Política de Segurança

1.INTRODUÇÃO

Conforme definição da norma ABNT NBR ISO/IEC 27002:2005, "*A **informação** é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, conseqüentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.*"

De acordo com a mesma norma, "***Segurança da informação** é a 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.*"

Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:

a)Integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações;

b)Confidencialidade: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação;

c)Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Ainda de acordo com a norma ABNT NBR ISO/IEC 27002:2005, *"A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio."*

Mediante tal embasamento e considerando o disposto em seu Planejamento Estratégico, a IMA resolve implantar um Sistema de Gestão de Segurança da Informação (S.G.S.I.), cuja estrutura e diretrizes são expressas neste documento.

2.TERMOS E DEFINIÇÕES

Para os efeitos desta Política, aplicam-se os seguintes termos e definições:

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. [ISO/IEC 13335-1:2004]

Áreas críticas: dependências da IMA ou de seus clientes onde esteja situado um ativo de informação relacionado a informações críticas para os negócios da empresa ou de seus clientes.

Ativo: qualquer coisa que tenha valor para a organização. [ISO/IEC 13335-1:2004]

Ativo de Informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. [ABNT NBR ISO/IEC 27002:2005]

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004]

Gestão de riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. [ABNT ISO/IEC Guia 73:2005]

IEC: International Electrotechnical Commission.

Incidente de segurança da informação: indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [ISO/IEC TR 18044:2004]

Informação: agrupamento de dados que contenham algum significado.

Informações críticas para os negócios da IMA: toda informação que, se for alvo de acesso, modificação, destruição ou divulgação não autorizada, resultará em perdas operacionais ou financeiras à IMA ou seus clientes. Cita-se, como exemplo, uma informação que exponha ou indique diretrizes estratégicas, contribua potencialmente ao sucesso técnico e/ou financeiro de um produto ou serviço, refira-se a dados pessoais de clientes, fornecedores, empregados ou terceirizados ou que ofereça uma vantagem competitiva em relação à concorrência.

ISO: International Organization for Standardization.

Risco: combinação da probabilidade de um evento e de suas conseqüências. [ABNT ISO/IEC Guia 73:2005]

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. [ABNT NBR ISO/IEC 27002:2005]

3.OBJETIVO

O presente documento constitui uma declaração formal da IMA acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua custódia, devendo ser observado por todos os seus empregados, estagiários, aprendizes e prestadores de serviços.

Seu propósito é formalizar o direcionamento estratégico acerca da gestão de segurança da informação na Organização, estabelecendo as diretrizes a serem seguidas para implantação e manutenção de um S.G.S.I., guiando-se, principalmente, pelos conceitos e orientações das normas ABNT ISO/IEC da família 27000.

4.ESTRUTURA NORMATIVA

Os documentos que compõem a estrutura normativa são divididos em três categorias:

a) **Política** (nível estratégico): constituída do presente documento, define as regras de alto nível que representam os princípios básicos que a IMA decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados;

b) **Normas** (nível tático): especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes da política;

c) **Procedimentos** (nível operacional): instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades da IMA.

4.1DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

Os documentos integrantes da estrutura devem ser divulgados a todos os empregados, estagiários, aprendizes e prestadores de serviços da IMA quando de sua admissão, bem como, através dos meios oficiais de divulgação interna da empresa e, também, publicadas na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

4.2APROVAÇÃO E REVISÃO

Os documentos integrantes da estrutura normativa da Segurança da Informação da IMA deverão ser aprovados e revisados conforme critérios descritos abaixo:

a)Política

- Nível de aprovação: Diretoria Executiva
- Periodicidade da revisão: anual

b)Normas

- Nível de aprovação: Diretoria Executiva
- Periodicidade da revisão: semestral

c)Procedimentos

- Nível de aprovação: Diretoria responsável pela área envolvida.
- Periodicidade da revisão: semestral

Durante o primeiro ano de vigência de cada documento, considerado a partir da data de sua publicação, a periodicidade das revisões será igual à metade dos períodos acima definidos.

5.DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A seguir, são apresentadas as diretrizes da política de segurança da informação da IMA que constituem os principais pilares da gestão de segurança da informação da empresa, norteando a elaboração das normas e procedimentos.

5.1PROTEÇÃO DA INFORMAÇÃO

Define-se como necessária a proteção das informações da empresa ou sob sua custódia como fator primordial nas atividades profissionais de cada empregado, estagiário, aprendiz ou prestador de serviços da IMA, sendo que:

a)Os empregados devem assumir uma postura pró-ativa no que diz respeito à proteção das informações da IMA e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade da IMA;

b)As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;

c)Assuntos confidenciais não devem ser expostos publicamente;

d)Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;

e)Somente softwares homologados podem ser utilizados no ambiente computacional da IMA;

f)Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;

g)Todo usuário, para poder acessar dados das redes de computadores utilizadas pela IMA, deverá possuir um código de acesso atrelado à uma senha previamente cadastrados, sendo este pessoal e intransferível, ficando vedada a utilização de códigos de acesso genéricos ou comunitários;

h)Não é permitido o compartilhamento de pastas nos computadores de empregados da empresa. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;

i)Todos os dados considerados como imprescindíveis aos objetivos da IMA devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos à testes periódicos de recuperação;

j)O acesso à dependências da IMA ou à ambientes sob controle da IMA dispostos em dependências de seus clientes deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação ali armazenada ou manipulada, garantindo a rastreabilidade e a efetividade do acesso autorizado;

k)O acesso lógico à sistemas computacionais disponibilizados pela IMA deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação, garantindo a rastreabilidade e a efetividade do acesso autorizado;

l)São de propriedade da IMA todas as criações, códigos ou procedimentos desenvolvidos por qualquer empregado, estagiário, aprendiz ou prestador de serviço durante o curso de seu vínculo com a empresa.

5.2PRIVACIDADE DA INFORMAÇÃO SOB CUSTÓDIA DA IMA

Define-se como necessária a proteção da privacidade das informações que estão sob custódia da IMA, ou seja, aquelas que pertencem aos seus clientes e que são manipuladas ou armazenadas nos meios às quais a IMA detém total controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais da IMA e reafirmam o seu compromisso com a melhoria contínua desse processo:

a)As informações são coletadas de forma ética e legal, com o conhecimento do cliente, para propósitos específicos e devidamente informados;

b)As informações são recebidas pela IMA, tratadas e armazenadas de forma segura e íntegra, com métodos de criptografia ou certificação digital, quando aplicável;

c)As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;

d)As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados;

e)As informações somente são fornecidas a terceiros, mediante autorização prévia do cliente ou para o atendimento de exigência legal ou regulamentar;

f)As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

5.3CLASSIFICAÇÃO DA INFORMAÇÃO

Define-se como necessária a classificação de toda a informação de propriedade da IMA ou sob sua custódia, de maneira proporcional ao seu valor para a empresa, para possibilitar o controle adequado da mesma, devendo ser utilizados os seguintes níveis de classificação:

a)Confidencial: É uma informação crítica para os negócios da IMA ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à IMA ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

b)Pública: É uma informação da IMA ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

c)Interna: É uma informação da IMA que ela não tem interesse em divulgar, mas cujo acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da IMA.

6.PAPÉIS E RESPONSABILIDADES

6.1EMPREGADOS, ESTAGIÁRIOS, APRENDIZES E PRESTADORES DE SERVIÇOS

Cabe aos empregados, estagiários, aprendizes e prestadores de serviços da IMA cumprir com as seguintes obrigações:

a)Zelar continuamente pela proteção das informações da Organização ou de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada;

b)Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades estatutárias da Organização;

c)Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;

d)Garantir a continuidade do processamento das informações críticas para os negócios da IMA;

e)Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;

f)Atender às leis que regulamentam as atividades da Organização e seu mercado de atuação;

g)Selecionar de maneira coerente os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;

h)Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

6.2COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (C.G.S.I.)

O Comitê Gestor de Segurança da Informação (C.G.S.I.) é um grupo multidisciplinar que reúne representantes de diversas áreas da empresa, indicados pelas suas respectivas Gerências e com composição aprovada pela Diretoria, com o intuito de definir e apoiar estratégias necessárias à implantação e manutenção do S.G.S.I.

Compete ao C.G.S.I.:

a)Propôr ajustes, aprimoramentos e modificações na estrutura normativa do S.G.S.I., submetendo à aprovação da Diretoria;

b)Redigir o texto das normas e procedimentos de segurança da informação, submetendo à aprovação da Diretoria;

c)Requisitar informações das demais áreas da IMA, através das diretorias, gerências e supervisões, com o intuito de verificar o cumprimento da política, das normas e procedimentos de segurança da informação;

d)Receber, documentar e analisar casos de violação da política e das normas normas e procedimentos de segurança da informação;

e)Estabelecer mecanismos de registro e controle de eventos e incidentes de segurança da informação, bem como, de não conformidades com a política, as normas ou os procedimentos de segurança da informação;

f)Notificar as gerências e diretorias quanto a casos de violação da política e das normas e procedimentos de segurança da informação;

g)Receber sugestões dos gestores da informação para implantação de normas e procedimentos de segurança da informação;

h)Propôr projetos e iniciativas relacionadas à melhoria da segurança da informação;

i)Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação;

j)Propôr a relação de gestores da informação;

k)Realizar, sistematicamente, a gestão dos ativos da informação;

l)Gerir a continuidade dos negócios, demandando junto às diversas áreas da empresa, planos de continuidade dos negócios, validando-os periodicamente;
m)Realizar, sistematicamente, a gestão de riscos relacionados a segurança da informação.

6.3GESTOR DA INFORMAÇÃO

O Gestor da Informação é um empregado da IMA sugerido pelo Comitê Gestor de Segurança da Informação (C.G.S.I.) e designado pela Diretoria como responsável por um determinado ativo de informação.

Este gestor deve dominar todas as regras de negócio necessárias à criação, manutenção e atualização de medidas de segurança relacionadas ao ativo de informação sob sua responsabilidade, seja este de propriedade da IMA ou de um cliente.

O Gestor da Informação pode delegar sua autoridade sobre o ativo de informação, porém, continua sendo dele a responsabilidade final pela sua proteção.

Compete ao Gestor da Informação:

a)Classificar a informação sob sua responsabilidade, inclusive aquela gerada por clientes, fornecedores ou outras entidades externas, que devem participar do processo de definição do nível de sigilo da informação;

b)Inventariar todos os ativos de informação sob sua responsabilidade;

c)Enviar ao C.G.S.I., quando solicitado, relatórios sobre as informações e ativos de informação sob sua responsabilidade. Os modelos de relatórios serão definidos pelo C.G.S.I. e aprovados pela Diretoria;

d)Sugerir procedimentos ao C.G.S.I. para proteger os ativos de informação, conforme a classificação realizada, além da estabelecida pela Política de Segurança da Informação e pelas Normas de Segurança da Informação;

e)Manter um controle efetivo do acesso à informação, estabelecendo, documentando e fiscalizando a política de acesso à mesma. Tal política deve definir quais usuários ou grupos de usuários têm real necessidade de acesso à informação, identificando os perfis de acesso;

f)Reavaliar, periodicamente, as autorizações dos usuários que acessam as informações sob sua responsabilidade, solicitando o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;

g)Participar da investigação dos incidentes de segurança relacionados às informações sob sua responsabilidade.

6.4 GERÊNCIAS

Cabe às Gerências:

a)Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;

b)Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;

c)Sugerir ao C.G.S.I., de maneira pró-ativa, procedimentos de segurança da informação relacionados às suas áreas;

d)Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação relacionados às suas áreas, quando solicitado pelo C.G.S.I.;

e)Comunicar imediatamente ao C.G.S.I. eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

6.4.1GERÊNCIA JURÍDICA

Cabe, adicionalmente, à Gerência Jurídica:

a)Manter as áreas da IMA informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;

b)Incluir na análise e elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da IMA;

c)Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

6.4.2GERÊNCIA DE RECURSOS HUMANOS

Cabe, adicionalmente, à Gerência de Recursos Humanos:

a)Assegurar-se de que os empregados, estagiários, aprendizes e prestadores de serviços comprovem, por escrito, estar cientes da estrutura normativa do S.G.S.I. e dos documentos que a compõem;

b)Criar mecanismos para informar, antecipadamente aos fatos, ao canal de atendimento técnico mais adequado, alterações no quadro funcional da IMA.

6.5 ÁREA DE SEGURANÇA DA INFORMAÇÃO

Cabe à área de Segurança da Informação:

a)Consolidar e coordenar a elaboração, acompanhamento e avaliação do S.G.S.I.;

b)Convocar, coordenar e prover apoio às reuniões do C.G.S.I.;

c)Prover as informações de gestão de segurança da informação solicitadas pelo C.G.S.I.;

d)Facilitar a conscientização, a divulgação e o treinamento quanto à política, às normas e os procedimentos de segurança da informação;

e)Executar projetos e iniciativas visando otimizar a segurança da informação na IMA.

6.6 DIRETORIA EXECUTIVA

Cabe à Diretoria Executiva:

a)Aprovar a política e as normas de segurança da informação e suas revisões;

b)Aprovar a composição do C.G.S.I.;

c)Nomear os gestores da informação, conforme as indicações do C.G.S.I.;

d)Receber, por intermédio do C.G.S.I., relatórios de violações da política e das normas de segurança da informação, quando aplicável;

e)Tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação, mediante a apresentação de propostas do C.G.S.I.

7.AUDITORIA

Todo ativo de informação sob responsabilidade da IMA é passível de auditoria em data e horários determinados pelo C.G.S.I., podendo esta, também, ocorrer sem aviso prévio.

A realização de uma auditoria deverá ser, obrigatoriamente, aprovada pela Diretoria e, durante a sua execução, deverão ser resguardados os direitos quanto a privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade da IMA ou de seus clientes de forma que se misture ou impeça o acesso à informações de propriedade ou sob responsabilidade da IMA.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações da política, das normas ou dos procedimentos de segurança da informação, a área de Segurança da Informação poderá realizar monitoramento e controle pró-ativos, mantendo a confidencialidade do processo e das informações obtidas.

Em ambos os casos, as informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

8. VIOLAÇÕES E SANÇÕES

8.1 VIOLAÇÕES

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

a)Quaisquer ações ou situações que possam expôr a IMA ou seus clientes à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

b)Utilização indevida de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do Gestor da Informação;

c)Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da IMA ou de seus clientes;

d)A não comunicação imediata à área de Segurança da Informação de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um empregado, estagiário, aprendiz ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar.

8.2 SANÇÕES

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à política de segurança da informação da IMA são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

9.LEGISLAÇÃO APLICÁVEL

Correlacionam-se com a política, com as diretrizes e com as normas de Segurança da Informação as Leis abaixo relacionadas, mas não se limitando às mesmas:

a)Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);

b)Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);

c)Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);

d)Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);

e)Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);

f)Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);

g)Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias).

Serviços

Webmail (http://webmail.ima.sp.gov.br)

Diário Oficial (http://www.campinas.sp.gov.br/diario-oficial/)

Transparência (/transparencia)

Concursos (/concursos)

Licitações (http://licita.ima.sp.gov.br/)

Intranet (http://intraima.ima.sp.gov.br/)

Política de Segurança (/politica-de-seguranca-da-informacao)

Localização

Rua Bernardo de Sousa Campos, 42 - Praça Dom Barreto - Ponte Preta

Campinas - SP - CEP 13041-390

Fone: (19) 3755-6500

Soluções em

GED (/solucoes/ged) | Planejamento e Urbanismo (/solucoes/planejamento-e-urbanismo)

e-DOM - Diário Oficial do Município (/solucoes/e-dom-diario-oficial-do-municipio)

Atendimento (/solucoes/atendimento) Consultoria (/solucoes/consultoria)

Educação (/solucoes/educacao) Saúde (/solucoes/saude)