeitos da condenação à perda dos móveis e objetos de decoração do local |
| Falar mal de alguém em um chat por sua cor | Preconceito ou Discriminação Raça-Cor-Etnia | 20 da Lei 7.716/89 | Reclusão de um a três anos e multa |
| Ver ou enviar fotos de crianças nuas online | Pedofilia | 247 da Lei 8.069/90 | Multa de três a vinte salários de referência, aplicando-se o dobro em caso de reincidência |
| Usar logomarca de empresa em um link na página da internet, em uma comunidade, em um material, sem autorização do titular, no todo ou em parte | Crime contra a propriedade industrial | 195 da Lei 9.279/96 | Detenção de três meses a um ano ou multa |
| Empregar meio fraudulento para desviar clientela de outrem (Exemplo: uso da marca do concorrente como palavra-chave ou link patrocinado em buscador) | Crime de concorrência desleal | 95 da Lei 9.279/96 | Detenção de três meses a um ano ou multa |
| Usar cópia de *software* sem ter a licença para tanto | Crimes contra software, "pirataria" | 12 da Lei 9.609/98 | Detenção de seis meses a dois anos ou multa |

Fonte: Pinheiro, (2005a)

A cada dia cresce o número de fraudes cometidas no meio virtual. Estão disponíveis para consulta no *site* do Centro de Estudos sobre as Tecnologias da Informação e da Comunicação - CETIC.br as estatísticas atualizadas. Só no 2º semestre de 2008 as tentativas de fraude na internet brasileira cresceu 96%, esse "*(...) índice foi impactado por um aumento nas notificações de casos de violação de direitos autorais por meio da distribuição de arquivos protegidos em redes P2P* [15]."

[15] São redes que permitem o compartilhamento de arquivos contendo áudio, vídeo ou dados digitalizados de qualquer natureza entre os usuários da internet.

O CETIC.br é responsável pela produção de indicadores sobre o uso da Internet no Brasil. Realiza anualmente pesquisa para medir o acesso dos usuários domiciliares e das empresas aos recursos tecnológicos e serviços disponibilizados. Os dados consolidados apresentaram que domicílios tiveram um aumento significativo de computadores para o extrato da população que possui renda familiar entre dois e cinco salários mínimos, o acesso à internet via banda larga que ultrapassou a conexão discada, a expansão das *Lan House* sendo o principal local de acesso à internet. Já nas empresas a significância está no uso de novas tecnologias como rede wireless, sistemas de gestão, automatização de processos por meio do comércio eletrônico e do governo eletrônico. As pesquisas foram publicadas em 2008 e referem-se ao período de setembro a novembro de 2007.

Nos estudos feitos pelo CETIC.br referente à segurança na rede, uso dos serviços governamentais, comércio eletrônico e habilidades com computador e internet, 29% dos usuários entrevistados declara ter encontrado problemas de segurança, número esse que aumentou em comparação com os anos de 2005 e 2006. 17% dos municípios brasileiros possuíam computador com acesso à internet e 34% da população era usuária de internet. Houve uma evolução nos hábitos de consumo pela internet e no uso dos serviços disponibilizados pelos órgãos públicos ao cidadão, e praticamente metade da população brasileira já realizou alguma atividade ao computador.

Uma das ações aguardadas pelos usuários da internet no Brasil é a votação do Projeto de Lei Substitutivo proposto pelo senador Eduardo Azeredo, em trâmite pelas comissões de Ciência e Tecnologia, Educação e Constituição, Cidadania e Justiça, que tipifica e criminaliza diferentes tipos de ação criminosa em redes privadas ou públicas de computadores.

# 8. CONSIDERAÇÕES FINAIS

Uma PSI bem elaborada, orientada, esclarecida e colocada em prática por todos os colaboradores, favorece a sociedade, mais que à própria instituição, pois, embora seja um documento interno, seu resultado visa à comunidade uma vez que a Administração Pública existe com a finalidade de atender ao bem comum. A implementação destas políticas contribui diretamente para a diminuição dos incidentes de segurança, pois permitem, que as informações trafeguem em segurança, garantindo assim sua chegada ao destinatário final inalteradas, favorecendo ao cumprimento satisfatório das atividades.

Para a implementação de uma PSI é importante observar dois extremos: o que se deseja proteger e quais são as ações que a organização deve tomar para atingir seu objetivo. Levando em conta que a complexidade e diversidade do grupo de pessoas que constituem a organização, é necessário também considerar que as mesmas possuem conhecimento técnico especializado e, atuantes em áreas críticas. Caso não sejam bem orientadas podem colocar em risco o negócio porque podem ser vítimas das investidas de engenheiros sociais que objetivam obter as informações ou também serem seduzidos por outras organizações com propostas salariais mais atrativas (no caso dos profissionais contratados), ou mudarem de setor e continuar a utilizar os privilégios de acesso e o conhecimento adquirido em benefício da unidade que o recebeu. Por esses motivos as pessoas tornam-se os ativos de maior relevância.

Os documentos que compõem a PSI ao serem elaborados devem considerar que, os indivíduos possuem costumes, valores, códigos de conduta ética e moral diferenciados. As mensagens são recebidas e decodificadas de forma diferenciada por cada indivíduo, podendo resultar em posturas diferenciadas diante às normas implementadas, ou seja, é possível que haja vários comportamentos diante uma mesma medida de segurança, que inicialmente tinha o objetivo de proteger o ativo. Quando de sua elaboração foi considerada clara, mas não se considerou a subjetividade.

A SEF/MG ao cumprir seu papel como uma unidade da administração pública, tem como missão arrecadar recursos para o Estado. Para fazer cumprir essa missão lida diariamente com informações altamente críticas, porque possui sob sua custódia uma base de dados contendo as informações cadastrais de todos os contribuintes do estado. Se uma informação desta base for corrompida ou perdida, pode levar as empresas à falência. São críticos também os planos de ação da fiscalização. Se revelados tendem a aumentar a sonegação fiscal diminuindo a arrecadação, resultando na precariedade dos serviços essenciais prestados à população, uma vez que sem recursos o Estado não pode investir em obras ou serviços de melhoria.

Ao contrário do que pensam a maioria dos usuários a PSI não objetiva cercear espaços e direitos adquiridos e sua implementação. Na SEF/MG não foi diferente. Estes documentos vieram a normatizar um espaço que até então não tinha uma padronização, bem como investiu-se em recursos tecnológicos que permitissem que as informações trafegassem em ambiente protegido.

Ao elaborar sua PSI a SEF/MG reviu todo o cenário organizacional, tecnológico e profissional, definindo alem das orientações prazos para expandir e modernizar os equipamentos de forma a retomar o controle dos diversos trabalhos descentralizados entre as unidades administrativas, em sua maioria desenvolvimento de aplicativos voltados para a agilização das rotinas de trabalho

Um dos grandes problemas vivenciados pela SEF/MG é o grande número de solicitação de serviços que objetivam a agilização das rotinas de trabalho no âmbito da instituição, que conflita diretamente com a falta de profissionais qualificados e com a indisponibilidade de recursos tecnológicos necessários à realização das atividades profissionais. Isso leva muitas vezes o próprio servidor a realizar este trabalho.

Atenta a essa deficiência e ciente da importância, tanto do trabalho desenvolvido pelo servidor, bem como da necessidade de estar conforme as políticas implementadas e vigentes, a SEF/MG buscou modernizar-se em equipamentos e serviços qualificados, esclarecendo aos usuários quais em bases tecnológicas são desenvolvidos os sistemas e serviços disponibilizados. Agindo assim a SEF/MG não

incorre em possíveis processos legais quanto ao uso indevido de *software* ou direitos autorais, retomando o controle sobre seus processos e serviços.

Se, por um lado, o processo de retomadas das suas atribuições gerou um cenário de descrédito por parte de um grupo de usuário, por outro lado, já é possível perceber que, embora a resistência de alguns, o nível de preocupação com as informações disponibilizadas nas estações de trabalho tendeu a aumentar, assim como também cresceu o número de servidores que se preocupam em manter o sigilo das senhas de acesso a sistemas e serviços, bem como estão mais alertas quanto a possíveis sondagens de pessoas inescrupulosas que buscam por meios escusos obter as informações que desejam.

Outro aspecto que vem auxiliando a elevar o nível de segurança foi a modernização e uniformização dos equipamentos, sistemas operacionais dos ambientes tecnológicos reduzindo o exaustivo trabalho de realizar procedimentos diferenciados para manter a funcionalidade e segurança dos equipamentos. Este são apenas alguns resultados já vislumbrados em um curto espaço de tempo que realçam os resultados positivos da implementação das políticas.

A segurança da informação veio contribuir para uma sensível melhoria no processo de governança da SEF/MG, resultado já percebido e reconhecido pelos usuários dos sistemas e serviços tais como: serviço de correio eletrônico mais atualizado, com melhor desempenho, sendo as mesmas resguardadas em segurança permitindo ainda serem acessadas de fora do ambiente corporativo com mais segurança; implementação do controle de acesso aos sistemas e serviços com procedimentos elaborados; aquisição de equipamentos mais potentes e com maior capacidade de armazenamento permitindo que as informações da SEF/MG estejam arquivadas e em local protegido.

A bibliografia consultada referente à aplicação de penalidades caso ocorra algum ilícito infringindo o que foi estabelecido na PSI, não é unânime quanto à imputação de penas. Alguns autores acreditam que o processo educativo funciona; outros, que a organização deve planejar e estruturar seus sistemas devidamente dando a quem de direito as permissões devidas; outros, ainda, acreditam que, em se tratando da

administração pública, existe a impunidade e, neste caso, somente atenuada com penalidades severas; outros, também, acreditam que os códigos de ética, aliados ao civil e penal dão o respaldo legal necessário.

O grande desafio, face ao grande enfoque dado pela mídia referente às graves faltas cometidas (corrupção, cartão corporativo, desvio de verba pública, etc.) é fazer com que os servidores e prestadores de serviços da SEF/MG percebam a importância que a segurança da informação representa, não para a instituição, mas para a sociedade.

Além da PSI/SEF outros documentos de legitimação, também de controle, foram criados para uma gestão ética na administração pública tais como a criação das Comissões de Ética e os Códigos de Conduta Ética na Administração Pública. Porém estes documentos são apenas normativos do que já está instituído pela Constituição Federal referente à segurança da informação na Administração Pública.

Embora requeira o texto do artigo 108 da Deliberação CGSINS nº 003 (SEF/MG, 2006), uma rediscussão sobre seu sucinto texto: ”*o não cumprimento deste normativo está sujeito às penalidades previstas em lei*”, identificando as infrações cometidas e sua penalidade, o documento como um todo tem o respaldo de sanções legais e vigentes para fazer valer o poder de polícia para com aqueles que violem essa norma, uma vez que todos os usuários podem ser penalizados administrativa, civil e penalmente, e a legislação acerca dos crimes cometidos nos meios virtuais está em constante evolução.

Porém considerando que a maioria dos crimes digitais já estão tipificados nos códigos civil e penal e também na Constituição Federal, a relevância em se redigir esses documentos não é uma ação de necessidade imediata.

Embora ainda ocorram ações que violem as normas instituídas, seja pela falta de clareza dos normativos, pela falta de tipificação dos crimes, pela morosidade na atuação das áreas responsáveis, valores como integridade, moralidade, honestidade, responsabilidade social, dentre outros, devem ser reforçados e ressaltados pela sociedade em geral de forma a iniciar um processo de

conscientização, não somente quanto aos usos dos recursos e no âmbito dos ambientes corporativos, mas elevar o nível de consciência da sociedade visando à coletividade.

O objetivo da SEF/MG ao elaborar a PSI foi muito além de ser apenas um procedimento do Plano Corporativo de Segurança do governo estadual, mas visando fazer uma gestão voltada para a conscientização dos usuários tendo em vista a multiplicidade, a existência de várias culturas compartilhando o mesmo espaço.

A elevação do nível de conscientização das pessoas ocorre por intermédios de campanhas de divulgação e sensibilização em segurança da informação as quais a SEF/MG tem realizado sistematicamente como um recurso pedagógico, por acreditar que este é o caminho para uma gestão pública mais consciente e moralmente fortalecida.

É importante salientar que, embora a grande relevância dada pela SEF/MG nas campanhas sensibilização, no processo educativo também é necessário ressaltar as devidas punições quanto aos ilícitos cometidos.

É certamente um momento de mudança, mas dizer a segurança da informação na SEF/MG tende a retroceder ao que era inicialmente é impossível. Não é vislumbrado um retorno no contexto da evolução tecnológica, uma vez que essa evolução permite a automação de processos, a agilização e mais precisão nos resultados, melhor divisão dos tempos e melhor aproveitamento das pessoas.

Todas essas considerações pesadas e medidas conduzem à conclusão de que é necessário um processo de amadurecimento e revisão de conceitos morais da sociedade e não apenas da Administração Pública, enquanto participante de um processo que visa à gestão por governança. A preocupação ultrapassa as fronteiras do ambiente corporativo, devendo ser de cada indivíduo que compõe a sociedade atual, a sociedade da informação.

# 9. REFERÊNCIAS BIBLIOGRÁFICAS


1 AGIA NETO, Tufic Abdala. *Combate às Fraudes e à Corrupção no Setor Público. In Controle Interno na Administração Pública*. Tribunal de Contas do Estado do Rio Grande do Sul – Escola Superior de Gestão e Controle Francisco Juruena, 2007.

2 AGOSTINHO, Denílson Aparecido. *Leis de Segurança da Informação*. Disponível em: <http://www.inf.ufsc.br/~bosco/ensino/ine5630/trabalhos2004-2/artigo-LeisDeSeguranca.pdf>, Acessado em 17.10.07.

3 ALMEIDA, Paulo Roberto de. *Os doze trabalhos da boa governança*. Disponível em: <http://www.espacoacademico.com.br>. [1º versão: Washington, 1º de setembro de 2003] [Revisão: Brasília, 23 de fevereiro de 2004]. Acessado em 04.05.08.

4 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – *ABNT NBR ISO/IEC 17799:2005*: Tecnologia da informação – técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

5 AURÉLIO, Dicionário Eletrônico – O Dicionário da Língua Portuguesa – edição de 1999.

6 BELO HORIZONTE. Secretaria de Estado de Fazenda. *Deliberação CGSINS Nº 003, de 26 de dezembro de 2006*. Regulamenta a Política de Segurança da Informação da SEF/MG.

7 BELO HORIZONTE. Secretaria de Estado de Fazenda. *Portaria CGSINS/SEF nº 001, de 09 de novembro de 2005*. Designa os conselheiros suplentes do Conselho Gestor de Segurança Institucional da Secretaria de Estado de Fazenda de Minas Gerais e o coordenador da Secretaria Executiva.

8 BELO HORIZONTE. Secretaria de Estado de Fazenda. *Resolução nº 3.700, de 28 de setembro de 2005*. Institui o Conselho Gestor de Segurança Institucional da Secretaria de Estado de Fazenda. Diário Oficial do Estado de Minas Gerais, Belo Horizonte, MG, 29 set. 2006.

9 BELO HORIZONTE. Secretaria de Estado de Fazenda. *Resolução nº 3.839, de 22 de dezembro de 2006*. Institui as diretrizes da Política de Segurança da Informação. Diário Oficial do Estado de Minas Gerais, Belo Horizonte, MG, 23 dez. 2006.

10 BELO HORIZONTE. Secretaria de Estado de Planejamento e Gestão. *Resolução nº 011, de 20 de fevereiro de 2006*. Institui a Política de Segurança da Informação. Diário Oficial do Estado de Minas Gerais, Belo Horizonte, MG, 21 fev. 2006.

11 BLUM, Renato Opice. JIMENE, Camilla do Vale. Uso indevido dos sistemas é responsabilidade do empregador? In *Revista Fonte*, Universidade Corporativa Prodemge – Janeiro/junho de 2007 – pág. 39-40.

12 BRASIL. *Constituição da República Federativa do Brasil* – texto promulgado em 05 de outubro de 1988. Senado Federal, Brasília: 2006, Disponível em: <http://www.senado.gov.br/sf/legislacao/const/>. Acessado em 11.10.07.

13 BRASIL. *Decreto nº 3.505, de 13 de junho de 2000*. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Disponível em: <http://www.planalto.gov.br/CCIVIL/decreto/D3505.htm>. Acessado em 11.10.07.

14 BRASIL. *Lei nº 6.437, de 20 de agosto de 1977*. Configura infrações à legislação sanitária federal, estabelece as sanções respectivas, e dá outras providências. Disponível em: <http://www.planalto.gov.br/CCIVIL/Leis/L6437.htm>. Acessado em 17.10.07.

15 CAMARGO, Coriolano Aurélio Almeida. *Aspectos constitucionais e jurídicos sobre a nota fiscal eletrônica*. 2005. Disponível em: <http://www.almeidacamargo.com.br/almeidacamargo/downloads/MAGNA1.ppt>. Acessado em 28.07.08

16 CAMPOS, André. *Sistema de Segurança da Informação: controlando riscos*. Disponível em: <http://www.visualbooks.com.br/bin/01103.pdf>. Acessado em 12.10.07.

17 CARDOSO, Antônio Semerato Rito. *Ética pública: esvoaçante e sem pouso*. Disponível em: <http://portal.ouvidoria.fazenda.gov.br/ouvidoria/ActionServlet?idInformacao=379&objeto=br.com.tellus.ouvidoria.negocio.InformacaoUtil&acao=recover>. Acessado em 01.07.08

18 CARNEIRO, João Geraldo Piquet. et al. *Promoção da ética: a experiência da comissão de ética pública*. In: VII Congresso Internacional do Centro Latino-Americano de Administração para o Desenvolvimento – CLAD, Painel: ética como instrumento de gestão, Lisboa, Portugal, p. 11-27, out./2002.

19 CHAGAS, José Ferreira. Governança Corporativa – Aplicabilidade do Conceito, dos Princípios e Indicadores à Gestão de Pequenas e Médias Organizações. In: *VIII Congresso Internacional de Costos*, 2004, Punta Del Leste. Anais do VIII congresso Internacional de Costos, 2004, V. 01. p. 424-439. Disponível em <http://eco.unne.edu.ar/contabilidad/costos/VIIIcongresso/085.doc>. Acessado em 18.05.08.

20 COMISSÃO DE VALORES MOBILIÁRIOS. *Cartilha de Governança. Recomendações da CVM sobre Governança Corporativa* – Junho 2002. Disponível em: <www.cvm.gov.br>.

21 Comitê Gestor da Internet no Brasil - CGI.br. *Pesquisa sobre o uso das Tecnologias da Informação e da Comunicação no Brasil: TIC Domicílios e TIC Empresas 2007*. São Paulo: Comitê Gestor da Internet no Brasil, 2008. Disponível em: <http://www.cetic.br/>. Acessado em 24.07.08.

22 DIAS, Cláudia. *Segurança e Auditoria da Tecnologia da informação*. Rio de Janeiro: Axcel Books do Brasil, 2000.

23 FREY, Klaus. *Governança Eletrônica: experiências de cidades européias e algumas lições para países em desenvolvimento*. I Conferência Eletrônica do Centro Virtual de estudos Políticos (CEVEP), com o tema Internet, Democracia e Bens Públicos, promovida pelo Departamento de Ciência Política da UFMG e pela empresa de Informática e Informação do Município de Belo Horizonte (Prodabel) entre 01 e 30 de novembro de 2000.

24 GAJANIGO, Mário. *A TI e a Governança Corporativa*. *Decision Report*, 14.07.2006 Disponível em <http://www.cscbrasil.com.br/imprensa/2006/A_TI_e_a_Governanca_Corporativa.pdf>. Acessado em 18.05.2008.

25 MINAS GERAIS. Decreto nº 43.885, de 04 de outubro de 2004. Dispõe sobre o Código de Conduta Ética do Servidor Público e da Alta Administração Estadual. *Diário Oficial*, Belo Horizonte, 04. out. 2004.

26 MINAS GERAIS. *Lei nº 869, de 05 de julho de 1952*. Dispõe sobre o Estatuto dos Funcionários Civis do Estado de Minas Gerais.

27 GRÜN, Roberto. Convergência das elites e inovações financeiras: a governança corporativa no Brasil. *Revista Brasileira de Ciências Sociais*. Vol. 20, nº 58, junho/2005, p. 67-90.

28 HAMELINK, Cees. J. Direitos Humanos para a Sociedade da Informação. In MARQUES DE MELO, J.; SATHLER, L. *Direitos à Comunicação na Sociedade da Informação*. São Bernardo do Campo, SP: Umesp, 2005, pag. 103-151. Disponível em www.wacc.al.net/livros/livrodireitos/cap_tulo4. Acessado em 10.10.2008.

29 HOUAISS, Instituto Antônio. *Dicionário Eletrônico Houaiss da Língua Portuguesa.* Editora Objetiva, versão 1.0, dezembro/2001.

30 INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA – IBGC. *Código das Melhores Práticas de Segurança Corporativa*. 3ª ed. São Paulo: SP, 2003.

31 IDG*NOW*. Disponível em <http://idgnow.uol.com.br/internet/2008/11/25/crimes-eletronicos-geram-17-mil-decisoes-judiciais-no-brasil-em-6-anos/*IDGNoticiaPrint_view*/>. Acessado em 30.11.2008

32 LAIA, Marconi Martins., LARA, Rodrigo Diniz. Ações de segurança da informação no governo mineiro 2005/2007. *Revista Fonte*. Universidade Corporativa da Companhia de tecnologia de Informação do Estado de Minas Gerais. Ano 4 – nº 07 – julho/dezembro 2007, pg. 63-69.

33 LOPES, Cícero. *O que é governança corporativa.* Disponível em: <http://imasters.uol.com.br/artigo/3941/governanca/o_que_e_governanca_corporativa/ Seções relacionadas: Gerência - Governança de TI>. Abr.2006. Acessado em 23.05.2008.

34 MACHADO, Ana Maria Nogueira. Informação do senso comum ao uso científico. In.: *Informação e controle bibliográfico: um olhar sobre a cibernética.* São Paulo: Editora UNESP, 2003. p. 15-25.

35 MACHADO, Sulamita Crespo Carrilho. *Aspectos jurídicos da prevenção e do controle da corrupção*. Disponível em: <http://www.fjp.mg.gov.br/escoladegoverno/index.php?option=com_content&task=view&id=134&Itemid=181>, 2008. Acessado em 05.03.2009.

36 MARINHO, Sérgio. Segurança da Informação: Conceitos e Modelo de Gestão. Nov. 2004. Disponível em: http://www2.dem.inpe.br/ijar/Auditoria%20de%20SI/Aulas/SegInform.pdf, acessado em 11.10.07.

37 MARQUES, Maria da Conceição da Costa. *Aplicação dos princípios da governança corporativa no sector público*. *RAC*, v. 11, n. 2 Abr./Jun. 2007: 11-26.

38 NAKAMURA, Emílio Tissato. e GEUS, Paulo Lício de. *Segurança de redes em ambientes corporativos*. São Paulo: Berkeley Brasil, 2002.

39 NEXTGENERATION CENTER. Curso de Governança Corporativa de Tecnologia da Informação. Disponível em http://www.scribd.com/doc/3808623/-Gerenciamento-Governanca-Corporativa?autodown=pdf. Acessado em: 29.06.09.

40 Organização das Nações Unidas – ONU. *Declaração Universal dos Direitos Humanos*. Assembléia Geral das Nações Unidas, em 10 de dezembro de 1948

41 PINHEIRO, Patrícia Peck. *O mundo corporativo depois da Sarbanes-Oxley – Regulamentações em TI.* Seminário Ícaro. 2005a. Disponível em <http://www.patriciapeck.com.br/banco_arquivos/pagina_unica/%7BD9537F4F-466C-431E-A739-65C62E1A55F2%7D_icaropalestrapatriciapecksarbanesreduzido1.pdf>, Acessado em 19.07.08.

42 PINHEIRO, Patrícia Peck. *Arcabouço Jurídico e Segurança da Informação.ppt*. 2005b. Disponível em <http://www.pppadvogados.com.br/Publicações. Acessado em 29.06.09.

43 _____. *Direito Digital*. 2ª ed. rev., atual. e ampl. São Paulo: Saraiva, 2008.

44 PUCMINAS - PONTÍFICA UNIVERSIDADE CATÓLICA DE MINAS GERAIS. Pró-Reitoria de Graduação. Sistema de bibliotecas. *Padrão PUC Minas de normalização*: normas da ABNT para apresentação de trabalhos científicos, teses, dissertações e monografias. Belo Horizonte, 2006. Disponível em <http://www.pucminas.br/biblioteca/>

45 *PPP – Patrícia Peck Pinheiros Advogados*: <http://www.pppadvogados.com.br/paginas_unicas.asp?PaginaUnicaTipoID=17&intePaginaUnicaID=43>. Acessado em 17.10.07.

46 PRODEMGE. *Política de Segurança da Autoridade Certificadora Prodemge*. Disponível em: <http://icp-brasil.certisign.com.br/repositorio/ps/AC_PRODEMGE/PS_AC_PRODEMGE_v2.0.pdf>. Acessado em 11.10.07.

47 RAMOS, Anderson (org.). *Security Officer – 1: Guia Oficial para formação de gestores em segurança da informação*. Porto Alegre, RS: Zouk, 2006.

48 RIBEIRO, Milton Nassau. *Governança e Legalidade. Para fins legais, o que é governança corporativa*> APIMECMG. Julho/2007. Disponível em: <http://www.apimecmg.com.br/artigos/609_Microsoft%20Word%20-%20Governanca%20e%20Legalidade%20_Julho%202007_.pdf>. Acessado em 29.06.08.

49 RORAIMA. *Lei complementar nº 083, de 17 de dezembro de 2004*. Define as infrações e penalidades a serem aplicadas no caso de descumprimento das normas referentes à segurança contra incêndio e pânico no âmbito do Estado de Roraima e dá outras providências, disponível em: <http://www.al.rr.gov.br/publico/setores/000/2/download/Leis%20Complementares/Lei%20Complementar%20n%C2%BA%20083%20de%2017.12.04.pdf>.

50 RUAS, Maria das Graças. Desafios da administração pública brasileira: governança, autonomia, neutralidade. *Revista do Serviço Público*. Ano 48, número 03 – Set.-Dez./1997. Disponível em: <http://www.bresserpereira.org.br/Documents/MARE/Terceiros-Papers/97-Rua,MdasGra%C3%A7as48(3).pdf>. Acessado em 29.06.08.

51 SATHLER, Luciano. Cúpula Mundial sobre a sociedade da informação: desafios para a sociedade civil. *Mídia Cidadã*, nov. 2005. Disponível em: <http://www2.metodista.br/unesco/agora/pmc_forum_eixos_luciano.pdf> Acessado em 11.10.07.

52 SCHIRM, Helena. *Apresentação de trabalhos acadêmicos*. Fundação João Pinheiro. Belo Horizonte, 2003.

53 SÊMOLA, Marcos. *Gestão da Segurança da Informação*. Rio de Janeiro: Campus, 2003.

54 TAKAHASHI, Tadao (org.). *Sociedade da Informação no Brasil: livro verde*. Brasília: Ministério da Ciência e Tecnologia, 2000.

55 VALDÉS, Daisy de Asper Y. *Ética e Governança: ouvidoria para a cidadania*. 2006: Brasilia, DF.