INFORMÁTICA DE MUNICÍPIOS ASSOCIADOS
Rua Bernardo de Sousa Campos, nº 42 - Bairro Ponte Preta - CEP 13041-390 - Campinas - SP

Inf. Mun. Assoc./IMA-DP/IMA-DP-DGCC

NORMA ADMINISTRATIVA

Campinas, 05 de dezembro de 2018.

NORMA ADMINISTRATIVA – 027

Assunto: ***POLÍTICA DE SEGURANÇA DA INFORMAÇÃO***

Emissão: 05/12/2018

Vigência: na data de sua publicação

I. INTRODUÇÃO

A Informática de Municípios Associados S/A – IMA é uma sociedade de economista mista, que tem como missão oferecer soluções tecnológicas inovadoras, impactando de forma estratégica nas organizações e na sociedade.

Conforme definição da norma ABNT NBR ISO/IEC 27002:2005 “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. ”

“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. ” Norma ABNT NBR ISO/IEC 27002:2005.

A IMA reconhece que a informação é um ativo essencial à administração pública e à sociedade, assim, com esta norma administrativa, atualiza a sua Política, estabelece a estrutura e diretrizes de Segurança da Informação e reafirma o compromisso de garantir a sua proteção.

II. OBJETIVO

O presente documento atualiza a formalização do compromisso da IMA e de todos os seus colaboradores com a proteção das informações de sua propriedade ou sob sua custódia e estabelece as diretrizes para implantação e manutenção do Sistema Gestão de Segurança da

Informação – SGSI, guiando-se, principalmente, pelos conceitos e orientações das normas ABNT ISO/IEC da família 27000. Assim, para cumprir sua missão, a Segurança da Informação tem tratamento prioritário na IMA e faz parte do dia-a-dia de todos os seus colaboradores.

III. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

1. **Integridade:** somente as alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações;
2. **Confidencialidade:** somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação;
3. **Disponibilidade:** a informação deve estar disponível às pessoas autorizadas sempre que necessário ou demandado;
4. **Autenticidade:** Garantir a não adulteração da informação;
5. **Irrefutabilidade:** Também chamada de “Não Repúdio” visa garantir a identificação/responsabilidade do autor em cada ação de maneira que o mesmo seja responsável por suas ações.

IV. 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 estão situados ativos de informação considerados críticos 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.

Colaboradores: Diretores, Gestores, empregados, estagiários, aprendizes e prestadores de serviço da empresa.

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: toda informação que, se for alvo de acesso, modificação, destruição ou divulgação não autorizada, resultará em perdas operacionais ou financeiras à IMA ou a 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.

PSI: Política de Segurança da Informação

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

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 (ABNT NBR ISO/IEC 27002:2005);

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

SGSI - Sistema de Gestão de Segurança da Informação: É um conjunto de regras, normas e procedimentos cuja prática visa garantir a manutenção e a melhoria da segurança da informação conforme a norma ISO 27001. SGSI não é um software ou aplicativo de segurança.

CGSI - Comitê Gestor de Segurança da Informação: Grupo de pessoas constituída pela empresa que são responsáveis por aplicar os preceitos do SGSI.

V. ESTRUTURA NORMATIVA

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

1. **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;
2. **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;
3. **Procedimentos/Processos (nível operacional):** instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades da IMA.

b. Divulgação e Acesso à Estrutura Normativa

Os documentos integrantes da estrutura devem ser divulgados a todos os

empregados, estagiários e aprendizes da IMA quando de sua admissão e aos prestadores de serviços antes do início das suas atividades, bem como, pelos meios oficiais de divulgação interna da empresa e, incluindo-se publicação na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

A aceitação à **PSI** deve ser manifestada por assinatura via sistema eletrônico de informações. As atualizações devem ser comunicadas pelo e-mail oficial da empresa, não sendo necessária nova assinatura.

c. Aprovação e revisão

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

1. **Política**

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

2. **Normas**

   - Nível de aprovação: Diretoria Executiva
   - Periodicidade mínima de revisão: Anual

3. **Procedimentos**

   - Nível de aprovação: Diretoria responsável pela área envolvida.
   - Periodicidade mínima de revisão: Anual

Nota: 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.

VI. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

As diretrizes da política de segurança da informação constituem os principais pilares da gestão de segurança da informação da IMA, norteando a elaboração das normas e procedimentos.

a. Proteção da Informação

Define-se 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:

1. Os empregados devem assumir uma postura proativa e ficarem atentos a todos os procedimentos que visam proteger acessos e informações contra ameaças externas, fraudes, roubo de informações e acesso indevido a sistemas de informação sob responsabilidade da IMA;
2. As informações não podem ser transportadas em qualquer meio físico, sem as

devidas proteções;
3. Assuntos confidenciais não devem ser expostos publicamente;
4. Credenciais de acesso (Senhas, chaves, etc.) não podem ser compartilhadas ou divulgadas e a responsabilidade pelo uso das mesmas é intransferível;
5. Somente softwares homologados podem ser utilizados no ambiente computacional da IMA;
6. Nas estações Windows somente a área de suporte técnico ao usuário poderá realizar a instalação de softwares;
7. Mudança de sistema operacional somente poderá ser realizada de acordo com os padrões técnicos e autorização do gestor da área;
8. Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;
9. Todo usuário para acessar um recurso computacional, deve ter credencial de acesso própria; não deve realizar nenhuma ação anônima, inclusive navegação anônima ou acesso anônimo a rede;
10. Toda credencial de acesso pertence a apenas um único usuário, assim, jamais se deve criar e/ou utilizar credenciais (senhas ou outros meios) genéricos ou para uso compartilhado;
11. Apenas informações pertinentes ao trabalho devem existir no ambiente computacional da empresa. O armazenamento deve ser nos servidores e, em caso de necessidade de compartilhamento, devem ser configurados nos servidores apropriados, atentando-se às permissões de acesso aplicáveis aos referidos dados;
12. Todos os dados da empresa e de seus clientes devem ser armazenados em servidores da IMA, onde são protegidos por diversos controles de segurança e pelas melhores práticas de administração de dados;
13. O acesso lógico a sistemas computacionais disponibilizados pela IMA e o acesso físico às suas dependências ou à ambientes sob controle da IMA, devem ocorrer somente com a aplicação dos princípios da segurança da informação, garantindo-se também a rastreabilidade e a efetividade do acesso autorizado;
14. São de propriedade da IMA e/ou de seus clientes, todas as criações desenvolvidas por qualquer colaborador no exercício de suas funções durante o seu vínculo com a empresa.

b. Proteção da Informação sob custódia da IMA

Define-se como prioritária a proteção das informações sob custódia da IMA, ou seja, 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.

Para isso, as informações devem ser:

1. Coletadas de forma ética e legal, com o conhecimento do cliente, para propósitos específicos e devidamente informados;
2. Recebidas pela IMA, tratadas e armazenadas de forma segura e íntegra, com métodos de criptografia ou certificação digital, quando aplicável;
3. Acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
4. As informações somente podem ser disponibilizadas para atendimento às exigências legais ou às empresas contratadas, mediante a formalização do compromisso com a política e diretrizes de segurança da informação da IMA e

com a autorização prévia do cliente;
5. As informações e dados constantes em nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais são fornecidos somente aos próprios interessados e mediante solicitação formal, seguindo os requisitos legais vigentes.

c. Tratamento de dados

Manter atualizadas as normas e procedimentos necessários para tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural, de acordo com o estabelecido na Lei 13.709 de 14 de agosto de 2018.

A disciplina da proteção de dados pessoais tem como fundamentos:

a. o respeito à privacidade;
b. a autodeterminação informativa;
c. a liberdade de expressão, de informação, de comunicação e de opinião;
d. a inviolabilidade da intimidade, da honra e da imagem;
e. o desenvolvimento econômico e tecnológico e a inovação;
f. a livre iniciativa, a livre concorrência e a defesa do consumidor; e
g. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

d. Classificação da Informação

Define-se como necessário classificar toda informação de propriedade da IMA ou sob sua custódia, de acordo com o seu valor à empresa, possibilitando o controle adequado da mesma, utilizando-se para isso os seguintes níveis de classificação:

1. **Confidencial**: 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 ou criminais à IMA ou a seus clientes. É restrita a um grupo específico de pessoas, podendo ser composto por empregados, clientes e/ou fornecedores.
2. **Pública:** Informação da IMA ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo de caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre para cumprimento de legislação que exija publicidade da mesma.
3. **Interna:** Informação da IMA em que não há interesse em divulgar ao público externo, à empresa, o que deve ser evitado. Caso seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com o mesmo impacto de uma informação confidencial. Portanto, pode ser acessada sem restrições, somente, pelos empregados, estagiários, aprendizes e prestadores de serviços da IMA.

Assim, os documentos da empresa devem ser datados e classificados, no rodapé da primeira página, de acordo com a sua natureza: Confidencial, Público ou Interno. Caso o documento tenha mais de um tipo de classificação (e.g.: Confidencial e Público), ele deverá ter o tratamento da classificação mais restritiva.

VII. PAPÉIS E RESPONSABILIDADES

a) Compete à Diretoria Executiva

1. Aprovar a política e as normas de segurança da informação e suas revisões;
2. Aprovar a composição do C.G.S.I. – Comitê Gestor da Segurança da Informação e dos Pontos Focais;
3. 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.

b) Comitê Gestor de Segurança da Informação – CGSI

O Comitê Gestor de Segurança da Informação é um grupo multidisciplinar que reúne representantes da área de segurança da informação e 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 Sistema de Gestão da Segurança da Informação – SGSI.

Compete ao CGSI:

1. Consolidar e coordenar a elaboração, acompanhamento e avaliação do SGSI;
2. Propor ajustes, aprimoramentos e modificações na estrutura normativa do SGSI, submetendo à aprovação da Diretoria;
3. Executar projetos e iniciativas visando otimizar a segurança da informação na IMA;
4. Facilitar a divulgação e o treinamento quanto à política, às normas e os procedimentos de segurança da informação, com o objetivo de conscientização;
5. Requisitar informações das demais áreas, com o intuito de verificar o cumprimento da política, das normas e procedimentos de segurança da informação;
6. Receber e analisar casos de violação da política, normas ou procedimentos de segurança da informação;
7. Estabelecer mecanismos de registro e controle de eventos e incidentes de segurança da informação, bem como, de não conformidades com a política, normas ou procedimentos de segurança da informação;
8. Aprovar os modelos dos relatórios de informações e de ativos de informação;
9. Notificar as gerências e diretorias se houver casos de violação da política, das normas ou dos procedimentos de segurança da informação- SI;
10. Receber sugestões dos gestores da informação para implantação de normas e procedimentos de SI;
11. Propor projetos e iniciativas relacionadas à melhoria da SI;
12. Acompanhar o andamento dos projetos e iniciativas relacionados à SI;
13. Definir com os gestores, a relação de Pontos focais de SI em todas as áreas da empresa;
14. Realizar, sistematicamente, a gestão dos ativos da informação;
15. Gerir a continuidade dos negócios, demandando junto às diversas áreas da empresa, planos de continuidade dos negócios, validando-os periodicamente;
16. Realizar, sistematicamente, a gestão de riscos relacionados à segurança da informação.

c) Compete à Área de Segurança da Informação

1. Participar da coordenação técnica do SGSI;
2. Acompanhar e avaliar o SGSI;
3. Participar a apoiar tecnicamente as reuniões do CGSI;
4. Prover as informações de gestão de segurança da informação solicitadas pelo CGSI;
5. Acompanhar as eventuais alterações na legislação, normas e regulamentos envolvendo segurança da informação e apresentar ao Comitê Gestor de Segurança da Informação.

d) Compete a área de Governança e Compliance.

1. Participar das reuniões do Comitê de Segurança da Informação;
2. Elaborar, revisar, atualizar e divulgar normas, políticas e procedimentos referentes à segurança da informação;
3. Auditar, em conjunto com o Comitê de Segurança, os sistemas de gestão de segurança da informação;
4. Auxiliar as áreas da empresa na interpretação e aplicação da legislação, normas e regulamentos que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;
5. Divulgar as deliberações do Comitê Gestor de Segurança da Informação.

e) Compete às Gerências

1. Cumprir e fazer cumprir a política, normas e procedimentos de segurança da informação;
2. Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;
3. Sugerir ao C.G.S.I., de maneira proativa, procedimentos de segurança da informação relacionados às suas áreas;
4. 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.;
5. Comunicar imediatamente ao C.G.S.I. eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

Da Gerência Jurídica:

1. Orientar as áreas da empresa na interpretação e aplicação da legislação, normas e regulamentos;
2. Incluir na análise e elaboração de contratos, sempre que necessárias, cláusulas específicas relacionadas à segurança da informação com o objetivo de proteger os interesses da IMA;
3. Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

Da Gerência de Recursos Humanos

1. Assegurar e comprovar que, nos treinamentos de integração de pessoal, seja dada ampla ciência aos colaboradores da estrutura normativa do S.G.S.I. e dos documentos que a compõem;
2. Informar as alterações do quadro de pessoal da IMA às seguintes equipes: central de serviços, gerência administrativa, gerência de comunicação, gerência financeira, recepção e segurança patrimonial.

f) Ponto Focal de SI

Nas diversas áreas da empresa, conforme a quantidade e criticidade de ativos de informação, um empregado da IMA será indicado pelo gestor para tratar dos assuntos de segurança da informação, o qual será considerado o Ponto Focal de Segurança da Informação da área.

O ponto focal precisa dominar as regras de negócio necessárias à criação, manutenção e atualização de medidas de segurança relacionadas aos ativos de informação sob a responsabilidade da área, seja de propriedade da IMA ou de clientes.

Em cada área da empresa será definido um funcionário como Ponto Focal de SI e um responsável para cada ativo de informação. Essas definições deverão ser formalizadas pelo gestor ao CGSI.

Compete ao Ponto focal de SI e ao Responsável pelo ativo de Informação:

1. Classificar a informação sob responsabilidade da área, inclusive aquela gerada por clientes, fornecedores ou outras entidades externas, que devem participar do processo de definição do nível de sigilo da informação;
2. Inventariar todos os ativos de informação sob sua responsabilidade;
3. Enviar ao C.G.S.I., quando solicitado, relatórios sobre as informações e ativos de informação sob sua responsabilidade.
4. Sugerir ao C.G.S.I. procedimentos para proteger os ativos de informação, após classificá-los, de acordo com esta Política e Normas de Segurança da Informação;
5. Manter um controle efetivo do acesso à informação, estabelecendo, documentando e fiscalizando a política de acesso à mesma. Referido controle deve especificar quais usuários ou grupos de usuários têm real necessidade de acesso à informação, identificando os perfis de acesso;
6. 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;
7. Participar da investigação de incidentes de segurança relacionados às informações sob sua responsabilidade.

g) Competem ao presidente, diretores, gestores, empregados, estagiários, aprendizes e prestadores de serviços:

1. Zelar continuamente pela proteção das informações da organização ou de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada;
2. Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades estatutárias da Organização;
3. Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
4. Garantir a continuidade do processamento das informações críticas para os negócios da IMA;
5. Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
6. Atender às leis que regulamentam as atividades da Organização e seu mercado de atuação;
7. Selecionar de maneira coerente os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
8. Comunicar imediatamente à área de Segurança da Informação qualquer

descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

VIII. AUDITORIA

Todo ativo de informação, sob responsabilidade da IMA, é passível de auditoria em data e horário predeterminados pelo C.G.S.I., podendo, também, ocorrer sem comunicação prévia, de acordo com a necessidade da equipe de Segurança da Informação.

A realização de auditoria, por área competente, não exige autorização prévia, e, durante a sua execução, devem ser resguardados os direitos quanto à privacidade de informações pessoais, desde que não estejam dispostas em ambiente físico ou lógico de propriedade da IMA ou de seus clientes.

Com o objetivo de detectar atividades anômalas de processamento da informação ou de violações da política, das normas ou dos procedimentos de segurança da informação, a área de Segurança da Informação realizará monitoramento e controles proativos.

Nos dois casos, as informações obtidas poderão servir como prova, indício ou evidência em processo administrativo e/ou judicial.

IX. VIOLAÇÕES E SANÇÕES

a) Violações

São consideradas violações à segurança da informação as seguintes situações, não se limitando às mesmas:

1. Qualquer ação ou situação que possa expor a IMA ou seus clientes à perda financeira ou de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
2. Utilização indevida de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do Gestor da Informação;
3. Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que violam leis, regulamentos internos ou externos, a ética ou exigências de organismos reguladores da área de atuação da IMA ou de seus clientes;
4. A não comunicação imediata à área de Segurança da Informação de quaisquer descumprimentos da política, das 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.

b) Sanções

A violação ou a não aderência à política, às normas ou aos procedimentos de segurança da informação são consideradas faltas graves, passíveis de medidas educativas ou penalidades previstas em lei, conforme o caso.

X. DISPOSIÇÕES GERAIS

Esta Política de Segurança da Informação tem como base legal, mas não se limitando às mesmas:

- Lei Federal 8.159, de 08 de janeiro de 1991: Dispõe sobre a Política Nacional de Arquivos Públicos e Privados;
- Lei Federal 9.610, de 19 de fevereiro de 1998: Dispõe sobre Direito Autoral;
- Lei Federal 9.279, de 14 de maio de 1996: Dispõe sobre Marcas e Patentes;
- Lei Federal 3.129, de 14 de outubro de 1982: Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial;
- Lei Federal 10.406, de 10 de janeiro de 2002: Institui o Código Civil;
- Decreto-Lei 2.848, de 7 de dezembro de 1940: Institui o Código Penal;
- Lei Federal 9.983, de 14 de julho de 2000: Altera oCódigo Penal e dá outras providencias.
- Lei Federal 13.303, de 30 de junho de 2016: Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.
- Lei 13.709 de 14 de agosto de 2018: Dispõe sobre o tratamento de dados pessoais

XI. DISPOSIÇÕES FINAIS

1. Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação;
2. Com o objetivo de controle e organização, as normas de segurança da informação necessárias ou complementares, serão editadas e publicadas como documentos anexos a esta política;
3. Revogam-se as disposições em contrário, em especial a RD 090/2011.

Fernando Eduardo Monteiro de Carvalho Garnero

Diretor Presidente

Mario Armando Gomide Guerreiro

Diretor Administrativo-Financeiro

Leandro Telles Salgueiro Barboni

Diretor Técnico

Márcio Fernando Correa Ricardo

Diretor de Governança Corporativa e Compliance

Elaboração:

Gerência de Sustentação.

Governança Corporativa e Compliance.

Unidade de Hospedagem de Dados e Segurança da Informação

Classificação: Público

Documento assinado eletronicamente por **MARCIO FERNANDO CORREA RICARDO**, **Diretor(a) de Governança Corporativa e Compliance**, em 11/12/2018, às 10:01, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

Documento assinado eletronicamente por **LUANA MOISES FERREIRA MACIEL**, **Gerente Jurídico**, em 04/01/2019, às 14:50, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

Documento assinado eletronicamente por **LEANDRO TELLES SALGUEIRO BARBONI**, **Diretor(a) Técnico**, em 07/01/2019, às 09:57, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

A autenticidade do documento pode ser conferida no site https://sei.campinas.sp.gov.br/verifica informando o código verificador **1105928** e o código CRC **33AB5909**.

IMA.2017.00001318-18 1105928v4

INFORMÁTICA DE MUNICÍPIOS ASSOCIADOS
Rua Bernardo de Sousa Campos, nº 42 - Bairro Ponte Preta - CEP 13041-390 - Campinas - SP

Inf. Mun. Assoc./IMA-DP/IMA-DP-DGCC

NORMA ADMINISTRATIVA

Campinas, 05 de dezembro de 2018.

NORMA ADMINISTRATIVA – 027

Assunto: ***POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - ANEXO I***

Emissão: 05/12/2018

Vigência: na data de sua publicação

ANEXO 1

ACESSO AOS BANCOS DE DADOS DE PRODUÇÃO

1. INTRODUÇÃO

Atualizar bancos de dados é tarefa crítica; muito mais relevante que atualizar a aplicação, principalmente quando a base possui uma grande quantidade de dados. Testes em bancos de dados são mais difíceis e demorados para implementar, pois, geralmente requerem um banco de dados de teste semelhante ao de produção. Da mesma forma, é muito mais difícil reverter as alterações feitas de forma equivocada em um banco de dados do que nas aplicações. Às vezes, é até impossível. É muito desagradável informar ao cliente que alguns dados foram alterados acidentalmente e não é possível mais recuperá-los. Dados em ambiente de produção sempre são críticos, assim, trabalhar com segurança é o primeiro passo para evitar essa situação.

2. OBJETIVO

Este documento apresenta regras e comportamentos necessários para reduzir o risco de danos aos dados críticos durante atividades com um banco de dados de produção. Apresenta também as responsabilidades dos gestores, profissionais, técnicos e analistas em tecnologia da informação da IMA, quanto ao acesso, intervenção e proteção aos bancos de dados.

3. PAPÉIS E RESPONSABILIDADES

3.1. Diretor Técnico, Gerente de Sustentação, Gerente de Soluções, Coordenadores e Supervisores de Manutenção e Evolução de Sistemas, de Arquitetura e de Desenvolvimento de Sistemas e de Hospedagem (Data Center):

a) Estabelecer, cumprir e fazer cumprir as normas e responsabilidades no acesso às informações dos bancos de dados e sistemas em ambiente de produção, bem como os procedimentos, melhores práticas e processos associados ao acesso dos bancos de dados de produção;

b) Assegurar que suas equipes possuam acesso e entendimento desta norma;

c) Comunicar imediatamente à chefia imediata e/ou ao Comitê Gestor de Segurança da Informação - CGSI, eventuais casos de violação desta norma;

d) Indicar e registrar quais funcionários, Analistas e Técnicos, devem possuir acesso aos bancos de dados de produção, quais os privilégios do acesso (leitura, gravação, etc.), prazo de validade do acesso e objetivos que justificam a concessão;

3.2. Exclusivamente aos **Analistas de Tecnologia da Informação na função de DBA**:

a) Verificar se a solicitação de execução de *script* em produção está devidamente autorizada pelo gestor imediato e/ou, se o solicitante tem permissão para efetuar acesso ou intervenção no banco de dados de produção;

b) Registrar todo e qualquer acesso que efetuar às bases de dados de produção, independente do objetivo, com as seguintes informações: (i) data e hora do acesso; (ii) duração do acesso; (iii) ação executada ou intervenção realizada; (iv) nome e matrícula do solicitante; (v) número da ordem de serviço ou chamado;

c) Conceder acesso aos bancos de dados somente aos analistas e técnicos de TI autorizados por suas chefias;

d) Verificar se o *script* encaminhado está de acordo com as boas práticas e, caso não esteja, analisar a criticidade e alertar o Analista ou o Técnico solicitante responsável pelo *script*;

e) Monitorar eventuais impactos na performance da aplicação (ou do ambiente servidor) decorrente da execução dos *scripts* de banco de dados e tomar ações para mitigação, em conjunto com o analista / técnico responsável pelo sistema;

f) Analisar a performance dos *scripts* contendo *queries* de bancos de dados, avaliando-as em relação à sua estrutura, tempo de execução e recursos que precisam ser implementados para melhorar o desempenho, tais como criação de *views*, índices, etc.

g) Avaliar o impacto da execução de *scripts* que movimentem uma grande quantidade de registros ou demande uma alta utilização de recursos do ambiente servidor e, agendar janela de execução em horário que represente menor impacto aos sistemas, sempre em conjunto com o analista / técnico responsável pelo sistema;

h) Monitorar a disponibilidade e a performance dos bancos de dados de produção, avaliar as causas das falhas dos ambientes dos bancos de dados e promover ações para mitigar, recuperar o estado normal de operação, bem como analisar e identificar ações para contenção de falhas, acompanhamento do crescimento da base de dados em relação ao espaço disponível em ambiente operacional;

i) Efetuar a atualização e configuração dos ambientes tecnológicos dos sistemas de bancos de dados e dos SGBD (Sistemas Gerenciadores de Bancos de Dados);

j) Configurar rotinas de manutenção das bases de dados (coleta de estatísticas, *vacuumm*, reorganize).

k) Executar rotinas de *backup* e *restore* de *backup* dos bancos de dados.

3.3. **Analistas e Técnicos de Tecnologia de Informação**, inclusive **aos que atuam na função de DBA** e **Serviços de Sistemas Operacionais**:

a) Tomar conhecimento e cumprir as instruções desta norma;

b) Zelar pela integridade, confidencialidade e disponibilidade dos dados e informações contidas nos sistemas, devendo comunicar por escrito a sua chefia imediata quaisquer indícios de falhas identificadas, bem como, irregularidades que possam expor os sistemas à exploração de vulnerabilidades, mesmo que em bases e sistemas que não façam parte do seu escopo de trabalho;

c) Seguir os procedimentos e processos de trabalho que forem definidos, incluindo as melhores práticas que forem recomendadas, pela equipe de Arquitetura e pela equipe do Data Center [Hospedagem] da IMA, quanto ao envio de *scripts* para atualização dos dados em bancos de dados de produção. Em casos fortuitos ou não previstos, em que não for possível seguir o processo, antes de executar qualquer procedimento técnico que acesse ou modifique dados em qualquer banco de dados de produção, o funcionário deve reportar o motivo e obter autorização da sua chefia imediata, ambos por escrito em e-mail, com cópia para seus respectivos coordenadores e gerentes;

d) Responder pelas consequências de suas ações ou omissões, que possam colocar em risco ou comprometer o sigilo, a confidencialidade, a integridade e a disponibilidade dos dados e informações dos bancos de dados;

e) Prestar informações para auditoria interna ou externa, somente quando autorizado por sua chefia.

4. DEFINIÇÕES

Apresentamos as definições e orientações que devem ser seguidas por todos os profissionais:

4.1. BANCOS DE DADOS DE PRODUÇÃO

a) Os SGBDs - Sistemas Gerenciadores de Bancos de Dados (PostGreSQL, Oracle, MySQL, etc.) e as bases de dados são as estruturas que mantém os dados organizados e disponíveis às aplicações. Para fins de simplificação, chamaremos ambos de Bancos de Dados;

b) Os bancos de dados de produção são aqueles que mantêm o funcionamento dos sistemas que são usados pelos clientes e, portanto, armazenam os dados correntes das aplicações usadas pelos clientes;

c) O acesso aos bancos de dados de produção deve ser restrito e controlado. As intervenções nos bancos de dados devem ser executadas apenas por pessoas capacitadas e que estejam autorizadas.

4.2. ACESSO AOS BANCOS DE DADOS

a) Apenas profissionais autorizados podem ter acesso aos bancos de dados. Esse acesso deve ser concedido pela chefia, e deve se extinguir após o encerramento do projeto ou da atividade;

b) O acesso será concedido eletronicamente através da autenticação de usuário e senha, que são únicos e intransferíveis. Não serão fornecidas credenciais de acesso para grupo de usuários;

c) As senhas dos bancos de dados devem ser fortes, conter letras minúsculas e maiúsculas, números e caracteres especiais, para reduzir a probabilidade de serem descobertas;

d) Os profissionais devem receber as permissões mínimas necessárias para executar *scripts* nos bancos de dados e de acordo com sua função no projeto. Não serão concedidos, sob qualquer hipótese, acessos do tipo DBA ou ROOT aos funcionários, analistas ou técnicos, que não atuem na equipe de DBAs;

e) Credenciais de acesso (usuário e senha) para aplicações são consideradas especiais e poderão ser usadas somente pelas aplicações e não por pessoas;

f) Não deverão ser reveladas a outra pessoa senhas de acesso a sistemas e bancos de dados, independente do motivo ou situação;

g) As senhas deverão ser alteradas, sempre que obrigatório ou quando suspeitar que possa ter sido descoberta.

4.3. SIGILO E CONFIDENCIALIDADE DOS DADOS E INFORMAÇÕES

Possuir acesso a uma base de dados, mesmo que com privilégios apenas de leitura, implica em responsabilidade de sigilo e confidencialidade. Dessa forma, as seguintes instruções devem ser observadas e seguidas:

a) Ter cuidado quando da exibição de dados de banco de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que pessoas não autorizadas tenham acesso a dados e informações, totais ou parciais;

b) Não se ausentar da estação de trabalho sem bloquear ou encerrar a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por terceiros;

c) Não divulgar dados e informações obtidas dos bancos de dados e sistemas, mesmo que para pessoas envolvidas nas atividades de projetos que requeiram tais informações. Solicitações de dados e informações devem ser expressadas de maneira formal, via SEI, devidamente justificadas tecnicamente e chanceladas pelo superior imediato do requerente, sendo sua cessão somente possível após aceite, também via SEI, do gestor responsável pela base de dados;

d) Cópias de bancos de dados, totais ou parciais, que forem extraídas do servidor de banco de dados e copiadas para outros servidores, para o computador local ou mídias externas, deverão ser completamente apagadas após o término das atividades ou término do projeto. Para a realização de tais cópias, é necessária solicitação formal, com a justificativa técnica, via SEI, que deverá ser autorizada pelo superior imediato do requerente e também pelo gestor da base de dados em questão.

4.4. CUIDADOS À INTEGRIDADE, AUTENTICIDADE E DISPONIBILIDADE DOS DADOS E DOS SISTEMAS DE INFORMAÇÃO

a) Quando for necessária intervenção nos bancos de dados, os profissionais envolvidos devem manter a confidencialidade e o sigilo e, também, a integridade, a disponibilidade e a autenticidade dos dados e dos sistemas de informação que utilizam esses dados;

b) Manter a **integridade** significa garantir que a informação ou dado armazenado no banco de dados está correto e de acordo com as características originais geradas pelo dono da informação;

c) Manter a **disponibilidade** significa garantir que a informação ou dado possa ser obtido, sempre que necessário, pelos usuários e/ou sistemas autorizados pelo dono da informação;

d) Manter a **autenticidade** é garantir que a informação ou dado contido no banco de dados é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo. Dessa forma, quando precisar intervir em bancos de dados, o profissional deve seguir as seguintes instruções:

- Não devem ser realizadas quaisquer mudanças nos dados de banco de dados sem pleno conhecimento e autorização do responsável pela informação do cliente;
- O responsável pela informação do cliente deve ter ciência dos impactos e riscos decorrentes das mudanças que forem autorizadas por ele, por isso, o documento emitido pelo responsável pela informação, que autoriza a mudança nos dados de banco de dados, deve constar que o responsável pela informação está ciente dos impactos e dos riscos e que está de acordo com eles;
- Não devem ser realizadas quaisquer mudanças nos dados de banco de dados que porventura possam modificar o comportamento do sistema de informação, mesmo com solicitação e autorização do responsável pela informação. Exceto, apenas, quando o comportamento do sistema for identificado como sendo incorreto e não houver tempo hábil para sua adaptação ou correção;
- Todos os *scripts* em linguagem SQL ou outras linguagens, que forem enviados para execução no ambiente de produção, devem ser testados e validados antes, em ambiente de homologação confiável;
- Todos os dados que forem alterados ou incluídos em ambiente de produção devem ser antes testados e validados em ambiente de homologação confiável;
- Como “testados e validados em ambiente de homologação confiável” entende-se que, após todas as verificações e precauções, o script e/ou dado não apresenta riscos e que seu resultado está de acordo com o efeito planejado, sem qualquer erro, falha ou efeito colateral indesejado;
- O ambiente de homologação é confiável quando o conjunto de dados a serem testados, bem como toda a estrutura da base de dados, são idênticos aos do ambiente de produção;
- Todos os dados a serem alterados ou incluídos em ambiente de produção devem ser confiáveis, verdadeiros e sua origem possa ser verificada;
- Todas as mudanças devem preceder de análise de impacto e plano de recuperação, em caso de ocorrerem falhas ou resultados indesejados;
- O plano de recuperação de falhas deve ser testado para garantir que será eficaz em caso de necessidade de sua aplicação, para que não aumente o impacto do incidente.

e) O profissional responsável pelo envio do *script* de banco de dados para execução em ambiente de produção deve:

- Ter conhecimento de como aplicar o plano de recuperação de falhas;
- Acompanhar a execução do *script* e verificar se o resultado está de acordo com o planejado e isento de erros ou falhas;
- Em caso de ocorrência de falhas, durante ou após a execução do *script* de banco de dados, deverá executar o plano de recuperação de falhas e alertar sua chefia imediata, com o objetivo de mitigar impactos à disponibilidade, integridade e autenticidade dos dados e informações, bem como dos sistemas que o utilizam;

- Seguir as boas práticas publicadas pela equipe de DBAs da Coordenação de Hospedagem (Data Center) e equipe de Arquitetura de Software da Gerência de Soluções.

4.5. PROCEDIMENTO PARA EXECUÇÃO DE *SCRIPTS* DE BANCOS DE DADOS EM AMBIENTES DE PRODUÇÃO

Há duas formas de executar *scripts* de bancos de dados em ambientes de produção:

a) **Primeira**: *Scripts* que requerem baixa complexidade ou que possuem baixo risco podem ser executados pelo sistema de execução de *scripts*. Para encaminhar *scripts* pelo sistema de execução de *scripts*, é necessário executar os seguintes procedimentos e requisitos:

- Acessar o tutorial da ferramenta de execução de *scripts* "Ferramenta BDWEB" disponível em: https://eurisko.ima.sp.gov.br;
- Ter acesso ao sistema de execução de *scripts*. O acesso é atribuído ao funcionário, analista ou técnico, de acordo com a alçada definida no projeto pelo gestor do funcionário;
- Acessar o sistema de execução de *scripts* usando usuário e senha de acesso de rede;
- Após a execução do *script*, verificar quais foram os resultados. Em caso de falhas, inicie o procedimento de recuperação de falhas imediatamente;
- Em caso de falhas, informe a chefia imediata e a equipe de DBAs, por e-mail, e conforme a urgência, por telefone também.

b) **Segunda:** Por intermédio da equipe de DBAs. É recomendado que a equipe de DBAs sempre intermedie processos de mudança em bancos de dados dos ambientes de produção, quando as mudanças forem mais complexas e/ou quando a mudança tiver riscos importantes que precisem ser contidos ou mitigados rapidamente. Para encaminhar *scripts* por intermediação da equipe de DBAs, é necessário executar os seguintes procedimentos e requisitos:

- Ter autorização para encaminhar *scripts* de banco de dados do ambiente de produção. A autorização é concedida pelos gerentes responsáveis pelo sistema impactado.A autorização deve ser feita do gerente ao funcionário, definindo o nome completo, matrícula e e-mail do funcionário autorizado e em quais bancos de dados possui alçada para efetuar modificações em produção;
- O funcionário com a devida autorização deve encaminhar chamado diretamente à equipe de DBAs, usando a ferramenta de abertura de chamados;
- No corpo do chamado ou no seu anexo, deve conter, no mínimo, as seguintes informações:
  - Nome do servidor:*<exemplo: pierce.ima.sp.gov.br>*
  - Tipo de banco de dados: *<exemplo: MySQL, PostGres, Oracle>*
  - Nome da base:
  - Sistema afetado:
  - Número de solicitação (RedMine):
  - Outros Chamados:
  - Objetivo: *<descrever de forma detalhada>*
  - Resultado esperado: *<descrever o que deve ocorrer após a execução do "script", em relação a mudança dos dados e como o DBA deverá avaliar se ocorreu o esperado>*
  - Ação a ser tomada pelo DBA em caso de sucesso: *<descrever o que o DBA deve fazer se o resultado for conforme o descrito no campo do item "resultado esperado">*
  - Ação a ser tomada pelo DBA em caso de fracasso: *<descrever o que o DBA deve fazer se o resultado não ocorrer conforme o descrito no campo do item "resultado esperado">*
  - Motivo do *script*: *<descrever o motivo de forma detalhada>*
  - Instruções para rodar o *script*: *<descrever como e quando o "script" deverá ser executado> <se houver mais de um "script" no chamado, informar a ordem de execução e as condições para executar o próximo>* <Exemplo: rodar a qualquer tempo / rodar na janela das 18 às 19 horas, etc.>
  - *Script*: *<em linha, ou no anexo>*
- *Scripts* complexos, que envolvam sistemas críticos, devem ser planejados com maior antecedência, para possibilitar que a equipe de DBAs possa avaliar os impactos nos ambientes de bancos de dados da produção, bem como, se necessário, efetuar *backups* que podem levar dias devido a quantidade de dados;
- Acompanhar a execução do *script*. Caso requeira uma análise de performance enquanto o *script* é executado, solicite que o acompanhamento seja feito pela equipe de DBAs e também, para ser avisado quando for iniciar a execução do *script*;
- Após a execução do *script*, verifique quais foram os resultados e, em caso de falhas, inicie imediatamente o procedimento de recuperação de falhas planejado;
- Em caso de falhas, informe sua chefia imediata e a equipe de DBAs, por e-mail, e conforme a urgência, por telefone também;
- Em caso de falta de informações ou de dúvidas, a equipe de DBAs não irá executar o chamado, encerrando-o e comunicando ao solicitante para que complemente ou melhore o nível das informações;
- Se precisar que a equipe de DBAs faça revisão no *script*, para avaliar consistências e performance, especifique essa necessidade no chamado. No entanto, essa atividade poderá levar mais tempo em função da alocação da equipe e da complexidade do projeto.

c) Um funcionário que tenha acesso para execução de *scripts*, por meio do sistema de execução de *scripts* (primeira forma), não está autorizado a solicitar execução de *scripts* por intermédio da equipe de DBA (segunda forma), e vice-versa.

5. DISPOSIÇÕES FINAIS

5.1. Os casos omissos serão resolvidos pelo Gerente de Sustentação.

5.2. Este documento é Anexo à Política de Segurança da Informação da Informática de Municípios Associados, NA 27;

5.3. Revogam-se as disposições em contrário.

TERMO DE CIÊNCIA E RESPONSABILIDADE NO ACESSO ÀS INFORMAÇÕES DOS BANCOS DE DADOS E SISTEMAS EM AMBIENTE DE PRODUÇÃO IMA

Eu, ..., declaro que tomei conhecimento e estou plenamente esclarecido e consciente das normas e procedimentos adotados pela IMA e que devo observar e cumprir as instruções deste Termo de Ciência e Responsabilidade.

a) É minha responsabilidade zelar pela integridade, confidencialidade e disponibilidade dos dados e informações contidas nos sistemas, devendo comunicar por escrito à minha chefia imediata quaisquer indícios de falhas identificadas, bem como, irregularidades que possam expor os sistemas à exploração de vulnerabilidades, mesmo que em bases e sistemas que não façam parte do meu escopo de trabalho.

b) Responderei pelas consequências das ações ou omissões de minha parte, que possam colocar em risco ou comprometer o sigilo, a confidencialidade, a integridade e a disponibilidade dos dados e informações dos bancos de dados, sem prejuízo da responsabilidade penal e civil e de outras infrações disciplinares.

c) Estou sujeito a auditoria interna ou externa, a ser realizada sem aviso prévio, mesmo que após findado o meu contrato de trabalho, de forma que as ações por mim executadas poderão ser analisadas, reproduzidas e utilizadas como prova ou indício em sindicâncias internas ou ações em outras esferas, inclusive, mas não se limitando, a cível.

Constitui infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos do sistema ou bancos de dados da administração pública, com o fim de obter vantagem indevida para si ou para outrem ou para causar dano, bem como, modificar ou alterar sistemas de informações ou programas de informática sem autorização ou sem solicitação de autoridade competente, ficando o infrator sujeito às punições previstas no Código Penal Brasileiro, conforme responsabilização por crime contra a Administração Pública, tipificado no art. 313-A e 313-B.

Declaro também **ESTAR DE ACORDO** com os procedimentos estabelecidos na NA 27 - Políticas de Segurança da Informação e em seu Anexo I – **ACESSO AOS BANCOS DE DADOS DE PRODUÇÃO**, comprometendo-me a respeitá-los e cumpri-los plena e integralmente e que, restando qualquer dúvida, deverei saná-la junto ao meu superior imediato antes de tomar qualquer atitude.

Campinas, ___ de _____ de 20___

Documento assinado eletronicamente por **MARCIO FERNANDO CORREA RICARDO**, **Diretor(a) de Governança Corporativa e Compliance**, em 11/12/2018, às 10:01, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

Documento assinado eletronicamente por **LUANA MOISES FERREIRA MACIEL**, **Gerente Jurídico**, em 04/01/2019, às 14:50, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

Documento assinado eletronicamente por **LEANDRO TELLES SALGUEIRO BARBONI**, **Diretor(a) Técnico**, em 07/01/2019, às 09:57, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

A autenticidade do documento pode ser conferida no site https://sei.campinas.sp.gov.br/verifica informando o código verificador **1106044** e o código CRC **7825F3B5**.

IMA.2017.00001318-18 1106044v6

INFORMÁTICA DE MUNICÍPIOS ASSOCIADOS
Rua Bernardo de Sousa Campos, nº 42 - Bairro Ponte Preta - CEP 13041-390 - Campinas - SP

Inf. Mun. Assoc./IMA-DP/IMA-DP-DGCC

NORMA ADMINISTRATIVA

Campinas, 22 de abril de 2019.

NORMA ADMINISTRATIVA – 027

Assunto: *POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - ANEXO II*

Vigência: na data de sua publicação

ANEXO 2

COMUNICAÇÃO ELETRÔNICA

I. OBJETIVO

Estabelecer as responsabilidades, os requisitos básicos e a conduta adequada nas comunicações eletrônicas no ambiente de Tecnologia da Informação e Comunicação da IMA.

II. INTRODUÇÃO

A boa comunicação com colegas de trabalho, clientes, fornecedores e público externo é fundamental para o bom relacionamento pessoal, integração, sucesso nos projetos de trabalho e fortalecimento empresarial.

Os usuários devem estar cientes que, sob o aspecto de segurança da informação, o uso da comunicação eletrônica é classificado de alto risco. Assim, devem observar o disposto nas Políticas de Segurança da Informação da IMA – NA 027 e na Lei Geral de Proteção de Dados – Lei 13.709/18.

III. APLICAÇÃO

Aplica-se aos usuários dos recursos de comunicação eletrônica disponibilizados pela IMA, sendo a utilização autorizada com o Termo de Responsabilidade disponível na unidade de Folha de Pagamento e Benefícios e arquivado no prontuário do funcionário.

IV. UTILIZAÇÃO DE CORREIO ELETRÔNICO

a. O e-mail é um documento oficial da empresa e uma ferramenta de comunicação muito importante. Assim, seja claro, objetivo, utilize vocabulário adequado e após terminar de escrevê-lo, revise o texto antes de enviar.

b. O usuário de correio eletrônico deve ter cautela para acesso ou execução de arquivos ou programas baixados ou recebidos por correio eletrônico. Como parte de seu esforço pela segurança deve assegurar-se que o sistema de antivírus instalado na máquina esteja funcionando a contento.

V. SISTEMA DE MENSAGEM INSTANTÂNEA

A comunicação instantânea, necessária à realização das atividades profissionais entre os funcionários, deve ser efetuada somente pela plataforma Talk IMA, que fornece comunicação por mensagens de texto, de voz e, em alguns casos, por vídeo conferência.

Para utilização é necessária a instalação do software disponível em: https://rocket.chat/install. Existe a opção de instalação no desktop Windows e Linux, no celular ou acesso via navegador pelo link: https://talk.ima.sp.gov.br.

VI. INTRANET

A Intranet IMA foi criada para ser um portal de conteúdo corporativo com informações de produtos e serviços da IMA, recursos humanos, finanças, governança corporativa, compliance, processos de trabalho, entre outros. Também, deve ser utilizada para publicações de notícias da empresa, eventos e utilidade pública.

Para facilitar a utilização, será organizada por assunto, sendo que haverá um espaço específico para postagem de classificados.

Assim, é permitida a publicação de pequenos anúncios classificados dos funcionários, indicando-se que os contatos necessários sejam efetuados por telefone e fora da jornada de trabalho.

VII. RESPONSABILIDADES DO USUÁRIO

a. Cumprir com o estabelecido nesta Norma e seguir todos os procedimentos de segurança da informação para utilização de comunicação eletrônica.

b. O serviço de correio eletrônico e chat da empresa são ferramentas de trabalho concedidas ao funcionário, portanto, utilizar somente para a execução de suas funções.

c. Utilizar a Intranet como um canal para publicação de comunicações oficiais da empresa, matérias educativas e noticias de utilidade pública.

d. Estar ciente que a IMA possui mecanismos e o direito de monitorar, registrar e analisar o tráfego nas suas redes de comunicação e o uso de correio eletrônico, emitir relatórios, quando necessário, para certificar-se do cumprimento desta norma.

> d.1. Os empregados em teleatendimento ficam cientes também que, são monitorados seus atendimentos, bem como, pode ocorrer gravação de voz e monitoramento nas comunicações escritas nas ferramentas de trabalho.

e. Enviar suas dúvidas ou sugestões por email ou consultar por telefone à área responsável e não postar na Intranet.

f. Cada usuário é responsável por todas as atividades realizadas com seu login e senha, portanto, deve mantê-los confidenciais, jamais divulgar ou compartilhar, pois são pessoais e intransferíveis.

VIII. NÃO É PERMITIDO

a. Utilizar a Intranet para fazer, por conta própria, propaganda, comércio ou negociação habitual.

b. Inserir comentários, perguntas ou dúvidas em anúncios classificados postados na intranet, uma vez que suas dúvidas e comentários devem ser efetuados diretamente com o anunciante e fora do horário de trabalho.

c. Utilizar a Intranet como grupo de bate-papo.

d. Postar na Intranet conteúdo ou comentários ofensivos ou inadequados.

e. Efetuar em qualquer meio, a divulgação, compartilhamento e o uso indevido de informações sigilosas ou de propriedade da IMA ou de seus clientes.

f. Distribuir qualquer material que caracterize violação de direito autoral.

g. Enviar mensagens que contenham código executável ou envio de arquivo de qualquer outra extensão que represente um risco à segurança, de acordo com os critérios estabelecidos pela Gerência de Sustentação da IMA.

h. Enviar mensagens do tipo “corrente”, “spam” ou o envio intencional ou acidental de mensagens que contenham vírus eletrônico ou qualquer forma de programação prejudicial ou danosa.

i. Utilizar listas de endereços eletrônicos da IMA ou de seus clientes para a distribuição de mensagens que não sejam de estrito interesse funcional.

j. Enviar, publicar ou armazenar material de pornografia, ameaças, difamação ou assédio, assuntos de caráter obsceno, prática de qualquer tipo de discriminação, pedofilia, intolerância e de outros contrários à Lei.

k. Enviar, publicar, armazenar ou manusear material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente norma, lesivos aos direitos e interesses da IMA ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos, dados ou arquivos ou prejudicar a imagem da empresa ou de qualquer de seus clientes.

IX. DAS PENALIDADES

a. A não observância desta Norma implicará na aplicação de sanções administrativas, cíveis ou penais, previstas na legislação.

Nota: Caso a transgressão cometida caracterize qualquer tipo de crime, será registrado um Boletim de Ocorrências na Delegacia de Repressão a Crimes de Informática do Estado de São Paulo.

X. DISPOSIÇÕES FINAIS

a. A IMA se reserva o direito de auditar e monitorar o conteúdo relacionado ao uso dos sistemas de comunicação da empresa, para garantir o cumprimento da presente norma.

b. A IMA se reserva o direito emitir relatórios para verificar se o uso dos meios de comunicação eletrônica está de acordo com o estabelecido nesta norma.

c. Constatada não conformidade poderão ser tomadas ações como:

c.1. Suspender ou cancelar o acesso;

c.2. Notificar os gestores dos responsáveis.

d. Esta Norma Administrativa será levada ao conhecimento de todos os funcionários da IMA, publicando-a na Intranet e em informativo por e-mail a todos os usuários.

e. Os casos omissos serão resolvidos pela Diretoria.

f. Revogam-se as disposições em contrário, em especial a Norma Administrativa 004/2010.

Elaboração:

Gerência de Soluções

Gerência de Sustentação

- Unidade de Hospedagem de Dados e Segurança da Informação

Governança Corporativa e Compliance.

Classificação: Público

Documento assinado eletronicamente por **LUANA MOISES FERREIRA MACIEL**, **Gerente Jurídico**, em 24/04/2019, às 12:43, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

Documento assinado eletronicamente por **MARIO ARMANDO GOMIDE GUERREIRO**, **Diretor(a) Administrativo e Financeiro**, em 24/04/2019, às 17:25, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

Documento assinado eletronicamente por **LEANDRO TELLES SALGUEIRO BARBONI**, **Diretor(a) Técnico**, em 25/04/2019, às 14:55, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

Documento assinado eletronicamente por **MARCIO FERNANDO CORREA RICARDO**, **Diretor(a) de Governança Corporativa e Compliance**, em 25/04/2019, às 17:29, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

A autenticidade do documento pode ser conferida no site https://sei.campinas.sp.gov.br/verifica informando o código verificador **1391644** e o código CRC **3F90A1EE**.