PORTARIA N° 349/2026

(Dispõe sobre a política de Tecnologia da Informação – PTI – no âmbito do SAAE de Sorocaba)

O DIRETOR GERAL do Serviço Autônomo de Água e Esgoto de Sorocaba, no uso de suas atribuições legais constantes na Lei N.º 9.895, de 28 de dezembro de 2011,

CONSIDERANDO a necessidade de normatizar a atuação do STI – Setor de Tecnologia da Informação,

CONSIDERANDO a necessidade de estabelecer diretrizes e procedimentos para o uso eficiente dos recursos de Tecnologia da Informação – TI,

CONSIDERANDO que os recursos de tecnologia da informação são ativos estratégicos que suportam processos de negócios institucionais,

CONSIDERANDO a necessidade de garantir a integridade e disponibilidade dos recursos de TI do SAAE de Sorocaba,

CONSIDERANDO a necessidade da consolidação da política de Tecnologia da Informação,

RESOLVE:

CAPÍTULO I - DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui a **Política de Tecnologia da Informação – PTI** no âmbito do Serviço Autônomo de Água e Esgoto de Sorocaba – SAAE, com o objetivo de estabelecer normas, diretrizes e responsabilidades para o uso adequado, seguro e eficiente dos ativos tecnológicos da Autarquia.

Art. 2º O SAAE de Sorocaba deverá seguir as diretrizes do PDTI - Plano Diretor de Tecnologia da Informação, gerido pela Prefeitura Municipal de Sorocaba.

Parágrafo único. O STI deverá elaborar, anualmente, e manter no âmbito da Autarquia, o Planejamento Estratégico de TI (PETI) alinhado às diretrizes estratégicas institucionais e ao PDTI.

Art. 3º Para os fins desta Portaria, consideram-se recursos de Tecnologia da Informação todos os equipamentos, sistemas e serviços utilizados no âmbito do SAAE de Sorocaba, incluindo computadores desktop e notebooks, periféricos como teclados, mouses, scanners, microfones e fones de ouvido, além dos ativos e passivos de rede (switches, roteadores, cabos e conectores), projetores, impressoras, acesso à Internet, sistemas desenvolvidos ou softwares adquiridos, serviços da rede de dados, informações armazenadas ou em trânsito na rede, o serviço de e-mail corporativo e demais dispositivos tecnológicos disponibilizados pela Autarquia.

Art. 4º A Política de Uso dos Recursos de TI tem como princípios fundamentais:

I – a **segurança da informação**, garantindo a confidencialidade, integridade e disponibilidade dos dados institucionais;

II – a **eficiência e economicidade** no uso dos recursos tecnológicos;

III – o **uso ético e responsável** dos sistemas e equipamentos;

IV – o **respeito à legislação vigente**, especialmente às normas de proteção de dados pessoais e de segurança da informação;

V – a **sustentabilidade**, por meio do uso racional dos insumos tecnológicos e de energia.

Art. 5º São **destinatários** desta Política todos os servidores, funcionários e empregados públicos, estagiários, prestadores de serviço, comissionados, contratados e demais colaboradores que utilizem, de forma direta ou indireta, qualquer recurso de TI pertencente ao SAAE de Sorocaba, doravante denominados, em conjunto, "**Usuários de TI**".

Art. 6º A aplicação e fiscalização das normas previstas nesta Portaria caberão ao **Setor de Tecnologia da Informação – STI**, que atuará como órgão gestor e orientador das práticas de uso, segurança e manutenção dos recursos tecnológicos da Autarquia.

Art. 7º As questões que ultrapassam a esfera de competência do Setor de Tecnologia da Informação devem ser encaminhadas à instância hierárquica superior imediata, seguindo o fluxo ascendente até a Diretoria Geral.

§ 1º Alterações técnicas com impacto em múltiplas unidades administrativas dependem de ciência da chefia do STI e anuência da autoridade competente na cadeia hierárquica, conforme a matéria, com registro no GLPI.

Art. 8º É de **responsabilidade de cada usuário de TI**:

I – utilizar os recursos de TI apenas para fins institucionais;

II – zelar pela segurança e integridade dos equipamentos e das informações a que tiver acesso;

III – manter sigilo sobre suas credenciais de autenticação;

IV – comunicar ao STI qualquer irregularidade, incidente de segurança, falha ou uso indevido dos sistemas ou equipamentos;

V – movimentar, realocar, desmontar e montar seus equipamentos de TI, exceto impressoras, quando houver mudança de local, salvo casos excepcionais;

VI – informar imediatamente ao remetente o recebimento de mensagens encaminhadas por equívoco, devido a endereçamento incorreto;

VII – Abrir e acompanhar seus chamados no GLPI;

VIII – observar as demais normas complementares emitidas pelo STI.

Art. 9º É de responsabilidade do STI:

I – governança de TI;

II – gerenciamento de projetos de TI;

III – análise de negócio;

IV – segurança da informação;

V – gerenciamento de infraestrutura;

VI – gestão dos serviços terceirizados de TI;

VII – manutenção e upgrade de recursos de informática.

Art. 10 Não é de **responsabilidade do STI**:

I – equipamentos eletroeletrônicos;

II – telefones fixos e móveis;

III – sistemas de telefonia em geral, incluindo, mas não se limitando a: PABX analógico, digital ou em nuvem, seja via rádio, ótico ou cabeado;

IV – sistemas de distribuição elétrica;

V – sistemas de transmissão de dados telemétricos;

VI – sistemas especializados de medição e telemetria;

VII – sistemas de arrefecimento;

VIII – sistemas de sonorização;

IX – sistemas de iluminação;

X – computadores e dispositivos de terceiros;

XI – serviços de logística;

XII – serviços de transporte;

XIII – digitação de documentos;

XIV – formatação de documentos;

XV – revisão de documentos;

XVI – impressão de documentos;

XVII – abastecimento de consumíveis em equipamentos.

CAPÍTULO II – DOS RECURSOS DE INFORMÁTICA

Seção I – Equipamentos de computação

Art. 11 Os recursos de TI se destinam, exclusivamente ao atendimento das atividades laborais e são disponibilizados aos Usuários de TI com configuração padronizada, vedada a alteração por pessoas não autorizadas.

Art. 12 É proibida a instalação de softwares nos computadores da Autarquia sem autorização do STI.

Art. 13 Os computadores laptop (notebooks) e seus acessórios requisitados junto ao STI são de guarda exclusiva de seus portadores, cabendo a estes a responsabilidade de preservação de suas condições físicas e operacionais, devendo comunicar o STI quando qualquer problema for detectado nos equipamentos e acessórios.

Art. 14 A manutenção e upgrade dos recursos de informática é de responsabilidade do STI ou a quem este delegar, sendo vedada violação de equipamentos ou manutenção por pessoas não autorizadas.

Seção II – Monitores, teclados, mouses e periféricos

Art. 15 O fornecimento e substituição de monitores, teclados, mouses e periféricos, são gerenciados pelo STI, sendo vedado o uso de dispositivos particulares, inclusive impressoras.

Art. 16 A conservação dos dispositivos citados nesta seção é de responsabilidade dos Usuários de TI.

CAPÍTULO III - DAS IMPRESSORAS E RECURSOS DE IMPRESSÃO

Art. 17 Os equipamentos de impressão destinam-se apenas para produção de documentos institucionais.

Art. 18 Não é permitida a impressão de arquivos pessoais.

Art. 19 Quando aplicável, haverá controle de utilização de cotas de impressão ou controle por grupos e Usuários de TI.

Art. 20 As impressões em equipamentos do tipo colorido devem ser utilizadas com moderação, isto quando houver a possibilidade de imprimir em equipamentos do tipo monocromáticos, de forma a evitar o uso desnecessário de recursos.

Parágrafo único. Imprimir somente em preto em um equipamento de impressão do tipo colorido não reduz o custo por página, que é cobrado pelo tipo do equipamento não pela quantidade de cores utilizada.

Art. 21 Cabe a cada usuário a preservação do sigilo em suas impressões, evitando esquecer seus trabalhos na bandeja de saída exposto aos demais Usuários de TI.

Art. 22 Todas as falhas dos equipamentos de impressão devem ser reportadas ao STI, para acionamento da manutenção da empresa contratada, quando aplicável.

Art. 23 Os Usuários de TI devem solicitar a reposição de insumos como toner ou tintas ao STI, quando for aplicável.

Parágrafo único. A substituição de insumos será realizada automaticamente pela empresa de outsourcing contratada antes destes acabarem, quando houver esta previsão no contrato ou, em último caso, pelos Usuários de TI sob orientação do STI.

Art. 24 Para reportar ao STI quaisquer incidentes com os equipamentos de impressão ou fazer a solicitação de insumos, quando aplicável, é necessário informar o código de identificação do equipamento, sua localização e telefone de contato do solicitante.

CAPÍTULO IV - DA REDE COMPUTADORES E DA INTERNET

Seção I – Credenciais de rede

Art. 25 É permitido o acesso à rede de computadores e Internet mediante identificação e autenticação da conta do usuário, por senha pessoal e intransferível, que são chamadas de **credenciais**.

Art. 26 É proibido o compartilhamento de credenciais de rede.

§ 1º Suspeitas de comprometimento deverão ser imediatamente comunicadas ao STI e à chefia, com abertura de chamado no GLPI para bloqueio/prevenção e troca da senha.

Art. 27 A nomenclatura padrão para criação de contas de usuário de rede seguirá o seguinte formato: **primeira letra do prenome + ponto + último sobrenome.**

§ 1º Havendo coincidência de nomes de conta, serão adicionadas outras letras do prenome ou sobrenome.

§ 2º As contas legadas que não seguem a nomenclatura do *caput* deste art. serão mantidas inalteradas.

§ 3º As contas resultantes da aplicação do estabelecido no *caput* e § 1º deste art. que causem constrangimento ou que sejam vexatórias, serão analisadas e modificadas pelo STI.

Art. 28 As senhas de autenticação da rede e Internet seguirão os seguintes requisitos:

I – comprimento mínimo de 8 (oito) caracteres;

II – no mínimo 1 (uma) letra maiúscula;

III – no mínimo 1 (um) número;

IV – no mínimo 1 (um) caractere especial: (# ! @ *);

V – letras minúsculas.

Art. 29 A alteração da senha da rede respeitará o intervalo de 90 (noventa) dias ou a critério do STI.

Art. 30 A alteração de senha da rede, terá reflexos em todos os sistemas que utilizam este mesmo usuário e senha para autenticação de acesso.

Art. 31 É vedado, quando da alteração de senha, o uso das 6 (seis) últimas senhas já utilizadas.

Art. 32 A conta da rede será bloqueada provisoriamente durante 5 (cinco) minutos, quando ocorrerem 5 (cinco) tentativas fracassadas de digitação da senha, sendo a conta desbloqueada automaticamente para nova tentativa após a expiração desse prazo.

Seção II – Níveis de privilégio e acesso à rede

Art. 33 Cada usuário de TI terá um perfil com nível de acesso aos recursos de rede que incluem:

I – pastas compartilhadas;

II – impressoras.

Art. 34 Na posse de um novo usuário de TI, é de responsabilidade da chefia imediata/mediata solicitar ao STI a criação de usuários de rede, informando um perfil modelo de um usuário já existente ou definindo expressamente quais recursos serão permitidos ao novo usuário.

Art. 35 Na remoção de um usuário de TI, é de responsabilidade da chefia imediata/mediata do setor de origem, solicitar ao STI a exclusão dos perfis de rede dos Usuários de TI que deixarem de estar lotados naquela unidade.

Art. 36 Na remoção de um usuário de TI, é de responsabilidade da chefia imediata/mediata do setor de destino, solicitar ao STI modificação do usuário que está

ingressando na unidade informando um perfil modelo de um usuário já existente ou definindo expressamente quais recursos serão permitidos ao servidor naquela unidade.

Art. 37 No afastamento de usuário de TI é de responsabilidade da chefia imediata/mediata, solicitar ao STI o bloqueio de sua credencial de rede.

Art. 38 No retorno de afastamento de um usuário de TI é de responsabilidade da chefia imediata/mediata, solicitar ao STI o desbloqueio de sua credencial de rede e correio eletrônico (e-mail).

Art. 39 Na exoneração/desligamento de um usuário de TI é de responsabilidade da chefia imediata/mediata, solicitar ao STI o bloqueio da credencial de rede do usuário.

Art. 40 É de responsabilidade da chefia imediata/mediata a revisão periódica dos níveis de acesso de todos os seus liderados, solicitando ao STI as informações de acesso e requisitando as eventuais readequações dos perfis de Usuários de TI.

Seção III – Níveis de privilégio e acesso à Internet

Art. 41 Na posse de um novo usuário de TI, é de responsabilidade da chefia imediata/mediata solicitar ao STI a atribuição de perfil de acesso à Internet com base em um perfil de usuário modelo preexistente ou especificando quais acessos são necessários.

Art. 42 Na remoção de um usuário de TI, é de responsabilidade da chefia imediata/mediata do setor de origem, solicitar ao STI a exclusão dos perfis de acesso à Internet daqueles Usuários de TI que deixarem de estar lotados naquela unidade.

Art. 43 Na remoção de um usuário de TI, é de responsabilidade da chefia imediata/mediata do setor de destino, solicitar ao STI modificação do perfil de acesso à Internet com base em um perfil de usuário modelo pré-existente ou especificando quais acessos são necessários.

Art. 44 Devem ser obedecidos os princípios da legalidade e moralidade para o uso da Internet, sendo vedado:

§ 1º Utilizar os serviços para fins comerciais e políticos, ou como instrumento de ameaça, calúnia, injúria ou difamação;

§ 2º Transmitir ou acessar conteúdo que comprometa a integridade ou a disponibilidade dos recursos de TI;

§ 3º Transmitir ou acessar conteúdo lascivo, preconceituoso, ilegal ou qualquer outro que atente contra a honra, a moral e os bons costumes, exceto por necessidade de trabalho, quando o acesso for expressamente autorizado pela chefia em conjunto com o STI;

§ 4º Utilizar serviços não autorizados de compartilhamento de arquivos ou similares, exceto se permitido expressamente pela chefia em conjunto com o STI;

§ 5º Acessar sítios de relacionamento e serviços de mensagens instantâneas não autorizados, exceto quando a necessidade do serviço o determinar, hipótese que deverá ser expressamente autorizada pela chefia em conjunto com o STI.

Art. 45 O acesso à Internet dos Usuários de TI será objeto de monitoramento com o propósito de prevenir o uso excessivo de banda de rede e poderá resultar na limitação e, em último caso, na suspensão de acesso a determinados sites/serviços, com ciência da chefia quando houver impacto continuado.

Art. 46 O STI reserva-se o direito de bloquear previamente endereços de Internet reconhecidos como propagadores de spam, phishing, fraudes ou malwares para preservar a infraestrutura da Autarquia.

Art. 47 Os endereços de Internet que eventualmente estejam bloqueados e que, por força da atividade laboral, necessitem ser liberados, é necessário acionar o STI mediante GLPI, informando as URLs (endereço do site) e a justificativa funcional; a liberação será temporária e registrada no chamado, sendo bloqueados novamente após o uso.

Art. 48 A banda de Internet disponibilizada pela Autarquia será priorizada para acessos dos serviços essenciais à continuidade de negócio, sendo facultado ao STI a redução temporária de banda dos serviços menos críticos, em casos de consumo excessivo de banda.

Art. 49 Todos os endereços de Internet acessados pelos Usuários de TI ficam registrados em arquivos de *log*, para auditoria.

CAPÍTULO V – DO CORREIO ELETRÔNICO (E-MAIL)

Seção I – Contas de e-mail

Art. 50 É permitido o acesso ao serviço de e-mail mediante identificação e autenticação da conta do usuário, por senha pessoal e intransferível, que são chamadas de **credenciais**.

Art. 51 É proibido o compartilhamento de credenciais de e-mail.

§ 1º Suspeitas de comprometimento deverão ser imediatamente comunicadas ao STI e à chefia, com abertura de chamado no GLPI para bloqueio/prevenção e troca da senha.

Art. 52 A nomenclatura padrão para criação de contas de e-mail seguirá o seguinte formato: **primeiro prenome + ponto + último sobrenome**.

§ 1º Havendo coincidência de nomes de conta, serão adicionadas outras letras do prenome ou sobrenome.

§ 2º As contas legadas que não seguem a nomenclatura do *caput* deste art. terão mantidas inalteradas.

§ 3º As contas resultantes da aplicação do estabelecido no *caput* e § 1º deste art. que causem constrangimento ou que sejam vexatórios, serão analisadas e modificadas pelo STI.

Art. 53 As senhas de autenticação de e-mail seguirão os seguintes requisitos:

I – comprimento mínimo de 10 (dez) caracteres;

II – no mínimo 1 (uma) letra maiúscula;

III – no mínimo 1 (um) número;

IV – no mínimo 1 (um) caractere especial: (# ! @ *);

V – letras minúsculas.

Art. 54 Na posse de um novo usuário de TI, é de responsabilidade da chefia imediata/mediata solicitar ao STI a criação de usuários e-mail, caso seja aplicável.

Art. 55 No afastamento de um usuário de TI é de responsabilidade da chefia imediata/mediata, solicitar ao STI o bloqueio de sua credencial de e-mail, caso o usuário possua uma.

Art. 56 No retorno de afastamento de um usuário de TI é de responsabilidade da chefia imediata/mediata, solicitar ao STI o desbloqueio de seu credencial e-mail, caso o usuário possua uma.

Art. 57 Na exoneração/desligamento de um usuário de TI, é de responsabilidade da chefia imediata/mediata, solicitar ao STI o bloqueio da credencial de e-mail, caso o usuário possua uma.

Art. 58 As credenciais de e-mail e os dados ligados a ela daqueles Usuários de TI exonerados serão excluídas em, no máximo, 30 (trinta) dias após a notificação oficial publicada na Imprensa Oficial do Município ou pela informação do Departamento de Recursos Humanos.

§ 1º Quando necessário à continuidade do serviço, a chefia imediata poderá solicitar, por ato formal e com registro no GLPI, medidas transitórias (p. ex., acesso institucional à caixa postal ou resposta automática), limitadas ao mínimo necessário e pelo prazo estritamente indispensável.

§ 2º Findo o prazo e cumpridas as obrigações administrativas, proceder-se-á à exclusão definitiva da conta, preservados os registros conforme a política de backup e de segurança da informação.

Seção II – Uso do e-mail

Art. 59 Fica definido como padrão de assinaturas de e-mail, o modelo abaixo, em formato de texto, isento de imagens e outros elementos gráficos:

Nome
Departamento/Setor
Cargo

Serviço Autônomo de Água e Esgoto de Sorocaba

Endereço:
Bairro:
CEP: xxxxx-xxx – Sorocaba – SP
Telefone: (15) xxxx-xxxx
www.saaesorocaba.com.br

§ 1.º Os elementos padronizados a serem utilizados são:

I – fonte Arial ou Calibri;

II – tamanho 11;

III – cor preto, azul ou cinza;

IV – fonte em negrito;

Art. 60 O STI não dará suporte à criação e manutenção de assinaturas de e-mail que não sigam o estabelecido no art. anterior, sendo permitido o uso de imagens, mas sua criação e manutenção será de responsabilidade do usuário.

Parágrafo único. As mensagens enviadas com assinaturas em formato de imagem podem sofrer bloqueios nos sistemas de segurança e servidores de e-mail dos destinatários,

apagando as imagens da assinatura, deixando um espaço vazio na mensagem e impedindo que o destinatário tenha os dados de contato do remetente.

Art. 61 O serviço de e-mail institucional destina-se exclusivamente às comunicações de trabalho relacionadas às atividades da Autarquia.

Art. 62 É vedado o uso para fins particulares, recreativos, políticos ou alheios ao interesse público.

Art. 63 É proibido utilizar o e-mail institucional para:

I – encaminhar correntes, mensagens em massa não solicitadas ou de teor promocional/propagandístico;

II – enviar anexos pessoais alheios ao serviço;

III – transmitir conteúdo ofensivo, discriminatório, ilícito, difamatório ou que atente contra a honra, a moral e os bons costumes;

IV – distribuir materiais que violem direitos autorais ou licenças de uso;

V – compartilhar arquivos que comprometam a segurança da informação (ex.: executáveis, scripts ou formatos de alto risco), salvo autorização da chefia em conjunto com o STI e registro no GLPI.

Seção III – Retenção de mensagens de e-mail e restauração

Art. 64 O tempo de retenção das mensagens em backup é de, no máximo, 7 (sete) dias.

§ 1º Não há garantia de restauração de mensagens além do período e das condições previstas na política de backup.

§ 2º Pedidos de restauração deverão ser formalizados via GLPI.

§ 3º Mensagens armazenadas localmente pelo usuário não integram a política de backup, aplicando-se, no que couber, as regras gerais desta Portaria.

§ 4º O prazo de retenção de 7 (sete) dias para a de e-mail decorre de cláusula contratual vigente do serviço terceirizado de correio eletrônico e de backup, observada a economicidade e as limitações técnicas do fornecedor.

§ 5º Alterações contratuais supervenientes que ampliem ou reduzam a janela de retenção poderão ser implementadas por ato do STI, com comunicação à Diretoria e atualização do presente normativo.

Art. 65 Os prazos técnicos de retenção de e-mails e backups não afastam a obrigação legal de preservação de registros quando houver:

I – determinação judicial;

II – processo administrativo em curso;

III – investigação ou auditoria;

IV – requisição de autoridade competente.

Parágrafo único. Nesses casos, caberá ao STI adotar medidas extraordinárias para preservação dos registros necessários.

CAPÍTULO VI - DO HELP DESK (SUPORTE TÉCNICO)

Seção I – Níveis de atendimento

Art. 66 Ficam instituídos 2 (dois) níveis de atendimento técnico no STI.

§ 1º O primeiro nível atenderá aos chamados técnicos de baixa complexidade e é composto por:

I – estagiários;

II – técnicos de informática.

§ 2º O segundo nível atenderá aos chamados técnicos de maior complexidade e cuidará das rotinas administrativas do STI e é composto por:

I – analistas de sistemas;

II – chefia do STI.

Art. 67 Toda solicitação de serviço técnico **será direcionada ao primeiro nível de atendimento do STI.**

Seção II – Sistema de controle de chamados

Art. 68 Fica instituído o sistema de help desk GLPI – Gestor Livre de Parque de Informática – como plataforma centralizada na rede local para gerenciamento de chamados técnicos, reservas para empréstimo de itens de TI e comunicação entre as partes envolvidas nos chamados.

Art. 69 Toda solicitação técnica, de qualquer tipo, deverá ser realizada pela plataforma no endereço Web **http://glpi.saae.local** a partir de qualquer navegador de Internet.

Art. 70 O acesso ao sistema GLPI usará o mesmo nome de usuário e senha da rede, observando o que estabelecem os arts. 28 e 30.

Art. 71 Não havendo possibilidade de abertura de chamado técnico pelo sistema GLPI devido à limitação de recurso computacional ou de conectividade por parte do requisitante, a solicitação pode ser feita por telefone ou e-mail.

Art. 72 Toda a comunicação entre os envolvidos no atendimento será registrada somente pelo sistema GLPI, que notificará todos os envolvidos pela plataforma.

Art. 73 Os chamados terão um número de identificação que será gerado para o requisitante no momento da abertura no sistema, para acompanhamento.

Art. 74 Os chamados serão atendidos de acordo com a ordem de chegada e priorizados conforme o tipo de solicitação.

Art. 75 É de responsabilidade de cada usuário acompanhar seus chamados criados no GLPI.

Seção III – Escopo de atuação

Art. 76 O STI não atenderá chamados que envolvam tarefas administrativas componentes da súmula de atribuições de cargos diferentes dos técnicos e analistas de sistemas, limitando-se a esclarecer o uso de sistemas e ferramentas.

Art. 77 O STI não fornecerá treinamento em quaisquer softwares de terceiros instalados nos equipamentos de TI, limitando-se a orientar o usuário a pesquisar junto ao fornecedor do software ou Internet sobre as funcionalidades e procedimentos de uso.

Art. 78 Não é de responsabilidade do STI a reserva de salas de reunião ou auditórios, além de não prestar atendimento aos itens elencados no art. 10.

Seção IV – Acesso remoto

Art. 79 O acesso remoto às estações de trabalho poderá ser realizado exclusivamente pelo STI para fins de suporte técnico, manutenção, resposta a incidentes e auditoria, mediante registro prévio no GLPI e anuência do usuário/chefia sempre que operacionalmente possível.

§ 1º O acesso remoto restringe-se ao mínimo necessário, com registro da intervenção no chamado.

§ 2º. Fica diferida a exigibilidade de procedimentos automatizados de consentimento e de gravação de sessão até a disponibilização de ferramenta apropriada, a ser regulamentada em ato complementar do STI.

Seção V – Reserva de itens de TI

Art. 80 Serão disponibilizados, para reserva, os seguintes itens:

I – notebooks;

II – projetor de imagem;

III – drive de leitor/gravador de DVD.

Art. 81 Os itens do art. anterior podem sofrer adições ou supressões em função da disponibilidade.

Art. 82 É de responsabilidade do usuário requisitante acessar o sistema GLPI, entrar na página de Reservas e efetuar a reserva na data e horário desejados.

Art. 83 É de responsabilidade do usuário requisitante a retirada dos itens de TI reservados, bem como sua devolução, quando finalizar o período de empréstimo.

Art. 84 Quando da devolução, todos os arquivos gravados e manipulados nos equipamentos, inclusive as mídias removíveis precisam ser retiradas.

Art. 85 Caso haja necessidade de apoio técnico para montagem dos itens de TI, será necessário também que o usuário requisitante faça a abertura de chamado técnico à parte da reserva, informando previamente o horário e local de montagem.

Art. 86 É de responsabilidade do usuário organizador de eventos obter antecipadamente, de seus convidados e preletores, informações sobre quais recursos e configurações serão necessários para a realização de seus trabalhos, para a reserva de itens de TI e solicitação de apoio técnico.

Seção VI – Prazos

Art. 87 Para o disposto nesta Portaria, considera-se:

I – tempo de atendimento: é definido a partir da hora da abertura do chamado técnico no GLPI até a sua atribuição a um técnico ou analista responsável pela intervenção.

II – tempo de solução: é o período compreendido entre o horário de atribuição do chamado técnico até a solução final do problema.

a) entende-se por "solução do problema" a identificação e adoção de medidas corretivas e efetivas que foram implementadas para sanar o problema que resultou na abertura do chamado.

Art. 88 O tempo de atendimento dos chamados técnicos abertos no GLPI será de até 2 (duas) horas.

Art. 89 Os chamados técnicos requisitando a criação, alteração de perfil de acesso, ou qualquer atividade de manutenção de perfis de Usuários de TI e grupos da rede corporativa e e-mail terão tempo de solução de até 3 (três) dias úteis após a atribuição do chamado a um responsável.

Art. 90 Fica definido que o status **Pendente** de um chamado é quando o corpo técnico está aguardando manifestação do requerente para prestar algum esclarecimento ou aguardando uma validação da chefia sobre o prosseguimento do atendimento.

§ 1º O prazo máximo para um chamado permanecer com status Pendente é de 5 (cinco) dias, sendo fechado após a expiração deste prazo.

CAPÍTULO VII – DOS SISTEMAS CORPORATIVOS E DADOS

Seção I – Sistemas

Art. 91 Para os fins desta Portaria, os dados armazenados nos ambientes gerenciados pelo STI -- incluindo servidores de arquivos de rede, sistemas de correio eletrônico e registros de log — classificam-se em duas categorias distintas, sujeitas a regimes jurídicos diferentes:

I — dados de infraestrutura de TI: informações produzidas e armazenadas nos ambientes tecnológicos da Autarquia com finalidade operacional, técnica ou de suporte à atividade laboral, que não constituem, por si sós, documentos oficiais da Administração Pública, compreendendo, entre outros, arquivos de trabalho em elaboração, rascunhos,

duplicatas de arquivos, e-mails de comunicação interna de natureza operacional, registros temporários e logs de acesso a sistemas e à Internet;

II — documentos oficiais: aqueles que, independentemente do suporte ou meio em que foram produzidos, registram atos administrativos, decisões, ordens de serviço, comunicações funcionais formalizadas, contratos, licitações, registros de pessoal e demais manifestações com valor jurídico, administrativo, probatório ou histórico para a Autarquia, os quais são necessariamente formalizados e custodiados nos sistemas oficiais de gestão documental do SAAE, em especial o SEI — Sistema Eletrônico de Informações, gerenciado pelo Setor de Protocolo Geral e Gestão Documental, ou em processo físico autuado.

Art. 92 Os dados de infraestrutura de TI referidos no inciso I do artigo anterior são regidos exclusivamente pelas políticas técnicas e operacionais estabelecidas nesta Portaria, sujeitando-se aos prazos de retenção e às regras de backup e descarte nela previstos, sem aplicação da Tabela de Temporalidade de Documentos do Arquivo Público e Histórico Municipal de Sorocaba.

Parágrafo único. A Tabela de Temporalidade de Documentos, instituída pelo Decreto Municipal nº 22.419/2016, é instrumento de gestão documental que rege os documentos oficiais da Administração Pública Municipal, sendo de competência exclusiva do Setor de Protocolo Geral e Gestão Documental sua aplicação e fiscalização.

Art. 93 É responsabilidade do Usuário de TI garantir que todo ato ou comunicação com caráter de documento oficial seja formalizado e autuado nos sistemas de gestão documental competentes, em especial o SEI, não cabendo ao STI a guarda ou preservação de documentos oficiais por meio dos sistemas de backup de infraestrutura.

§ 1º O STI não responde pela perda, destruição ou indisponibilidade de documentos oficiais que, em descumprimento ao disposto neste artigo, tenham sido mantidos exclusivamente em áreas de rede, caixas postais de e-mail ou dispositivos locais sujeitos às janelas de retenção de infraestrutura estabelecidas nesta Portaria.

§ 2º A responsabilidade pela correta classificação e destinação dos documentos produzidos no âmbito das atividades de cada unidade administrativa é do servidor que os produziu e de sua chefia imediata.

Art. 94 Para fins de clareza operacional, presume-se que constituem dados de infraestrutura, sem caráter de documento oficial, os seguintes tipos de conteúdo armazenados nos ambientes de TI:

I — arquivos em elaboração ou em versão intermediária, que ainda não foram formalizados por ato administrativo competente;

II — e-mails de comunicação operacional cotidiana que não registrem decisões administrativas, ordens de serviço ou comunicações funcionais formalizadas;

III — duplicatas, cópias de trabalho e versões provisórias de documentos já autuados no SEI ou em processo físico;

IV — arquivos de log, registros de acesso e demais metadados de infraestrutura de rede;

V — arquivos temporários gerados automaticamente pelos sistemas operacionais ou aplicativos.

Art. 95 Em caso de dúvida quanto à classificação de determinado conteúdo como dado de infraestrutura ou documento oficial, o Usuário de TI deverá consultar o Setor de Protocolo Geral e Gestão Documental, adotando, por precaução, o tratamento mais conservador, que é o de formalizá-lo no SEI antes da expiração da janela de retenção aplicável.

Art. 96 Todos os acessos aos sistemas existentes na Autarquia possuem como base perfis de uso de acordo com as peculiaridades de cada atividade funcional, que é determinada pela chefia imediata/mediata onde o usuário estiver lotado.

Art. 97 É proibido o uso de sistemas para fins pessoais ou sem vínculo funcional.

Art. 98 O STI não é responsável por criar credenciais de acesso para os sistemas:

I – SEI – Sistema Eletrônico de Informações, que é gerenciado diretamente pelo Setor de Protocolo geral e Gestão Documental;

II – VPN do Conam, que é gerenciado pela Prefeitura Municipal de Sorocaba, com mediação do STI, através de solicitação pelo GLPI;

III - Conam SIAP, SIAM e SIAF, que são gerenciados diretamente pelos usuários *master* de cada módulo, que são: chefe imediato do Departamento de Recursos Humanos, Administração de Materiais e Departamento Financeiro, respectivamente.

Art. 99 A gestão de conteúdo e notícias do site institucional é de responsabilidade da Assessoria de Comunicação, ao STI compete a infraestrutura e a arquitetura técnica do site (incluídas manutenções estruturais e técnicas).

§ 1º Ao STI cabe prover e manter a infraestrutura técnica (hospedagem, DNS, certificados, integrações), conforme demanda formalizada via GLPI.

§ 2º No caso de terceirização do site institucional, caberá à contratada a gestão total da solução, com apoio técnico do STI.

§ 3º Demandas de publicação/revisão editorial deverão ser formalizadas à unidade competente, sem prejuízo do suporte técnico do STI.

Seção II – Credenciais e sigilo

Art. 100 As credenciais de acesso aos sistemas, contas de rede e e-mails institucionais são pessoais, intransferíveis e de uso exclusivo do titular, sendo vedado o compartilhamento com terceiros sob qualquer pretexto.

Art. 101 Todas as informações e dados institucionais produzidos, armazenados ou processados nos sistemas e equipamentos do SAAE de Sorocaba são de propriedade exclusiva da Autarquia e devem ser tratados com observância dos princípios de confidencialidade, integridade e disponibilidade.

Art. 102 É dever de todos os Usuários de TI preservar o sigilo das informações a que tiverem acesso em razão do exercício de suas funções, sendo vedada a sua reprodução, divulgação, transmissão ou compartilhamento sem autorização expressa da chefia imediata ou do Setor de Tecnologia da Informação – STI.

Art. 103 O acesso às informações institucionais deve ocorrer apenas por meio de sistemas, plataformas e dispositivos oficialmente autorizados, sendo proibido o armazenamento de dados da Autarquia em mídias externas, dispositivos pessoais ou serviços de nuvem não homologados pelo STI.

Art. 104 A manipulação, consulta ou extração de dados institucionais somente poderá ocorrer para fins de interesse público ou necessidade de serviço, devendo ser observadas as normas internas e a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018).

Art. 105 É expressamente proibida a utilização de informações sigilosas do SAAE para fins pessoais, políticos, comerciais ou qualquer outro que não se relacione diretamente às atividades institucionais.

Art. 106 Qualquer incidente de segurança da informação, suspeita de vazamento de dados, acesso indevido ou perda de confidencialidade deverá ser comunicado imediatamente ao STI, que registrará o evento e adotará as medidas técnicas e administrativas cabíveis.

Art. 107 O descumprimento das normas previstas neste Capítulo sujeitará o infrator às sanções disciplinares previstas na legislação aplicável, sem prejuízo da responsabilidade civil e penal.

Art. 108 Todos os Usuários de TI têm o dever de comunicar imediatamente ao STI qualquer ocorrência que envolva falhas, erros, comportamentos anômalos, perda de desempenho, suspeita de infecção por código malicioso ou qualquer outra anormalidade identificada nos sistemas, equipamentos ou serviços de rede.

Art. 109 O usuário deverá reportar também qualquer tentativa, acesso indevido ou suspeito a sistemas, arquivos, pastas compartilhadas, contas de e-mail ou dispositivos de armazenamento de dados pertencentes à Autarquia.

Art. 110 O reporte de incidentes ou irregularidades deverá ser realizado preferencialmente por meio do sistema de chamados técnicos oficial (GLPI), descrevendo o ocorrido com o maior nível de detalhamento possível, incluindo data, hora aproximada e sintomas observados.

Art. 111 Nos casos em que o sistema de chamados não estiver disponível, o reporte poderá ser feito por e-mail institucional ou contato telefônico direto com o STI, que registrará a ocorrência posteriormente na plataforma oficial.

Art. 112 É dever do STI registrar, analisar e tratar todas as ocorrências comunicadas, adotando medidas corretivas, preventivas e, quando necessário, comunicando formalmente à chefia do departamento envolvido e ao Coordenador de Proteção de Dados (CPD) do SAAE.

Art. 113 A comunicação de falhas ou irregularidades feita de boa-fé não constituirá infração, sendo incentivada como prática de segurança colaborativa e de prevenção de danos à infraestrutura tecnológica do SAAE.

Seção IV – Armazenamento de dados

Art. 114 O serviço de armazenamento dos Servidores de Arquivos da rede dispõe de cota limitada e compartilhada de espaço, com acesso exclusivo aos Usuários de TI de setores e departamentos autorizados pela chefia imediata/mediata.

§ 1º É vedado o compartilhamento de pastas ou outros recursos dos computadores locais com outros Usuários de TI da rede, salvo com anuência expressa do STI.

Art. 115 As cotas de disco dos setores e departamentos são gerenciadas pelo STI, mediante solicitação de reajuste de valor via GLPI.

Art. 116 É de responsabilidade dos Usuários de TI evitar a duplicidade de arquivos e pastas para não consumir espaço de cota de disco de maneira desnecessária.

§ 1º Antes de solicitar o aumento de cota de disco pelo GLPI é de responsabilidade do solicitante apurar e eliminar as duplicidades de arquivos e pastas, situação em que o STI pode fornecer, a pedido, relatórios com as localizações destas ocorrências para tratamento pelo solicitante.

Art. 117 Os arquivos de trabalho devem ser armazenados na estrutura de diretórios dos servidores de rede, pois fazem parte da política de backup.

Art. 118 É vedado o armazenamento na rede ou localmente de arquivos protegidos por direitos autorais, excetuadas obras legalmente adquiridas mediante comprovação de licença válida, desde que restritas ao ambiente interno da organização e ao propósito profissional específico.

Art. 119 Não é permitido armazenar na rede, localmente ou em mídias externas de propriedade da Autarquia arquivos pirateados de softwares, documentos, músicas, vídeos e ou outros formatos de origem ilegal.

Art. 120 Os arquivos armazenados na rede corporativa do SAAE deverão observar o limite máximo de **255 caracteres** para o caminho completo (path), incluindo nome do arquivo, pastas, subpastas, unidade de rede e extensão.

§ 1º O excesso do limite de caracteres poderá impedir a gravação, cópia ou exclusão de arquivos, bem como comprometer o funcionamento dos sistemas de backup e replicação de dados.

§ 2º Para evitar tais ocorrências, recomenda-se que os Usuários de TI utilizem nomes de pastas e arquivos curtos, objetivos e padronizados, preferencialmente sem acentuação, espaços duplos ou caracteres especiais (* / : ? " < > |).

§ 3º Caso o STI identifique diretórios que ultrapassem o limite previsto neste artigo, poderá renomeá-los ou realocá-los, mediante comunicação à chefia do setor responsável.

CAPÍTULO VIII – DA SEGURANÇA DA INFORMAÇÃO

Art. 121 A Segurança da Informação no âmbito do SAAE de Sorocaba tem por finalidade proteger os ativos de informação contra acessos não autorizados, alterações indevidas, perdas ou destruição, assegurando a continuidade dos serviços institucionais.

Art. 122 São princípios fundamentais da Segurança da Informação:

I – Confidencialidade, assegurando que a informação seja acessível apenas por pessoas devidamente autorizadas;

II – Integridade, garantindo que a informação mantenha sua exatidão e completude, não sendo alterada de forma indevida;

III – Disponibilidade, assegurando que a informação esteja acessível e utilizável sempre que necessário pelos Usuários de TI autorizados.

Art. 123 É obrigatório o uso de software antivírus corporativo atualizado em todos os equipamentos de informática da Autarquia, bem como a ativação de atualizações automáticas do sistema operacional e dos aplicativos instalados.

§ 1º A desativação de antivírus, firewall ou serviços de atualização automática somente poderá ocorrer mediante autorização expressa do STI.

§ 2º O STI deverá garantir a manutenção e atualização contínua das ferramentas de proteção e segurança instaladas.

Art. 124 Todos os computadores e notebooks deverão possuir mecanismo de bloqueio automático de tela após período máximo de 15 (quinze) minutos de inatividade.

§ 1º A exceção do bloqueio automático de tela se dará aos computadores da telemetria do sistema de abastecimento e esgoto e aos sistemas de chamada de senha no Setor de Atendimento.

§ 2º O usuário deve bloquear manualmente sua estação de trabalho ao se ausentar do local, ainda que por curtos períodos.

§ 3º O desbloqueio somente poderá ser realizado pelo titular da credencial de acesso, sendo vedado o uso por terceiros.

Art. 125 É vedado o armazenamento, tratamento ou compartilhamento de dados pessoais sensíveis, nos termos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), fora dos sistemas oficiais da Autarquia.

Parágrafo único. Consideram-se dados pessoais sensíveis, entre outros, os que revelem origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Art. 126 As mídias de armazenamento, como discos rígidos, DVDs, CDs, pendrives, SSDs ou fitas magnéticas, que contenham informações institucionais, deverão ser descartadas de forma segura, mediante procedimentos de exclusão permanente, inutilização física ou destruição controlada.

§ 1º. O descarte deverá ser executado sob supervisão do STI ou por empresa contratada especificamente para essa finalidade, mediante registro do procedimento realizado.

§ 2º. É vedada a doação, reutilização ou descarte de mídias sem a prévia eliminação total dos dados nelas contidos.

§ 3º. A eliminação lógica dos dados deverá ocorrer por meio de ferramentas de sobrescrita múltipla ou métodos equivalentes, que impeçam a recuperação da informação.

CAPÍTULO IX – DOS DISPOSITIVOS MÓVEIS

Art. 127 O uso de celulares particulares durante o expediente e em áreas operacionais não é regulamentado por esta Portaria, devendo seguir orientações específicas que vierem a ser estabelecidas por ato próprio da Direção do SAAE.

CAPÍTULO X – DOS SOFTWARES E LICENCIAMENTO

Art. 128 Todos os softwares instalados nos equipamentos de informática do SAAE de Sorocaba deverão possuir licença válida de uso corporativo, em conformidade com a legislação vigente sobre direitos autorais e propriedade intelectual.

Art. 129 É vedada a instalação, cópia, reprodução, compartilhamento ou distribuição de softwares sem a devida autorização do STI, ainda que se trate de programas gratuitos, trial ou de código aberto.

§ 1º A autorização de instalação de qualquer software deverá ser formalmente registrada em chamado técnico no sistema oficial de atendimento (GLPI).

§ 2º Softwares sem comprovação de licenciamento, instalados sem consentimento do STI, poderão ser removidos automaticamente, mediante comunicação à chefia do setor responsável.

Art. 130 O controle das licenças de uso dos softwares corporativos, incluindo suas chaves, certificados digitais e prazos de validade, será de responsabilidade exclusiva do STI, que manterá inventário atualizado em sistema próprio.

§ 1º O STI deverá assegurar que as licenças adquiridas estejam de acordo com as quantidades contratadas e com os contratos de manutenção vigentes.

§ 2º O inventário de softwares deverá conter, no mínimo, o nome do software, versão, número de licenças, titularidade, fornecedor e setor de utilização.

Art. 131 O STI realizará auditorias periódicas de licenciamento de softwares, com o objetivo de verificar a conformidade entre as licenças adquiridas e as instalações efetivamente existentes nos equipamentos da Autarquia.

§ 1º As auditorias poderão abranger servidores, estações de trabalho e notebooks, inclusive os alocados em unidades externas.

§ 2º Os resultados das auditorias deverão ser formalizados em relatório técnico e encaminhados à Diretoria Administrativa e à Controladoria Interna.

Art. 132 O Usuário de TI que realizar instalação, cópia ou distribuição de software não autorizado ou sem licença válida responderá pelas consequências legais e administrativas decorrentes, sem prejuízo das sanções previstas nesta Portaria e demais normas aplicáveis.

CAPÍTULO XI – DO BACKUP E RECUPERAÇÃO

Art. 133 A cópia de segurança (backup) de todos os arquivos armazenados nos servidores da rede corporativa será realizada de segunda a sexta-feira, no período noturno.

Parágrafo único. O cronograma de backup estabelecido no caput pode sofrer alterações em função da disponibilidade tecnológica vigente.

Art. 134 A cópia de segurança dos arquivos armazenados no disco rígido dos computadores desktop, notebooks, pendrives ou HDs externos é de responsabilidade do próprio usuário, pois não fazem parte da política de backup.

Parágrafo único. No caso de falha do dispositivo de armazenamento local, o STI direcionará todos os esforços para a tentativa de recuperação dos dados eventualmente perdidos, mas não pode garantir que os dados sejam extraídos e que estejam íntegros.

Art. 135 A restauração de cópia de segurança de arquivos armazenados nos servidores de rede pode ser solicitada pela chefia imediata/mediata via GLPI, que deverá informar

a data mais próxima da versão desejada do arquivo, o caminho de gravação e o nome completo do arquivo.

§ 1º Na impossibilidade de indicação do caminho completo pelo usuário, o STI poderá realizar busca limitada por nome do arquivo e/ou pasta de trabalho dentro do escopo do setor do solicitante, condicionada à anuência da chefia e registro do chamado no GLPI, sem garantia de êxito.

Art. 136 O tempo máximo de retenção das cópias de segurança é de 20 (vinte) dias.

Parágrafo único. O prazo máximo de 20 (vinte) dias observa a capacidade instalada do ambiente de backup em fitas LTO-5 disponível no SAAE, sendo compatível com o parque de mídias e a política de rotação vigente.

CAPÍTULO XII – DA CAPACITAÇÃO E CONSCIENTIZAÇÃO

Art. 137 O STI deverá realizar, de forma periódica, a divulgação de cartilhas, informativos e alertas de segurança, especialmente em ocasiões de aumento de incidentes ou vulnerabilidades conhecidas.

§ 1º Os materiais de conscientização deverão ser elaborados em linguagem clara, objetiva e acessível, visando à compreensão por todos os públicos da Autarquia.

§ 2º O envio de comunicados, cartilhas e alertas deverá ser feito prioritariamente por e-mail institucional ou publicação na intranet, caso seja aplicável, sob responsabilidade do STI.

CAPÍTULO XIII – DOS PROJETOS DE CONSTRUÇÃO, REFORMA E AMPLIAÇÃO

Art. 138 Os projetos de obras de engenharia envolvendo os próprios da Autarquia deverão prever a infraestrutura necessária para a conexão de computadores e

dispositivos de rede e deverão contar com a participação formal de, no mínimo, um analista de sistemas do STI.

§ 1º São considerados projetos, entre outros:

I – novas edificações;

II – reformas;

III – ampliações;

IV – modificações prediais;

V – alterações física ou lógica da rede de dados.

CAPÍTULO XIV – DAS AQUISIÇÕES

Art. 139 Toda aquisição, upgrade e distribuição de recursos de TI deve estar preferencialmente prevista no PETI, conforme o art. 2º.

Parágrafo único. Aquisições não previstas no PETI estarão sujeitas a limitações técnicas e orçamentárias.

Art. 140 A aquisição ou upgrade de hardware ou software deverá ser expressamente submetida ao STI, para proceder com a análise de viabilidade técnica.

Art. 141 O STI não será responsável pelo resultado de aquisições ou contratações realizadas pela Autarquia sem a participação formal de seu corpo técnico e que resultem em incompatibilidades, falhas, paralisações ou mau funcionamento dos bens ou serviços adquiridos ou contratados.

Art. 142 O STI pode não conseguir dar solução efetiva aos problemas oriundos da má aquisição ou contratação, previstos no art. anterior limitando-se a dar as orientações necessárias ao responsável para a resolução do problema.

Art. 143 Na hipótese do art. anterior, o gestor demandante da aquisição/contratação ficará responsável por coordenar as ações corretivas junto ao fornecedor, ouvido o STI quanto aos requisitos técnicos mínimos para mitigação de riscos e restabelecimento operacional.

Parágrafo único. O STI prestará orientação técnica registrada no GLPI, sem assumir responsabilidade sobre prazos, custos ou resultados da correção.

Art. 144 Os sistemas e softwares deverão atender a padrões de desenvolvimento, suporte operacional, segurança da informação, gestão documental, interoperabilidade e outros que venham a ser recomendados pelo STI.

§ 1º Os novos sistemas e softwares deverão:

I – ser portáveis e interoperáveis;

II – manter documentação atualizada;

III – ser homologados antes de entrar em produção.

CAPÍTULO XV – DAS PENALIDADES E DA RESPONSABILIZAÇÃO

Art. 145 O descumprimento das normas estabelecidas nesta Portaria sujeitará o infrator às sanções administrativas previstas na Lei Municipal nº 3.800, de 2 de dezembro de 1991 – Estatuto dos Servidores Públicos Municipais de Sorocaba, sem prejuízo das responsabilidades civil e penal cabíveis.

Art. 146 O usuário de TI que causar, por ação ou omissão, danos, vazamentos de informações, perda de dados, interrupção de serviços ou mau uso de recursos de Tecnologia da Informação, responderá pelas consequências de seus atos na forma da legislação vigente.

§ 1º A responsabilidade administrativa referida no caput independe da obrigação de ressarcimento dos prejuízos causados ao erário ou aos sistemas da Autarquia.

§ 2º A apuração das condutas será feita mediante procedimento administrativo próprio, assegurados o contraditório e a ampla defesa.

Art. 147 Todo incidente de segurança, falha operacional, violação de dados ou uso indevido de recursos tecnológicos deverá ser registrado formalmente pelo STI, com a descrição do ocorrido, data, hora, envolvidos e medidas corretivas adotadas.

§ 1º. O STI manterá histórico atualizado dos incidentes registrados, para fins de auditoria e controle interno.

§ 2º Sempre que o incidente configurar infração disciplinar ou indício de dolo, o STI deverá comunicar formalmente à chefia do departamento responsável e à Diretoria Administrativa, para a devida instauração de processo administrativo.

§ 3º Nos casos de indício de crime, a Direção Geral do SAAE poderá determinar o encaminhamento das informações às autoridades competentes.

Art. 148 A reincidência no descumprimento das normas desta Portaria poderá implicar bloqueio temporário de acesso, suspensão de privilégios de rede ou outras medidas técnicas preventivas determinadas pelo STI, sem prejuízo das penalidades disciplinares aplicáveis.

Art. 149 O usuário que tiver conhecimento de uso indevido, incidente ou violação às normas desta Portaria e não comunicar o fato ao STI ou à chefia imediata, poderá ser responsabilizado por omissão, nos termos da Lei Municipal nº 3.830/1991, dentro do critério de razoabilidade.

CAPÍTULO XVI – DAS DISPOSIÇÕES TRANSITÓRIAS

Art. 150 Enquanto vigentes o contrato de correio eletrônico e backup terceirizado que estabelece retenção de mensagens por 7 (sete) dias e a política de backup em fitas LTO-5 para arquivos de rede com retenção de 20 (vinte) dias, permanecem aplicáveis os prazos previstos nos arts. 64 e 136. Havendo modificação contratual ou de infraestrutura

que permita janela distinta, o STI poderá ajustar os prazos por ato próprio, mediante anuência do Diretor Geral e promovendo a atualização desta Portaria.

CAPÍTULO XVII – DAS DISPOSIÇÕES FINAIS

Art. 151 Fica instituído o "Termo de Ciência e Responsabilidade – Política de Tecnologia da Informação (PTI)", constante do Anexo I desta Portaria, a ser obrigatoriamente firmado por todos os Usuários de TI que utilizem recursos tecnológicos do SAAE de Sorocaba.

Art. 152 A assinatura do Termo de que trata o artigo anterior será exigida:

I – na posse ou início de exercício de novos servidores, empregados, estagiários, prestadores de serviço ou quaisquer colaboradores que venham a utilizar recursos de TI;

II – quando da lotação em unidade em que o uso de recursos de TI seja condição necessária para o desempenho das atribuições;

III – sempre que houver atualização relevante da Política de Tecnologia da Informação (PTI) que justifique a coleta de nova ciência formal.

Art. 153 Compete ao Departamento de Recursos Humanos, em conjunto com o STI, adotar os procedimentos necessários à coleta, guarda e atualização dos Termos de Ciência e Responsabilidade, bem como garantir que sua assinatura integre os fluxos de admissão, movimentação e desligamento de pessoal.

Art. 154 Os Termos de Ciência e Responsabilidade assinados terão validade enquanto vigente a presente Portaria ou até que novo termo venha a substituí-lo, devendo ser arquivados em meio físico ou digital, conforme normas internas de gestão documental.

Art. 155 Esta Portaria entra em vigor na data de sua publicação, produzindo efeitos imediatos em todo o âmbito do Serviço Autônomo de Água e Esgoto de Sorocaba – SAAE.

Art. 156 Fica revogada a Portaria nº 943/2014 – STI, bem como quaisquer outras disposições internas que contrariem ou conflitem com o conteúdo desta norma.

Art. 157 O STI deverá promover a divulgação interna desta Portaria por meio eletrônico e físico, garantindo o amplo conhecimento de seu conteúdo por todos os Usuários de TI da Autarquia.

Art. 158 Os casos omissos ou as situações excepcionais decorrentes da aplicação desta Portaria serão resolvidos pelo Diretor da área, em conjunto com o Diretor Geral do SAAE.

Art. 159 Publique-se, registre-se e cumpra-se.

Sorocaba, 19 de junho de 2026.

Glauco Enrico Bernardes Fogaça

Diretor Geral

ANEXO I

TERMO DE CIÊNCIA E RESPONSABILIDADE

POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO (PTI)

Pelo presente instrumento, eu, **[NOME COMPLETO DO SERVIDOR]**, inscrito no CPF sob o nº **[000.000.000-00]** e matrícula nº **[0000]**, lotado no setor **[NOME DO SETOR]**, declaro ter recebido cópia integral, lido e compreendido os termos da **Portaria nº [XX]/2025**, que institui a **Política de Tecnologia da Informação (PTI)** no âmbito do **SAAE de Sorocaba**, comprometendo-me a observar as seguintes condições:

1. Natureza Institucional dos Recursos

Estou ciente de que todos os ativos de TI (computadores, notebooks, tablets, smartphones, acesso à internet e e-mail institucional) são ferramentas de trabalho fornecidas pelo SAAE exclusivamente para o exercício de minhas funções profissionais, permanecendo sob a propriedade e o controle da Autarquia.

2. Dever de Monitoramento e Auditoria

Tenho plena ciência de que, conforme os **Arts. 45 e 49 da Portaria**, o SAAE utiliza sistemas de monitoramento que registram logs de acesso à internet, tráfego de dados e uso de e-mail institucional. Autorizo e reconheço o direito da Administração Pública de auditar tais recursos a qualquer tempo, sem aviso prévio, para garantir a segurança da informação e a conformidade com o interesse público.

3. Proteção de Dados (LGPD)

Comprometo-me a tratar dados pessoais aos quais tenha acesso em razão do cargo estritamente conforme a **Lei Federal nº 13.709/2018 (LGPD)** e o **Art. 125 da Portaria**, sendo vedado o armazenamento ou compartilhamento de dados pessoais sensíveis (**Art. 5º, II da LGPD**) em desacordo com as finalidades institucionais.

4. Guarda e Conservação

Assumo a responsabilidade pela guarda e uso zeloso dos equipamentos a mim confiados. Estou ciente de que a retenção de arquivos em rede e e-mails é limitada (**Arts. 64 e 136 da Portaria**), sendo minha obrigação salvar documentos oficiais nos sistemas de gestão documental apropriados.

5. Senhas e Acessos

Declaro que minhas credenciais de acesso (usuário e senha) são pessoais e intransferíveis, sendo eu o único responsável por qualquer ação realizada sob minha identidade digital, conforme previsto na **Lei Federal nº 12.965/2014 (Marco Civil da Internet)**.

6. Sanções Disciplinares

Estou ciente de que o descumprimento das normas estabelecidas na PTI sujeitará o infrator às sanções administrativas previstas na **Lei Municipal nº 3.800/1991 (Estatuto dos Servidores)**, sem prejuízo de eventuais responsabilidades civis e criminais.

Sorocaba, [dia] de [mês] de 202[x].

_____

[ASSINATURA DO SERVIDOR / COLABORADOR / USUÁRIO]