EMPRESA MUNICIPAL DE DESENVOLVIMENTO DE CAMPINAS S/A - EMDEC

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

EMDEC

Campinas-SP, 08 de novembro de 2021

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Empresa Municipal de Desenvolvimento de Campinas S/A (EMDEC), consciente da importância e da necessidade de adequar as suas operações de tratamento de dados pessoais à LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018) e, baseada na norma NBR ISO/IEC 27.001, definiu esta Política de Segurança da Informação (PSI).

Esta Política objetiva documentar e proteger as informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio da EMDEC, através da padronização de processos, estabelecer requisitos mínimos de segurança e definir um conjunto de controles e mecanismos que garante a confidencialidade, integridade, disponibilidade das informações, além da segurança dos dados tratados e armazenados pela empresa.

A sua aplicabilidade se estende aos empregados da EMDEC, a todos os terceiros, sejam eles pessoas físicas ou jurídicas que atuam para ou em nome da EMDEC em operações que envolvam tratamento de dados pessoais que sejam realizadas no escopo das atividades conduzidas pela EMDEC; aos agentes de tratamento de dados pessoais externos à EMDEC que de qualquer forma se relacionem com a Instituição; e aos titulares de dados pessoais, cujos dados são tratados pela EMDEC.

Todas as operações que envolvam tratamento de dados pessoais, e que sejam realizadas dentro do escopo das atividades conduzidas pela EMDEC estão sujeitas às normativas desta Política.

A LGPD estabelece que a responsabilidade no caso de danos patrimoniais, morais, individuais ou coletivos derivados de violações à legislação de proteção de dados pessoais é solidária, isto é, todos os agentes da cadeia que estão envolvidos no tratamento dos dados pessoais podem ser responsabilizados pelos eventuais danos causados.

Nesse sentido, a possibilidade da EMDEC ser responsabilizada pelas ações de terceiros implica na necessidade de empregar os melhores esforços para verificar, avaliar e garantir que os terceiros cumpram com as legislações de proteção de dados aplicáveis, previstos na LGPD.

Dessa forma, todos os contratos com terceiros deverão conter cláusulas referentes à proteção de dados pessoais, estabelecendo deveres e obrigações envolvendo a temática, e atestando o compromisso dos terceiros com as legislações de proteção de dados pessoais aplicáveis. Todos os terceiros devem assinar o termo de aceitação desta Política de Segurança da Informação, submetendo as atividades contratadas no âmbito da relação com a EMDEC também a essas normativas.

A EMDEC entende que os regramentos dispostos nesta Política de Segurança da Informação somente serão eficazes se houver o comprometimento de todas as partes envolvidas.

DIREITOS E DEVERES

1. DOS USUÁRIOS

I. Respeitar e seguir as normativas apresentadas nesta Política de Segurança da Informação;

II. Responder pela guarda e proteção dos recursos informáticos colocados à sua disposição para o exercício do trabalho, e zelar pela sua utilização;

III. Responder pelo uso exclusivo e intransferível de suas senhas de acesso a recursos de TI e a sistemas utilizados na empresa;

IV. Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;

V. Colaborar com a redução de custos da empresa, evitando, por exemplo, a impressão desnecessária de documentos;

VI. Relatar prontamente à área de TI, por meio de abertura de chamado (disponível em http://suporte.emdec.com.br) qualquer fato ou ameaça à segurança dos recursos de TI, como quebra da segurança, fragilidade, mau funcionamento de equipamento, presença de vírus, etc;

VII. Na impossibilidade da abertura do chamado, o colaborador deverá entrar em contato com o Suporte Técnico da TI, através do ramal 7100, que fará o registro da sua solicitação;

VIII. Assegurar que as informações e dados de propriedade da EMDEC não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico; deste modo, a utilização de dispositivos de armazenamentos de dados, como *pendrives*, discos rígidos externos, cartões SD e outros similares que não sejam fornecidos pela área de TI, fica proibida, a menos que haja aprovação registrada no GLPI, com a ciência e permissão do Gerente ou Líder do colaborador;

IX. Armazenar as informações empresariais em consonância com o capítulo III, item c.

X. Comprometer-se em não auxiliar terceiro ou não provocar invasão dos computadores ou da rede de dados, conforme previsto no artigo 154-A do Código Penal Brasileiro;

XI. Utilizar a assinatura de e-mail, fornecida pela EMDEC, e disponível em http://www.emdec.com.br/eficiente/sites/intranet_2015/pt-br/site.php?secao=email_assinatura, para o envio de e-mails institucionais.

XII. Relatar ao seu responsável hierárquico e à Gerência de TI, o surgimento da necessidade de um novo software para o exercício de suas atividades laborais;

XIII. Encaminhar ao superior hierárquico, após mudança de cargo, de função ou desligamento da empresa, as suas informações produzidas e mantidas no exercício do trabalho, para fins de arquivamento, utilização, descarte ou auditoria;

XIV. Utilizar os recursos tecnológicos para assuntos particulares é permitido ao colaborador, desde que não contrarie a esta Política e orientações internas de conduta, ou prejudique a execução de atividades profissionais de um ou mais

colaboradores; ou afete de forma negativa o relacionamento da empresa com clientes, fornecedores ou parceiros de negócios;

XV. Comprometer-se a não clicar em links desconhecidos ou suspeitos que, porventura, sejam recebidos em seu e-mail institucional. Nesta eventualidade, dar ciência ao nível hierárquico superior e à TI, através da abertura de um chamado no GLPI;

XVI. Manter o sigilo sobre as informações manipuladas em ambiente de trabalho;

XVII. Utilizar o correio eletrônico (*e-mail*) como ferramenta de comunicação para fins profissionais. A disseminação de conteúdos não permitidos, como correntes, pornografia, mensagens racistas, religiosas, políticas ou assuntos que ofendam os bons costumes da sociedade (item 5b do Código de Conduta e Integridade da EMDEC).

XVIII. Responder pelo prejuízo ou dano que vier a provocar à EMDEC ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas;

2. DOS RESPONSÁVEIS HIERÁRQUICOS

I. Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão;

II. Realizar, na fase de contratação e de formalização dos contratos individuais de trabalho CLT, o cumprimento desta PSI, através da coleta de assinatura do colaborador em uma cópia desta Política, arquivamento em prontuário e cientificação da Gerência de TI da EMDEC. A utilização de recursos de TI fica condicionada ao aceite desta Política, pelo colaborador.

III. Autorizar o acesso e definir o perfil do usuário junto ao gestor de liberações da área de TI.

IV. Autorizar solicitações enviadas pela área de TI, referente a solicitações de seus subordinados, realizadas no GLPI;

V. Autorizar as mudanças no perfil do usuário junto ao gestor de liberações da área de TI;

VI. Educar os usuários sobre os princípios e procedimentos de Segurança da Informação;

VII. Notificar imediatamente ao gestor de liberações da área de TI quaisquer vulnerabilidades e ameaças a quebra de segurança;

VIII. Assegurar treinamento aos colaboradores, para o uso correto dos recursos computacionais e sistemas de informação;

IX. Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança;

X. Obter aprovação técnica do gestor de liberações da área de TI antes de solicitar a compra de hardware, software ou serviços de informática;

XI. Adaptar as normas, processos, procedimentos e sistemas sob a sua responsabilidade, a fim de atender a esta PSI;

XII. Comunicar, imediatamente, a Gerência de TI sobre a exclusão ou manutenção de usuário de rede pertencente a colaborador desligado da EMDEC.

3. DA ÁREA DE TI

I. Configurar os equipamentos e sistemas, de modo a cumprir as normativas desta PSI;
II. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
III. Disponibilizar, em servidor apropriado, espaço para o armazenamento de informações empresariais pelos colaboradores. Todas as informações de interesse da EMDEC devem ser gravadas nos diretórios disponibilizados para esta finalidade (Mapeamentos de rede e OneDrive). A área de TI não se responsabiliza por cópias de segurança (*backup*) de conteúdos que estejam salvos no computador do colaborador;
IV. Fornecer sistema que permita a abertura de ordens de serviço (chamados);
V. Restringir ações de exclusão dos logs e trilhas de auditoria;
VI. Garantir segurança do acesso público e manter evidências que permitam a rastreabilidade para auditoria ou investigação;
VII. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;
VIII. Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio;
IX. Gerenciar o descarte de informações a pedido dos solicitantes;
X. Garantir que as informações de um usuário sejam removidas antes do descarte ou disponibilização do equipamento para outro usuário;
XI. Criar a identidade lógica dos colaboradores na empresa, de modo a permitir a utilização de computadores, sistemas, e qualquer outro ativo de informação pertinente à execução de suas funções;
XII. Proteger todos os ativos de informação da empresa contra códigos maliciosos e ou vírus;
XIII. Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção;
XIV. Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da empresa;
XV. Realizar inspeções periódicas de configurações técnicas e análise de riscos;
XVI. Dar suporte à instalação e utilização das assinaturas e certificados digitais.
XVII. Garantir que, após o recebimento da notificação da área de Recursos Humanos, o usuário de rede do colaborador desligado seja imediatamente bloqueado;
XVIII. Disponibilizar aplicativo para troca de mensagens instantâneas (Microsoft Teams);
XIX. Propor as metodologias sistemas e processos específicos que visem aumentar a segurança da informação;

XX. Promover a conscientização dos colaboradores em relação a relevância da segurança da informação;

XXI. Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços;

XXII. Buscar alinhamento com as diretrizes corporativas da empresa;

XXIII. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações;

XXIV. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado ou gerado;

XXV. Realizar a monitorização da capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos da EMDEC, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); atividade de todos os colaboradores durante os acessos as redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

XXVI. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior).

XXVII. Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade.

O desrespeito a qualquer item desta Política de Segurança da Informação estará sujeitos às ações disciplinares e administrativas, além das penalidades cíveis e criminais de acordo com a legislação vigente. O acesso e utilização dos recursos de TI fica condicionado à assinatura deste documento.

Essa política poderá ser alterada em qualquer momento, seja para garantir a segurança das informações empresariais ou por evolução tecnológica.

Eu,_____, matrícula _____, *login* de rede _____, da empresa EMDEC, CNPJ 44.602.720/0001-00; declaro que li, compreendi e cumprirei todas as recomendações expressas neste documento. E, para tal, firmo as duas vias, de igual teor. A primeira via será arquivada em meu prontuário, sob os cuidados do Departamento de Recursos Humanos da empresa e a segunda, em minha posse.

_____

Assinatura do colaborador

Campinas, _____de _____ de _____