PUBLICIDADE LEGAL

SEMASA

DEPARTAMENTO ADMINISTRATIVO E FINANCEIRO

Portarias assinadas pelo Senhor Superintendente - **ENG.º AJAN MARQUES DE OLIVEIRA**

PORTARIA N.º 535/2017, 17 DE NOVEMBRO DE 2017

DISPÕE sobre a Política Corporativa de Segurança da Informação do Serviço Municipal de Saneamento Ambiental de Santo André - SEMASA

ENG.º AJAN MARQUES DE OLIVEIRA, Superintendente do Serviço Municipal de Saneamento Ambiental de Santo André - SEMASA, no uso de suas atribuições legais,

CONSIDERANDO que a Autarquia produz e recebe informações essenciais ao exercício de suas competências constitucionais, legais e regulamentares, e que essas informações são patrimônio da Instituição e devem permanecer íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

CONSIDERANDO que as informações no SEMASA são armazenadas em diferentes suportes, veiculadas por diferentes formas, tais como meio impresso, eletrônico e, portanto, vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

CONSIDERANDO que as normas da Associação Brasileira de Normas Técnicas - ABNT NBR ISO IEC 27001:2013 e 27002:2013 estabelecem, respectivamente, o sistema de gestão e o código de boas práticas em segurança da informação e recomendam a implantação e revisões periódicas da política de segurança da informação das instituições;

CONSIDERANDO a Lei nº 12.965/2014 (MARCO CIVIL DA INTERNET):

CONSIDERANDO, por fim, os direitos e garantias individuais assegurados nos incisos IV, IX, X, XII, XIV e XXXIII do artigo 5º da Constituição Federal, bem como o disposto na Lei Federal nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso à informação,

RESOLVE:

Capítulo I
DAS DISPOSIÇÕES GERAIS

Art. 1º A Política Corporativa de Segurança da Informação do Serviço Municipal de Saneamento Ambiental de Santo André (PCSI) observará os princípios, as diretrizes e os objetivos estabelecidos nesta Resolução, bem como às disposições constitucionais, legais e regimentais vigentes.

Parágrafo único. Integram, também, a PCSI normas gerais e específicas de segurança da informação, bem como procedimentos complementares, destinados à proteção da informação e à disciplina de sua utilização, emanados no âmbito do SEMASA.

Art. 2º A PCSI alinha-se às estratégias do SEMASA e se aplica a todos, cujo acesso às informações recebidas ou produzidas pela Autarquia tenha sido autorizado.

Capítulo II
DAS DEFINIÇÕES

Art. 3º Para os efeitos da Política Corporativa de Segurança da Informação estabelecida por esta Resolução, entende-se por:
I - ativo de informação: recurso utilizado na produção, processamento, armazenamento, transmissão e recuperação da informação, incluindo a própria informação, sistemas de informação, locais onde se encontram esses meios e as pessoas que a eles têm acesso;
II - ciclo de vida da informação: conjunto de eventos relacionados à criação ou obtenção, à classificação, à distribuição, ao uso, ao armazenamento, ao descarte ou à guarda permanente da informação;
III - classificação da informação: ação que define o grau de sigilo e os grupos de acesso atribuídos à informação, visando a garantir um nível adequado de proteção;
IV- confidencialidade: garantia de que a informação seja acessada somente pelos usuários autorizados;
V - continuidade de negócios: capacidade estratégica e tática da organização de se planejar e responder a incidentes e interrupções de negócios para conseguir continuar suas operações em um nível aceitável previamente definido;
VI - custodiante da informação: usuário, grupo de trabalho ou área responsável pela manutenção dos requisitos de segurança associados aos ativos da informação sob sua guarda;
VII - desclassificação: ação que cancela a classificação, tornando públicos dados, informações e materiais sigilosos;
VIII - disponibilidade: garantia de que usuários possam ter pronto acesso às informações segundo sua demanda e em conformidade com a política de segurança;
IX - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;
X - gestão de riscos de segurança da informação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
XI - gestor da informação: responsável pela definição dos grupos de acesso, bem como dos requisitos de segurança associados aos ativos da informação em matéria de sua competência ou inerente à sua área de atuação;
XII - governança da segurança da informação: lideranças, estruturas organizacionais e processos que protegem a informação, visando a direcionar a gestão da segurança da informação de forma eficaz e transparente, alinhada com o negócio e considerando a evolução dos objetivos estratégicos da organização;
XIII - grau de sigilo: gradação atribuída a dados, informações ou áreas considerados sigilosos, em decorrência de sua natureza ou conteúdo;
XIV - grupo de acesso: pessoas, grupos de trabalho ou áreas autorizadas a terem acesso à determinada informação;
XV - incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha potencial para comprometer as operações do negócio e ameaçar a segurança da informação;
XVI - informação: conjunto de dados relacionados entre si que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
XVII - informação classificada como sigilosa: aquela que em razão da sua imprescindibilidade à segurança da sociedade ou do Estado, é classificada como ultrassecreta, secreta ou reservada, de acordo com a Lei 12.527, de 2011;
XVIII - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;
XIX - informação sigilosa: aquela abrangida pelas hipóteses legais de restrição de acesso ou a classificada como sigilosa;
XX - integridade: garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, inclusive quanto à origem, trânsito e destino;
XXI - não-repúdio: garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;
XXII - processo de negócio: conjunto de ações e atividades inter-relacionadas realizadas para obter um conjunto especificado de produtos, resultados ou serviços;
XXIII - reclassificação: ação de alterar a classificação de dado, informação, material ou área sigilosos;
XXIV - risco de segurança da informação: possibilidade de uma ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, prejudicando a organização;
XXV - rotulação: ato de registrar e evidenciar o grau de sigilo ou a natureza da restrição de acesso à informação;
XXVI - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
XXVII - Sistema de Gestão da Segurança da Informação - SGSI: sistema baseado na abordagem de riscos do negócio, que visa a estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação;
XXVIII - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
XXIV - usuário: pessoa autorizada a ter acesso a informações produzidas ou recebidas pelo SEMASA, conforme as medidas de proteção estabelecidas.

Art. 4º São atributos inerentes à segurança da informação:
I - autenticidade: característica que comprova que a informação foi produzida, expedida, recebida, modificada ou destruída por determinado indivíduo, equipamento, sistema, órgão ou entidade, de modo a garantir o não-repúdio quanto à transmissão ou à recepção da mesma;
II - criticidade: define a importância da informação para a continuidade do negócio da instituição.

Art. 5º Para fins de segurança da informação, os usuários são classificados em:
I - usuário interno: o servidor, o contratado ou o conveniado da Autarquia, que no exercício de suas funções, tenham acesso a informações produzidas ou recebidas pelo SEMASA;
II - usuário externo: a pessoa física ou a pessoa jurídica que tenha acesso a informações produzidas ou recebidas pelo SEMASA e que não seja caracterizada como usuário interno.

§ 1º Os usuários internos e externos estão sujeitos às diretrizes, às normas e aos procedimentos de segurança da informação da PCSI.
§ 2º Os usuários internos são responsáveis por garantir a segurança das informações do SEMASA a que tenham acesso e por reportar à Diretoria de Gestão e Governança os incidentes de segurança da informação de que tenham conhecimento.

Capítulo III
DOS PRINCÍPIOS, DAS DIRETRIZES E DOS OBJETIVOS

Art. 6º A segurança da informação no SEMASA abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos princípios básicos da administração pública, bem como os inerentes à segurança da informação, quais sejam: disponibilidade, integridade e confidencialidade.

Art. 7º São diretrizes da Política Corporativa de Segurança da Informação, no âmbito do SEMASA:
I - a observância da publicidade como preceito geral e do sigilo como exceção;
II - o alinhamento das ações de segurança da informação às atividades institucionais e às iniciativas estratégicas do SEMASA;
III - a gestão sistêmica da segurança da informação;
IV - a incorporação da segurança como requisito essencial dos sistemas de informação, informatizados ou não;
V - a observância de leis, regulamentos e obrigações contratuais aos quais os processos de negócio estão sujeitos, bem como as normas e boas práticas, nacionais e internacionais, aplicáveis;
VI - a instituição de normas específicas e procedimentos para a segurança da informação aderentes a esta Política;
VII - o respeito aos legítimos interesses dos usuários no acesso e no uso da informação;
VIII - a participação de todos, de modo a prevenir, detectar e responder aos incidentes de segurança da informação;
IX - a capacitação adequada dos usuários frente às necessidades de segurança da informação.

Art. 8º Respeitando os princípios e diretrizes descritos nos artigos 6º e 7º, esta Política tem como objetivos:
I - instituir uma cultura organizacional aderente à segurança da informação, compreendendo ações destinadas a fomentar entre os usuários a constante observância quanto às práticas destinadas à preservação dessa segurança;
II - implantar a gestão dos riscos relacionados à segurança da informação;
III - estabelecer mecanismos que visem a garantir a segurança da informação nos projetos, processos e atividades do SEMASA;
IV - implementar a governança da segurança da informação.

Capítulo IV
DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 9º As informações produzidas ou recebidas pela Autarquia poderão ser classificadas em função do seu grau de disponibilidade, de integridade e de sigilo.

§ 1º Norma específica disciplinará a classificação da informação, no âmbito do SEMASA.
§ 2º O acesso e o uso das informações devem ser controlados de acordo com a respectiva classificação.

Capítulo V
DAS RESTRIÇÕES DE ACESSO

Art. 10. O acesso a informações sigilosas, produzidas ou recebidas pelo SEMASA, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários internos.

Parágrafo único. Para acesso às informações sigilosas do SEMASA, os servidores do SEMASA ou à disposição do SEMASA deverão declarar compromisso com as práticas, responsabilidades e obrigações previstas nesta PCSI e em seus normativos correlatos.

Art. 11. Nos editais de licitação, nos contratos, nos convênios, nos acordos de cooperação técnica e em outros instrumentos congêneres celebrados com o SEMASA, deverá constar, quando necessário, cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta PCSI, bem como deverá ser exigida, da entidade contratada/conveniada, a assinatura do Termo de Sigilo das Informações, conforme modelo proposto no anexo único.

Capítulo VI
DAS RESPONSABILIDADES

Art. 12. Compete à Coordenadoria de Tecnologia da Informação - CTI:
I - coordenar o Sistema de Gestão de Segurança da Informação - SGSI, incluindo estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos;
II - coordenar e acompanhar a implementação da PCSI e normas complementares;
III - homologar processos de negócio e procedimentos operacionais necessários, nos aspectos relacionados à Segurança da Informação - SI;
IV - monitorar e avaliar periodicamente as práticas de segurança da informação adotadas pelo SEMASA;
V - coordenar a gestão dos riscos e de incidentes relacionados à segurança da informação;
VI - elaborar proposta e promover atualização periódica de plano com medidas que garantam a continuidade das atividades da Autarquia e o retorno à situação de normalidade em caso de desastre ou falhas nos recursos que suportam os processos vitais de negócio da Autarquia;
VII - coordenar, ações permanentes de divulgação, treinamento, educação e conscientização dos usuários, em relação aos conceitos e às práticas de segurança da informação em toda sua abrangência; VIII - adotar as medidas necessárias para análise periódica dos documentos sob custódia do SEMASA, submetendo ao Comitê de Segurança da Informação (CSI), previsto no artigo 16º desta Portaria, proposta motivada de classificação dos documentos a terem tratamento reservado, bem como dos procedimentos a serem adotados na sua tramitação e os prazos e eventos para sua desclassificação;
IX - adotar as medidas necessárias ao tratamento de situações inerentes à segurança da informação preexistentes à edição da PCSI;
X - prestar apoio técnico e administrativo às atividades do Comitê de Segurança da Informação (CSI).

Parágrafo único. Cabe às demais unidades do SEMASA, no âmbito de suas competências, a implementação e o acompanhamento de ações para segurança da informação.

Art. 13. São responsabilidades do gestor da informação, no que concerne às informações sob sua gestão, produzidas ou recebidas pelo SEMASA:
I - garantir o cumprimento das normas e procedimentos relativos à segurança das informações;
II - definir procedimentos e grupos de acesso, observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de segurança pertinentes;
III - conscientizar usuários internos em relação aos conceitos e às práticas de segurança da informação;
IV - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários internos;
V - rotular a informação sigilosa em matéria de sua competência ou inerente à sua área de atuação, enquadrada em hipótese legal de sigilo ou de segredo de justiça.

Art. 14. São responsabilidades do custodiante da informação:
I - garantir a segurança das informações, durante todo o seu ciclo de vida, observando se, na hipótese de informação sigilosa, as disposições normativas específicas sobre a matéria;
II - comunicar tempestivamente ao gestor da informação sobre situações que comprometam a segurança das informações sob sua custódia.

Art. 15. O uso de recursos computacionais do SEMASA será regulamentado em ato normativo, respeitando-se os dispositivos legais.

Capítulo VII
DAS DISPOSIÇÕES FINAIS

Art. 16. Fica instituído o Comitê de Segurança da Informação (CSI), órgão colegiado de natureza consultiva e de caráter permanente.

§ 1º O Comitê tem por finalidade formular e conduzir diretrizes para a PCSI, analisar periodicamente sua efetividade, propor normas e mecanismos institucionais para melhoria contínua, bem como assessorar a unidade organizacional responsável pela Segurança da Informação.
§ 2º Compete também ao Comitê a revisão da PCSI, no máximo a cada 2 (dois) anos, de modo a atualizá-la frente a novos requisitos corporativos.
§ 3º A composição e os regulamentos do Comitê serão estabelecidos por ato da Superintendência.
§ 4º Até o estabelecimento da composição do CSI, nos termos do § 3º, integrarão interinamente esse Comitê os seguintes membros: 1 membro da Superintendência, 1 Membro da Coordenadoria de Assuntos Jurídicos, 1 Membro da Coordenadoria de Comunicação Social, 1 membro do Departamento Administrativo e Financeiro e 1 membro da CTI.

Art. 17. A Gestão de Segurança da Informação do SEMASA abordará os seguintes aspectos, sem prejuízo de outros assuntos inerentes ao tema:
I - acesso, proteção e guarda da informação, em especial à informação sigilosa;
II - aquisição, desenvolvimento e manutenção de sistemas informatizados;
III - autenticação e controle de acesso à rede de dados, aos serviços de tecnologia da informação e aos sistemas de informação do SEMASA;
IV - classificação da informação, observado o disposto na Lei nº 12.527, de 2011, e em sua regulamentação específica no âmbito do SEMASA;
V - coleta e preservação de registros de segurança;
VI - cópias de segurança de dados e de sistemas informatizados;
VII - gestão de incidentes de segurança da informação;
VIII - gestão de continuidade de negócios;
IX - segregação de ambientes de tecnologia da informação, com a implementação de ambientes distintos de desenvolvimento, teste, homologação e produção de sistemas computacionais, feita em atendimento ao princípio da separação de funções, com a definição de papéis e responsabilidades específicos para cada ambiente;
X - segurança das instalações que hospedam os conteúdos informacionais e os recursos computacionais para os quais essa normatização seja necessária.
XI - definir o conteúdo da rede mundial de computadores acessível a partir da rede corporativa e de visitantes do SEMASA.

Art. 18. As informações produzidas por usuários internos, no exercício de suas funções, são patrimônio intelectual do SEMASA e não cabe a seus criadores qualquer forma de direito autoral.

Art. 19. A inobservância às normas da PCSI pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

PORTARIA N.º 536/2017, 17 DE NOVEMBRO DE 2017

DISPÕE sobre a Política de Uso Aceitável dos Recursos de Tecnologia da Informação do Serviço Municipal de Saneamento Ambiental de Santo André - SEMASA.

ENG.º AJAN MARQUES DE OLIVEIRA, Superintendente do Serviço Municipal de Saneamento Ambiental de Santo André -SEMASA, no uso de suas atribuições legais,

CONSIDERANDO que as informações são armazenadas e veiculadas por diferentes formas, incluindo os recursos de Tecnologia da Informação, e são essenciais ao desempenho das atribuições da Autarquia;

CONSIDERANDO o § 6º do artigo 37 da Constituição Federal que dispõe sobre a responsabilidade civil objetiva atribuída aos entes estatais;

CONSIDERANDO as normas da Associação Brasileira de Normas Técnicas - ABNT NBR ISO IEC 27001:2006 e 27002:2005 que estabelecem, respectivamente, o sistema de gestão e o código de boas práticas em segurança da informação recomendam o estabelecimento de regras para o uso aceitável dos ativos de informação;

CONSIDERANDO a Lei nº 12.965/2014 (MARCO CIVIL DA INTERNET),

RESOLVE:

Capítulo 1
Das Disposições Gerais

Art. 1º A Política de Uso Aceitável dos Recursos de Tecnologia da Informação no âmbito do SEMASA, bem como os direitos e as responsabilidades de quem os utiliza, regem-se pelas disposições da presente Resolução.

§ 1º Consideram-se recursos de Tecnologia da Informação do SEMASA o conjunto de ativos de TI mantidos ou operados pelo SEMASA, tais como equipamentos de rede, telecomunicações, computadores, aparelhos telefônicos, dispositivos móveis, dispositivos de armazenamento, programas, banco de dados, sistemas e serviços de TI.
§ 2º Esta Resolução integra a Política Corporativa de Segurança da Informação do SEMASA, instituída pela Portaria nº 535, de 17 de Novembro de 2017 e adota, no que couber, os conceitos definidos na Seção II daquela Resolução.

Art. 2º Esta Portaria aplica-se a todos os usuários que utilizam os recursos de TI do SEMASA.

Art. 3º O SEMASA se reserva no direito de inspecionar, sem a necessidade de aviso prévio, os computadores e qualquer arquivo armazenado, estejam no disco local dos computadores, nas áreas privativas ou nas áreas compartilhadas da rede, visando assegurar o rígido cumprimento desta política.

Capítulo II
DAS DEFINIÇÕES

Art. 4º Para os efeitos desta Resolução, entende-se por:
I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;
II - ativo de informação: recurso utilizado na produção, processamento, armazenamento, transmissão e recuperação da informação, incluindo a própria informação, sistemas de informação, locais onde se encontram esses meios e as pessoas que a eles têm acesso;
III - área privativa: área reservada e exclusiva para armazenamento de informações de um usuário interno, incluindo sua caixa postal;
IV - área compartilhada: área reservada para armazenamento e compartilhamento de informações de um grupo de usuários internos;
V - caixa postal: área individual de armazenamento de mensagens do correio eletrônico;
VI - conta: identificador único que permite acesso aos recursos de TI e o gerenciamento do uso desses recursos;
VII - dispositivos móveis - equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, mas não se limitando a estas: notebooks, smartphones, tablets, pen drives, USB drives, HDs externos e cartões de memória;
VIII - rede Corporativa: conjunto dos recursos de TI disponíveis no âmbito do SEMASA que possibilita o acesso aos diversos serviços de tecnologia da informação;
IX - usuário: pessoa utilizadora dos recursos de TI do SEMASA;
X - usuário interno: servidor, contratado ou conveniado da Autarquia, que no exercício de suas funções, tenham acesso aos recursos de TI do SEMASA;
XI - usuário externo: pessoa física ou jurídica que tenha acesso aos recursos de TI do SEMASA e que não seja caracterizada como usuário interno.

Capítulo III
DAS RECOMENDAÇÕES GERAIS

Seção I
DAS ATIVIDADES PERMITIDAS E DOS DIREITOS DOS USUÁRIOS INTERNOS

Art. 5º O uso dos recursos de TI do SEMASA pelos usuários internos, destina-se às atividades relacionadas com suas atribuições funcionais.

Art. 6º Os recursos de TI deverão ser utilizados respeitando-se os direitos de propriedade intelectual de qualquer pessoa ou empresa.

Art. 7º Respeitado o disposto na Lei Federal nº 9609, de 19 de fevereiro de 1998, que trata da propriedade intelectual de programa de computador, e ressalvadas as exceções previstas em contratos e convênios, são de propriedade do SEMASA os programas desenvolvidos para a Autarquia por usuários internos.

Art. 8º São garantidos aos usuários internos, no exercício de suas funções, após aprovação em treinamento específico:
I - ter conta para acesso à rede corporativa;
II - fazer uso legal dos recursos de TI colocados à sua disposição, respeitadas as normas de utilização estabelecidas pelo SEMASA;
III - ter acesso às informações que lhe são franqueadas nas áreas privativa e compartilhadas com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança;
IV - ter privacidade das informações armazenadas em sua área privativa;
V - ter acesso aos registros de suas ações (logs) existentes na rede corporativa;
VI - ter acesso remoto à rede corporativa do SEMASA, utilizando recursos de TI próprios, observados os requisitos de segurança estabelecidos pela CTI;
VII - solicitar suporte técnico à CTI.

§ 1º Usuários contratados e conveniados terão garantidos apenas os recursos necessários às atividades correspondentes à execução do contrato ou convênio.
§ 2º Sempre que for necessário para atividades de administração dos recursos de TI e suporte técnico ou nos casos de suspeita de violação de regras, a Coordenadoria de Tecnologia da Informação - CTI poderá acessar arquivos de dados privativos ou compartilhados.

Seção II
DAS ATIVIDADES VEDADAS AOS USUÁRIOS INTERNOS

Art. 9º É vedado o uso dos recursos de TI do SEMASA para processar, guardar e/ou encaminhar material de cunho político, não ético, discriminatório, malicioso, obsceno ou ilegal, além de atividades visando:
I - promoção pessoal;
II - venda de produtos ou engajamento em atividades comerciais de qualquer natureza;
III - constrangimento, assédio, calúnia, injúria, difamação, ameaça, ofensa ou agressão;
IV - distribuição voluntária de mensagens não desejadas, como circulares, manifestos políticos, correntes de cartas ou outros sistemas que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os recursos de TI;
V - ocultação de sua identidade quando utilizar os recursos de TI;
VI - acesso não autorizado ou indevido aos recursos de TI;
VII - violação dos sistemas de segurança dos recursos de TI, no que tange à identificação de usuários, senhas de acesso, sistemas de alarme, registro de eventos (log) e demais mecanismos de segurança e restrição de acesso;
VIII - instalação, alteração ou remoção de software sem acompanhamento ou autorização da equipe técnica da CTI.
§ 1º Para notebooks do SEMASA, a autorização para instalação, alteração ou remoção de software é decorrente do Termo de Compromisso, assinado pelo custodiante que optar pelo uso da senha de administrador.
§ 2º Entende-se por custodiante o usuário, grupo de trabalho ou área responsável pela manutenção dos requisitos de segurança associados aos ativos da informação sob sua guarda.

Seção III
DAS OBRIGAÇÕES DOS USUÁRIOS INTERNOS

Art. 10. São obrigações de todos os usuários internos:
I - manter em caráter confidencial e intransferível códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc.);
II - alterar periodicamente a senha de acesso de acordo com os procedimentos estabelecidos pela CTI;
III - zelar por toda e qualquer informação disponível pelos recursos de TI do SEMASA contra alteração, destruição, divulgação, cópia e acesso não autorizados;
IV - desligar ou bloquear computadores em uso quando houver necessidade de ausentar-se fisicamente do local;
V - fazer manutenção na sua área privativa periodicamente, evitando o acúmulo de informações desnecessárias.

§ 1º Os servidores do SEMASA ou à disposição do SEMASA deverão firmar compromisso com as práticas, responsabilidades e obrigações normativas referentes à Política Corporativa de Segurança da

Informação e à Política de Uso Aceitável dos Recursos de Tecnologia da Informação, conforme Termo de Responsabilização e Sigilo, constante no Anexo I.
§ 2º Nos contratos e convênios celebrados com o SEMASA, os contratados e os conveniados deverão assinar o Termo de Sigilo das Informações, assim como comprovar que os seus funcionários e prestadores de serviços, também assinaram, conforme previsto na Portaria 535, DE 2017, que dispõe sobre a Política Corporativa de Segurança da Informação.

Seção IV
DAS OBRIGAÇÕES DA CTI

Art. 11. São obrigações da Coordenadoria de Tecnologia da Informação - CTI:
I - manter e monitorar o uso dos recursos de TI disponibilizados sem interrupções, exceto em casos de imprevistos ou manutenção técnica programada;
II - monitorar a observância deste normativo, devendo, em caso de descumprimento, informar à Superintendência e tomar medidas imediatas de restrições de uso dos recursos, de acordo com o disposto nas normas computacionais;
III - implantar autorização ou restrição de acesso às informações do SEMASA, disponíveis através dos recursos de TI;
IV - autorizar ou restringir o acesso aos recursos de TI;
V - cancelar o acesso aos recursos de TI disponíveis imediatamente após o término do vínculo do usuário interno ou colaborador com o SEMASA;
VI - gerenciar os privilégios de usuários, as senhas de usuários, os procedimentos de logon e de política de troca de senha;
VII - desenvolver, adquirir, manter e auditar os sistemas de informação;
VIII - registrar as ações dos usuários internos na rede corporativa, inclusive o histórico de utilização da internet;
IX - proteger e manter a segurança dos dados armazenados na rede corporativa;
X - realizar a cópia de segurança de dados armazenados em discos de servidores da rede local;
XI - manter atualizadas as configurações necessárias para o acesso externo à rede corporativa, e orientar os usuários internos e colaboradores sobre seu uso e requisitos de segurança;
XII - orientar sobre a configuração dos recursos de TI do SEMASA;
XIII - providenciar o Termo de Compromisso e obter a aceitação dos usuários internos com as práticas, responsabilidades e obrigações previstas na Política Corporativa de Segurança da Informação e seus normativos correlatos.

Parágrafo único. A autorização e a restrição de acesso aos sistemas de informação também incumbem aos gestores dos respectivos sistemas.

Capítulo IV
DAS RECOMENDAÇÕES ESPECÍFICAS

Seção I
DO CONTROLE DE ACESSO

Art. 12. Controle de acesso é um dos mecanismos utilizados para proteger o ambiente de TI. O acesso aos recursos de TI deve ser permitido somente a entidades autorizadas, como usuários internos, de acordo com a Política Corporativa de Segurança da Informação.

§ 1º O direito de uso de qualquer recurso de TI cessa quando o usuário interno terminar o seu vínculo com o SEMASA.
§ 2º O servidor que permanecer em licença com duração superior a 180 (cento e oitenta) dias ou à disposição de outro órgão terá direito de acesso aos recursos de TI de forma limitada.

Art. 13. O acesso a recursos relacionados a sistemas corporativos será provido via perfis de trabalho ou por autorização do gestor da informação envolvida.
Parágrafo único. É considerado gestor da informação o servidor incumbido da definição dos grupos de acesso, bem como dos requisitos de segurança associados aos ativos da informação sob sua responsabilidade.

Art. 14. O cadastro de usuário interno para utilização dos recursos de TI será realizado pela CTI, mediante requisição da chefia da unidade organizacional ou do fiscal do contrato correspondente.

Art. 15. É prerrogativa exclusiva da CTI configurar o compartilhamento de recursos de TI na rede de computadores. Requisições de concessão e alteração de permissões de acesso a recursos de TI devem ser encaminhadas à CTI pela chefia da unidade organizacional interessada ou do fiscal de contrato.

Art. 16. Ao término do vínculo com o SEMASA de servidor, terceirizado, estagiário, conveniado ou prestador de serviço, o chefe da unidade organizacional ou o fiscal do contrato correspondente vinculado deve tomar as providências necessárias para que seja realizado o seu descadastramento.

Art. 17. Na ocorrência da inativação da conta do usuário interno, seus arquivos armazenados nos recursos de TI poderão ser avaliados pela chefia imediata visando à sua eliminação ou preservação.

Art. 18. Caberá ao Departamento Administrativo e Financeiro informar a CTI todo e qualquer desligamento, afastamento superior a 180 (cento e oitenta) dias, transferências, cessão, alteração de setores, ou qualquer outra alteração de funcionários que exija da CTI mudanças no uso dos recursos de informática.

Seção II
DA UTILIZAÇÃO DOS RECURSOS DE TI

Art. 19. Todos os procedimentos de manutenção, instalação, desinstalação, configuração e alteração de hardware e software em recursos de TI disponibilizados pelo SEMASA são prerrogativa exclusiva da CTI.
Parágrafo único. Compete à CTI definir os recursos de TI do SEMASA, bem como homologar a utilização de hardware ou software de propriedade do usuário no ambiente computacional do SEMASA.
Art. 20. Cada unidade organizacional terá disponível uma área compartilhada para guarda dos arquivos compartilhados entre seus usuários, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.
Art. 21. As áreas privativas e compartilhadas possuem tamanho limitado. Caberá à CTI definir os limites de armazenamento, de acordo com a disponibilidade.

Art. 22. Os dados armazenados fora das áreas privativa ou compartilhadas não possuem garantias de integridade, disponibilidade, controle de acesso ou cópia de segurança.

Art. 23. Aos técnicos da CTI é dado o direito de acesso remoto aos computadores e dispositivos móveis do SEMASA, em utilização pelos usuários, para fins de manutenção. O acesso remoto para suporte na área privativa do usuário apenas será iniciado mediante sua anuência, que deverá acompanhar todas as operações executadas pelo técnico da CTI.

Art. 24. As configurações e atribuições de parâmetros em todos os recursos de TI conectados à rede do SEMASA devem estar de acordo com as políticas e normas internas de gerenciamento.

Art. 25. As atividades dos usuários poderão ser reconstituídas a partir de registros de atividades (logs).

Art 26. As ações abaixo relacionadas somente poderão ser concedidas após solicitação do Diretor/Coordenador da área interessada e aprovadas pela CTI. As ações aprovadas somente poderão ser efetivadas/acompanhadas pela equipe da CTI.
I - aquisição ou instalação, bem como recebimento em doação de equipamentos de informática, como microcomputadores, impressoras, scanner, monitores, softwares, dentre outros;
II - aquisição ou instalação de software ou qualquer solução tecnológica voltada para informática;
III - contratação de links de comunicação de acesso à internet, serviços de fibra óptica, linha de voz ou outros;
IV - alterações nas configurações, acréscimos de dispositivos físicos dos equipamentos de informática;
V - alterações de layouts (disposição física do equipamento) por envolver a infraestrutura de lógica e telefonia, observando-se os prazos da Portaria 259, de 05 de abril de 2012;

Seção III
DA UTILIZAÇÃO DA REDE SEM FIO E DISPOSITIVOS MÓVEIS

Art. 27. O uso da rede sem fio é destinado a complementar a rede cabeada, possibilitando o acesso diferenciado para os usuários internos e externos aos recursos de TI do SEMASA.

§ 1º O SEMASA disponibiliza, pelo menos duas possibilidades de conexão à rede sem fio, que são:
I - rede destinada a dispositivos móveis do próprio SEMASA. Esta rede permite acesso tanto à internet quanto à intranet e os sistemas do SEMASA, mediante login semelhante ao dos computadores conectados à rede cabeada;
II - rede destinada ao uso por dispositivos móveis não pertencentes ao SEMASA. Esta rede permite acesso apenas à internet.
§ 2º O uso da rede sem fio por dispositivos móveis pertencentes a usuários internos e colaboradores será regulamentado pela CTI.

Art. 28. Os dispositivos móveis devem ser utilizados considerando-se soluções de segurança, de acordo com a Política Corporativa de Segurança da Informação do SEMASA.

Seção IV
DA UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

Art. 29. As unidades organizacionais disporão de um endereço eletrônico exclusivo para uso regular dos seus servidores, terceirizados e estagiários.
Parágrafo único. Outro endereço eletrônico será disponibilizado, quando solicitado, para recebimento de mensagens de usuários externos à unidade organizacional.

Art. 30. O usuário que perder o vínculo com o SEMASA, permanecer em licença com duração superior a 180 (cento e oitenta) dias ou à disposição de outro órgão terá seu endereço de correio eletrônico excluído e o conteúdo da respectiva caixa postal será mantido conforme Política de backup.

Seção V
DO ACESSO À INTERNET

Art. 31. Todos os usuários internos poderão ter acesso à internet, identificados pela sua conta, de uso pessoal e intransferível.

Art. 32. Cabe à CTI implantar os controles de acesso e mecanismos de auditoria que garantam o monitoramento do acesso à internet pela rede corporativa do SEMASA.

Art. 33. Cabe à Coordenadoria de Tecnologia da Informação-CTI, em conjunto com o Comitê de Segurança da Informação - CSI, instituído pela Portaria nº 535, de 17 de Novembro de 2017 que dispõe sobre a Política Corporativa de Segurança da Informação, definir o conteúdo da rede mundial de computadores acessível a partir da rede corporativa e de visitantes do SEMASA.
§ 1º Será bloqueado o acesso a sites de conteúdo considerado ofensivo, ilegal ou impróprio a exemplo de sites pornográficos, de jogos ou apostas.
§ 2º Os gestores das unidades organizacionais poderão solicitar à CTI restrição de acesso a sites para os usuários das respectivas unidades.

Art. 34. A CTI terá acesso aos históricos de utilização da Internet de todos os usuários do SEMASA e poderá informá-los aos gestores das respectivas unidades organizacionais.

Capítulo V
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 35. Compete à Superintendência, mediante apoio da CTI, garantir a implementação da Política de Uso Aceitável dos recursos de TI do SEMASA, segundo os objetivos, princípios e diretrizes estabelecidos pela Política Corporativa de Segurança da Informação.

Art. 36. Nos casos em que o usuário interno já possua a identificação e o acesso, mas que ainda não tenha declarado compromisso com as práticas, responsabilidades e obrigações previstas na Política Corporativa de Segurança da Informação e seus normativos correlatos, o compromisso deve ser obtido pela CTI em caráter de urgência.

§ 1º Os usuários internos que não encaminharem o termo de compromisso em até 30 (trinta) dias, terão seus acessos suspensos.

Art. 37. A não observância do disposto neste normativo, devidamente apurada e comprovada, pode acarretar o bloqueio da conta de acesso aos recursos de TI do SEMASA.

§ 1º O caso será informado ao usuário infrator, ao seu gerente imediato para ciência e ao Diretor/Coordenador, para deliberação.
§ 2º Além do bloqueio da conta de acesso, o usuário também poderá responder no âmbito administrativo, civil e criminal, pelas infrações cometidas e pelos danos causados em decorrência da não observância da Política Corporativa de Segurança da Informação.

ANEXO I - Termo de Responsabilização e Sigilo

Pelo presente instrumento, eu ____, CPF _______________, identidade _______________, expedida pelo ______, em ________, RE ________,DECLARO , sob pena das sanções cabíveis, nos termos da legislação vigente, que conheço e estou comprometido com as práticas, responsabilidades e obrigações normativas referentes à Política de Segurança Corporativa da Informação e à Política de Uso Aceitável dos Recursos de Tecnologia da Informação do SEMASA

Santo André, ______ de ________________ de ______.

____
Assinatura
Nome do usuário: ____________________________
Departamento/Coordenadoria:____________________________
Gerencia: ____________________________
Encarregatura:____________________________.

No caso de cessão de Notebook ou dispositivo móvel
Modelo:____________________
Patrimônio:____________________
Nº de Série:____________________

DESIGNAR

537/11/2017 - Os servidores: Engº ALEXANDRE PERRI DE MORAES, Engª Química IRACÉLIS IMACULADA DOS SANTOS e Arquiteto ROBSON DA SILVA MORENO para, sob a presidência do primeiro, constituírem a Comissão de Recebimento Definitivo dos serviços executados através do Processo Administrativo nº 2233/2017 referente à obra de impermeabilização da base da Etapa II B Ampliação da área de disposição de resíduos CTR Santo André, que é parte integrante dos serviços contratados no Processo de Compras nº 127/2016, contrato 23/2017.

Serviço Municipal de Saneamento Ambiental de Santo André, em 17 de Novembro de 2017.

ROBSON DE ALMEIDA COSTA
Diretor de Departamento