ESTÂNCIA TURÍSTICA DE AVARÉ
ESTADO DE SÃO PAULO

SEMANÁRIO

Oficial Eletrônico
avare.sp.gov.br

Quinta-feira, 28 de novembro de 2024 | Ano VIII | Edição nº 2199 | Prefeito: Joselyr B. Costa Silvestre

PODER EXECUTIVO

Atos Oficiais

Decretos

Decreto n.º 8.038, de 18 de novembro de 2024.

(Institui a Política Municipal de Segurança da Informação da Estância Turística de Avaré.)

JOSELYR BENEDITO COSTA SILVESTRE, Prefeito da Estância Turística de Avaré, usando das atribuições que lhe são conferidas por lei e,

CONSIDERANDO a necessidade de garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações e recursos de tecnologia da informação (TI) da Prefeitura Municipal da Estância Turística de Avaré;

CONSIDERANDO a importância de estabelecer procedimentos claros e objetivos para o gerenciamento e controle desses recursos.

D E C R E T A:

Art. 1º. Fica instituída a Política Municipal de Segurança da Informação no âmbito da Estância Turística de Avaré, cujo texto foi aprovado pela Secretaria Municipal de Administração e Secretaria Municipal de Governo.

Art. 2º. A Política Municipal de Segurança da Informação encontra-se amparada nos seguintes princípios:

I – Confidencialidade: propriedade da informação que só a torna disponível a indivíduos e entidades autorizadas;

II – Integridade: propriedade que garante que os dados sejam corretos, autênticos e confiáveis, tal como foram fornecidos;

III – Disponibilidade: propriedade que garante a acessibilidade dos dados e sistemas quando necessário.

IV – Autenticidade: garantia de que não há fraude nas informações e dados.

Art. 3º. A Política Municipal de Segurança da Informação instituída por este Decreto deverá ser observada por todos os Órgãos e Entidades da Prefeitura da Estância Turística de Avaré, que deverão promover, em articulação com a Secretaria Municipal de Administração, a adequação de suas estruturas à respectiva política em um prazo de até 04 (quatro) meses.

Art. 4º. Para efeito deste Decreto ficam estabelecidas as Diretrizes e Normas constantes no Anexo I.

Art. 5º. Em até 60 (sessenta) dias após a publicação deste Decreto, deverá ser nomeado o Comitê Gestor da Informação, que deverá ser composto por:

I. Departamento de Tecnologia da Informação - 2 (dois) membros titulares e 2 (dois) suplentes;

II. Secretaria de Administração - 1 (um) membro titular e 1 (um) suplente;

III. Secretaria de Fazenda – 01 (um) membro titular e 1 (um) suplente;

IV. Gabinete do Prefeito - 1 (um) membro titular e 1 (um) suplente;

V. Secretaria de Governo - 1 (um) membro titular e 1 (um) suplente;

VI. Secretaria de Comunicação - 1 (um) membro titular e 1 (um) suplente;

VII. Procuradoria Geral do Município - 1 (um) membro titular e 1 (um) suplente; e,

VIII. Controladoria Geral do Município - 1 (um) membro titular e 1 (um) suplente.

Art. 6º. Este Decreto entre em vigor na data de sua publicação.

Prefeitura da Estância Turística de Avaré, aos 18 de novembro de 2024.

JOSELYR BENEDITO COSTA SILVESTRE
PREFEITO

ANEXO I
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Documento de Diretrizes e Normas Administrativas
Versão 1.0
2024

HISTÓRICO DE REVISÕES

Data	Versão	Responsável	Aprovação
03/10/2024	1.0	Anderson Rui do Amaral Paulo Pera dos Santos Rodrigo de Souza	Patrícia de Cássia Furno Olindo Franzolin Ronaldo Adão Guardiano

APRESENTAÇÃO

A Prefeitura da Estância Turística de Avaré – adiante referida apenas como PREFEITURA – é responsável pelo armazenamento e processamento de informações de diversos segmentos da municipalidade, seja em Data Centers[1] existentes ou em serviços de computação em nuvem (cloud computing) devendo processar e disponibilizar essas informações adequadamente e protegê-las contra ameaças e riscos.

Políticas, normas e procedimentos que visem garantir a segurança da informação devem ser prioridades constantes da PREFEITURA, reduzindo-se os riscos de falhas, os danos e os prejuízos que possam comprometer seus objetivos e sua imagem.

A Política de Segurança da Informação, adiante referida como PSI, define as diretrizes, limites e controles que serão implantados na proteção de suas informações e a responsabilidade legal de todos os colaboradores[2] e usuários, devendo ser cumprida e aplicada em todas as áreas da administração direta e indireta.

Esta PSI baseia-se nas recomendações propostas pela norma técnica ABNT NBR ISO/IEC 27002:2005, assim como está em conformidade com as leis vigentes em nosso país, especialmente em relação à Lei Federal n. 13.709 de 14 de

agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). Também implanta controles definidos pelo *CIS Center for Internet Security* através do *CIS Critical Security Controls* ou *CIS Controls* em sua versão 8.

Este documento, bem como seus anexos, encontra-se disponível na intranet da PREFEITURA, na seção Normas e Documentos.

OBJETIVOS

I. Definir o tratamento a ser adotado em relação às informações armazenadas, processadas ou transmitidas no ambiente físico e no ambiente de tecnologia da PREFEITURA.

II. Estabelecer e definir normas, processos, procedimentos e controles específicos de segurança da informação, bem como implementá-los.

III. Preservar as informações quanto à:

a. **Confidencialidade:** Toda informação deve ser acessada por quem de direito, até que se torne pública. É obrigação da PREFEITURA assegurar que informações confidenciais e críticas não sejam subtraídas dos sistemas organizacionais por meio de ciberataques, espionagem, entre outras práticas.

b. **Integridade:** preservação da precisão, consistência e confiabilidade das informações e sistemas.

c. **Disponibilidade:** Garantia de acesso à informação durante o ciclo de sua existência.

d. **Conformidade:** Toda informação deve estar em conformidade com os padrões, regras e – especialmente – com a legislação vigente.

e. **Auditabilidade:** Configuração de sistemas e bases de dados de forma a possibilitar o rastreamento de atividades físicas e lógicas.

ESTRUTURA

I. **Política de Segurança da Informação:** constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;

II. **Normas de Segurança da Informação:** estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;

III. **Procedimentos de Segurança da Informação:** instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da PREFEITURA.

DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

I. A Política e as Normas de Segurança da Informação serão divulgadas a todos os colaboradores da PREFEITURA no âmbito da administração direta e indireta e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento, utilizando a internet, intranet e outros canais apropriados. Os Procedimentos de Segurança da Informação serão divulgados às áreas diretamente relacionadas à sua aplicação.

APROVAÇÃO E REVISÃO

I. Os documentos integrantes da estrutura normativa da Segurança da Informação da PREFEITURA serão aprovados e revisados quando motivados por algum fato relevante ou evento, com periodicidade mínima anual, sob responsabilidade do Departamento de Tecnologia da Informação.

ABRANGÊNCIA

I. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores da administração direta e indireta que utilizem ou gerem as informações da PREFEITURA.

II. Os colaboradores dos organismos da administração indireta, empresas, autarquias, fundações e afins, quando utilizando a estrutura da PREFEITURA, atenderão pelo menos o disposto nesta Política, podendo os referidos organismos estabelecer instrumentos próprios, se aprovados nas suas instâncias.

III. As diretrizes também se estendem aos prestadores de serviços que necessitem do acesso à rede corporativa para execução das atividades contratadas, assim como colaboradores em regime de exceção.

PRINCÍPIOS

I. Toda informação, produzida ou recebida pelos colaboradores como resultado da atividade profissional, pertence à PREFEITURA.

II. Todos os equipamentos, sistemas e informações devem ser utilizados pelos colaboradores para a realização de suas atividades profissionais.

III. Esta PSI dá ciência a cada colaborador de que os ambientes, sistemas, dispositivos informáticos[4] e redes, no âmbito da administração direta e indireta, poderão ser monitorados e gravados, conforme previsto na legislação nacional.

REQUISITOS

I. A PSI será comunicada a todos os colaboradores da PREFEITURA, com a finalidade de que seja cumprida dentro e fora da mesma, durante o acesso a sistemas, ambientes e equipamentos da rede corporativa da PREFEITURA.

II. É obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu superior imediato sempre que não estiver absolutamente seguro quanto à aquisição, uso ou descarte de informações.

III. A responsabilidade em relação à segurança da informação será comunicada na fase de contratação dos colaboradores. Todos os colaboradores serão orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos, devendo assinar o termo de responsabilidade.

IV. Em relação aos colaboradores já vinculados à PREFEITURA através de carreira efetiva ou contratações (comissionados, estagiários, prestadores de serviços) tomarão ciência em até 60 (sessenta) dias da aprovação desta Política.

V. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao superior imediato,

que dará ciência ao Departamento de Tecnologia da Informação (DTI).

VI. A PREFEITURA exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios de natureza civil, administrativa e criminal, bem como adotar as medidas legais cabíveis.

VII. Esta PSI será implementada na PREFEITURA por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente de nível hierárquico, função ou vínculo empregatício durante o acesso aos sistemas e equipamentos.

VIII. O não cumprimento dos requisitos previstos nesta PSI e demais instrumentos normativos complementares, acarretará violação às regras internas da administração municipal e sujeitará o usuário às medidas administrativas e legais cabíveis.

IX. Para a realização do controle e acompanhamento da Política de Segurança da Informação será criado o Comitê Gestor da Informação, que deverá ser composto, no mínimo, por:

a. 02 servidores do Departamento de Tecnologia da Informação;

b. 01 servidor da Secretaria de Administração;

c. 01 servidor da Secretaria de Fazenda;

d. 01 servidor do Gabinete do Prefeito;

e. 01 servidor da Secretaria de Governo;

f. 01 servidor da Secretaria de Comunicação;

g. 01 servidor da Procuradoria Geral do Município;

h. 01 servidor da Controladoria Geral do Município;

X. Exceções à PSI poderão ser atendidas desde que solicitadas através de abertura de chamado e deverão conter: justificativa da solicitação, usuários e equipamentos que deverão estar inclusos na exceção, data de início e fim da vigência da exceção.

XI. Os pedidos de atendimento a exceções definidos no item anterior serão avaliados pelo DTI e deverão ter registradas:

a. os riscos gerados pela exceção;

b. as mitigações que deverão ser implementadas;

c. as mitigações que deixarão de ser implementadas em razão da exceção;

d. as dificuldades (técnicas, monitoramento etc.);

e. data da autorização; e,

f. data para revisão.

XII. As informações constantes do item anterior deverão ser registradas independentemente da aceitação ou negação da implantação da exceção.

ATRIBUIÇÕES E RESPONSABILIDADES

Comitê Gestor da Segurança da Informação (CGSI)

Cabe ao CGSI**:**

I. Analisar a revisão da Política de Segurança da Informação encaminhada pelo DTI e aprovar suas modificações;

II. Aprovar e nomear os administradores da informação;

III. Propor e implementar ações voltadas à capacitação de colaboradores para a plena aplicação de normas e procedimentos voltados ao aprimoramento do consumo e utilização segura dos ativos de informação[5] da PREFEITURA;

IV. De acordo com a necessidade, qualquer funcionário da PREFEITURA e convidado externo poderá participar das reuniões do CGSI, quando solicitado;

V. Caberá ao Presidente do CGSI a coordenação dos trabalhos do comitê, cujas atribuições abrangerão a convocação das reuniões e a realização de outros atos de suporte às atividades desenvolvidas;

VI. As reuniões do CSGI:

a. Serão realizadas ordinariamente quadrimestralmente, podendo haver convocação extraordinária sempre que necessário;

b. As decisões do CSGI deverão ser registradas em ata. O CGSI deliberará por maioria dos votos presentes.

VII. As reuniões do CSGI poderão ocorrer de forma presencial ou à distância.

VIII. Os registros e assinaturas das atas das reuniões do CGSI deverão ser preferencialmente realizadas em formato digital e prioritariamente assinados com a utilização de assinatura digital do serviço GOV.br;

Departamento de Tecnologia da Informação (DTI)

Cabe ao DTI:

I. Propor ajustes, aprimoramentos e modificações desta Política e encaminhá-las ao CSGI;

II. Propor melhorias e aprovar as Normas de Segurança da Informação baseadas nas diretrizes estabelecidas pela PSI e pelo CSGI;

III. Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando ao CSGI;

IV. Propor projetos e iniciativas relacionados à melhoria da segurança da informação da PREFEITURA;

V. Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;

VI. Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão da segurança da informação e à tomada de decisão;

VII. Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;

VIII. Realizar o levantamento, identificação, avaliação e monitoramento dos riscos à segurança da informação, em consonância com diretrizes próprias para gestão de riscos em tecnologia da informação.

IX. Propor e implementar ações voltadas à capacitação de colaboradores para a plena aplicação de normas e procedimentos voltados ao aprimoramento do consumo e utilização segura dos ativos de informação da PREFEITURA;

X. Realizar o estudo, especificação e implantação de plataforma de aprendizado aos colaboradores da

PREFEITURA, propiciando capacitação contínua em, entre outros, temas relacionados ao controle da privacidade e segurança da informação;

Representantes da Segurança da Informação das Secretarias Municipais

Com a responsabilidade de divulgar, atualizar e difundir a Política de Segurança da Informação entre seus pares nas Secretarias Municipais serão indicados os Representantes da Segurança da Informação de cada Secretaria Municipal.

Caberá aos representantes:

I. Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores de sua secretaria ou órgão da administração direta e indireta;

II. Oferecer orientação sobre a PSI e suas Normas a todos os colaboradores de sua secretaria ou órgão da administração direta e indireta;

III. Analisar os riscos relacionados à segurança da informação da PREFEITURA em suas respectivas áreas;

IV. Apresentar relatórios sobre tais riscos ao DTI;

V. Realizar o registro e controle de infrações à PSI e comunicar essas infrações ao DTI.

VI. Incentivar a participação dos colaboradores de sua secretaria em ações de capacitação em relação à Segurança da Informação

Administradores da Informação

Os administradores da informação são colaboradores da PREFEITURA formalmente indicados pelas Secretarias ou órgãos municipais que serão responsáveis pela autorização de concessão, manutenção, revisão e solicitação de cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes à PREFEITURA ou sob a sua guarda.

Cabe ao administrador da informação:

I. Elaborar, para toda informação sob sua responsabilidade, matriz relacionando cargos e funções às autorizações de acesso concedidas prezando sempre pelo princípio do menor privilégio[6];

II. Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz de cargos e funções, a PSI e as Normas de Segurança da Informação da PREFEITURA e as diretrizes específicas do CGSI;

III. Manter registro e controle atualizados de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;

IV. Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;

V. Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;

VI. Participar, sempre que convocado, das reuniões do CGSI, prestando os esclarecimentos solicitados;

VII. Solicitar imediatamente a inativação do acesso aos sistemas da secretaria ou órgão quando da saída de colaboradores de sua área de responsabilidade;

Procuradoria Geral do Município

Cabe à Procuradoria Geral do Município:

I. Tomar as providências jurídicas cabíveis em casos de incidentes de segurança.

II. Prestar suporte ao CSGI para os casos em que se faça necessário.

Secretarias e Órgãos Municipais

Cabe aos Gestores das Secretarias e Órgãos Municipais:

I. Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;

II. Assegurar que suas equipes possuam acesso e conhecimento desta Política, das Normas e dos Procedimentos de Segurança da Informação;

III. Sugerir os Procedimentos de Segurança das Informações relacionados às suas áreas;

IV. Comunicar imediatamente eventuais casos de violação de segurança da informação ao DTI;

V. Solicitar a liberação de sites, sistemas, aplicações, seguindo o descrito nesta PSI.

Secretaria de Administração

Cabe à Secretaria de Administração:

I. Colher a assinatura do Termo de Responsabilidade dos funcionários, estagiários e terceirizados, arquivando-os nos respectivos prontuários;

II. Tomar as providências administrativas no caso de aplicação de penalidades aos trabalhadores quanto ao não cumprimento da PSI.

Colaboradores

Entende-se por colaborador toda e qualquer pessoa física, contratada (concursada ou comissionada) ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da prefeitura.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à PREFEITURA ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Para liberação de acesso à rede corporativa, será necessário o aceite do termo de responsabilidade (Anexo II para colaboradores e Anexo III para prestadores de serviços).

Cabe aos colaboradores:

I. Cumprir as normas definidas na PSI;

II. Reportar ao superior hierárquico, de imediato, qualquer incidente de segurança ou, até mesmo, suspeitas de incidentes;

III. Sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação

Colaboradores em Regime de Exceção (Temporários)

I. Compreende-se por colaborador em regime de exceção todo colaborador que não se enquadre como servidor público, agente político ou empregado público, tais como estagiários (com ou sem remuneração) e prestadores de serviços;

II. Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no Termo de Responsabilidade concedido pela PREFEITURA.

III. A concessão poderá ser revogada a qualquer tempo, se for verificada que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção, ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no termo.

IV. A revogação de concessão não desobriga o colaborador em regime de exceção de responder pelos riscos e incidentes de informação causados pelo não atendimento das condições definidas na PSI.

NORMAS GERAIS

Para garantir as regras mencionadas na PSI, a PREFEITURA adotará algumas ações, em relação a:

Criação de credenciais

I. Somente será realizada a criação das credenciais de acesso após assinatura do Termo de Responsabilidade de utilização da rede da Prefeitura pelo usuário;

II. A criação de credenciais deverá ser solicitada através de abertura de chamado individualizado para cada usuário;

III. A criação de credenciais a colaboradores, sejam estes agentes públicos ou estagiários, dependerá de confirmação das informações do usuário pelo Departamento de Recursos Humanos e Gestão de Pessoal;

IV. A credencial para acesso deverá ser composta por nome e sobrenome, preferencialmente utilizando-se o nome de nascimento, ao invés do nome adquirido após o casamento. Esta indicação não se aplica ao nome de exibição, somente ao nome utilizado para acesso aos dispositivos e/ou sistemas. Tal recomendação aplica-se em razão da necessidade de evitar-se a alteração de credencial, garantindo a integridade para a realização de auditorias.

V. Em caso de nomes compostos, em especial onde o primeiro nome possua poucos caracteres, preferencialmente será adotado o padrão do nome composto.sobrenome. Exemplo: Ana Paula Silva (anapaula.silva), Maria Carla Soares (mariacarla.soares), Jose Carlos Ribeiro (josecarlos.ribeiro) etc.

VI. As regras IV e V não se aplicarão a questões como mudança de nome em razão da mudança de gênero e/ou quaisquer outras alterações decorrentes de decisões judiciais ou de garantia de direitos do usuário.

Desativação de credenciais

I. A desativação das credenciais será realizada por:

a. Comprometimento da conta;

b. Falta de acesso ao e-mail em prazo superior a 15 (quinze) dias, quando o usuário possuir acesso a este;

c. Término do contrato do usuário;

d. Desligamento do usuário;

II. Caso a desativação ocorra através da hipótese “d”, o Departamento de Tecnologia da Informação deverá ser informado pelo DRHGP antes da comunicação ao usuário de seu desligamento, permitindo que sejam tomadas as ações necessárias para garantia da disponibilidade e integridade de dados, informações, documentos e dispositivos.

III. O Departamento de Tecnologia da Informação deverá realizar a desativação do usuário, mantendo-se registro das ações e ocorrências, de maneira célere, garantindo a revogação do acesso o mais rápido possível após a comunicação (hipóteses “c” e “d” ou a ocorrência do fato (hipóteses “a” e “b”).

Monitoramento e Auditoria do Ambiente

I. 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 será usada para identificar usuários e respectivos acessos efetuados, bem como o material manipulado;

II. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial e/ou para o atendimento a solicitações de comissões de processo administrativo e sindicância;

III. Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

IV. Instalar sistemas de proteção, para garantir a segurança das informações e dos perímetros de acesso.

Correio eletrônico

I. O uso do correio eletrônico da PREFEITURA é para fins corporativos, relacionados às atividades do colaborador dentro da prefeitura. É vedado o uso do correio eletrônico da PREFEITURA para fins pessoais;

II. É vedada a utilização de e-mails de provedores externos (Gmail, Hotmail, Outlook etc.) para o envio e recebimento de informações e comunicações, para o público interno ou externo, de assuntos relacionados à PREFEITURA. Para isto, é necessária a utilização da lista de distribuição provida pelo DTI a todos as secretarias, departamentos e unidades, que realiza o encaminhamento das mensagens recebidas para os colaboradores inclusos nestas listas. Em caso da necessidade de criação de nova lista de distribuição, é necessária a realização de abertura de chamado pelo representante da Secretaria ou Departamento contendo o nome desejado para a lista, quais usuários deverão receber acesso e a justificativa;

III. O envio de mensagens a todos os componentes da lista de endereços da PREFEITURA (todos@avare.sp.gov.br) restringir-se-á a assuntos de interesse geral dos servidores, sendo autorizada à: Secretaria Municipal de Administração, Departamento de Recursos Humanos e Gestão de Pessoal, Departamento de Tecnologia da Informação, Departamento de Telefonia, Departamento de Saúde do Servidor e Secretaria de Comunicação. Nos casos em que seja necessário o envio à lista geral de endereços da PREFEITURA, o requerente deverá abrir chamado solicitando a permissão com a justificativa. Caso aprovada, a autorização será temporária.

IV. Acrescentamos que é proibido o uso do correio eletrônico para:

a. Enviar, sem autorização, mensagens não solicitadas

para múltiplos destinatários (SPAM[7]), exceto se relacionadas a uso legítimo da prefeitura.

b. Enviar, sem autorização, mensagens pelo endereço de seu departamento ou usando o nome ou endereço de correio eletrônico de outra pessoa, exceto quando formalmente delegado o acesso, que deverá ser solicitado através de abertura de chamado.

c. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente, a PREFEITURA, ou suas unidades, vulneráveis a ações cíveis ou criminais.

d. Divulgar sem autorização da Chefia da Seção ou Departamento relacionados, qualquer informação ou imagem de tela de sistemas, documentos e afins, as quais não sejam estritamente relacionadas ao destinatário e à solicitação formalmente registrada através de sistema de protocolo e/ou similar.

e. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes ou destinatários.

f. Apagar mensagens de correio eletrônico, relacionadas a investigações a que a PREFEITURA estiver sujeita.

g. Produzir, transmitir ou divulgar mensagem ou imagem que contenha:

1. ato ou orientação que conflite ou contrarie os interesses da PREFEITURA;

2. contenha ameaças eletrônicas como: *spam*, *mail bombing*[8], *malwares* [9]etc.;

3. contenha arquivo executável (.exe, .com, .bat, .vbs, reg, .dll) ou qualquer outra extensão que represente um risco à segurança;

4. vise obter acesso não autorizado a outro computador, servidor ou rede;

5. vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

6. vise burlar qualquer sistema de segurança;

7. vise vigiar secretamente ou assediar outro usuário;

8. vise acessar informações confidenciais sem explícita autorização do proprietário da informação[10];

9. vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

10. inclua imagens criptografadas ou de qualquer forma mascaradas, exceto aquelas previstas em norma ou procedimento;

11. contenha anexo(s) superior(es) a 20MB para envio ou recebimento;

12. contenha conteúdo considerado impróprio, obsceno ou ilegal;

13. seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros;

14. contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

15. tenha a finalidade de propagar propaganda política;

16. inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;

V. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

Nome do colaborador
Cargo
Departamento
Secretaria Municipal
Telefone(s)
Correio eletrônico

Internet e intranet

I. Todas as regras atuais da PREFEITURA visam o desenvolvimento de um comportamento ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da PREFEITURA com a internet ofereça benefícios, abre a porta para riscos significativos para os ativos de informação;

II. Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a PREFEITURA, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela;

III. Os equipamentos, tecnologias e serviços oferecidos para o acesso à internet são de propriedade da prefeitura, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede ou internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua PSI.

IV. A PREFEITURA, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e autorização do DTI para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador, superior imediato e registrado como incidente de segurança da informação a ser reportado ao CSGI. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processo civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

V. Somente os colaboradores que estão devidamente autorizados a se manifestar em nome da PREFEITURA (por exemplo, Prefeito, Secretários, Assessoria de Comunicação, Titulares da Administração Indireta etc.) poderão manifestar-se para os meios de comunicação em relação a informações não públicas sob guarda da PREFEITURA, seja por e-mail, entrevista on-line, podcast[11], seja por documento físico, entre outros, exceto nos casos expressamente autorizados.

VI. Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à

proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

VII. É proibida a divulgação ou o compartilhamento indevido de informações não públicas em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha a surgir na internet.

VIII. O uso, a instalação, a cópia ou distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são proibidos. Qualquer software não autorizado baixado será excluído pelo DTI e deverão ser comunicados ao colaborador, a seu superior imediato e registrado como incidente de segurança da informação a ser reportado ao CSGI. Situações ocorridas anteriores a publicação desta PSI serão informadas ao CGSI para conhecimento e normatização, se cabível.

IX. Os colaboradores não poderão, em hipótese alguma, utilizar os recursos da PREFEITURA para efetuar o download ou distribuição de software ou dados não licenciados ou ilegais, atividade considerada delituosa de acordo com a legislação nacional.

X. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato), desde que não contrariem o disposto no item anterior, poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos secretários municipais, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, desde que comprovada sua utilidade pública.

XI. Colaboradores com acesso à internet não poderão efetuar *upload* ou cópia de qualquer software licenciado à PREFEITURA ou dados de sua propriedade aos seus parceiros e clientes sem expressa autorização do responsável pelo software ou pelos dados.

XII. Os colaboradores não poderão utilizar os recursos da PREFEITURA para deliberadamente propagar qualquer tipo de vírus, Worms[12], cavalo de troia, spam, assédio, e quaisquer outros considerados maliciosos ou ofensivos;

XIII. O acesso a softwares Peer-to-Peer[13] não será permitido, exceto se expressamente autorizado após apresentação de justificativas para seu uso e inexistência de outros protocolos para alcançar o objetivo almejado.

XIV. Os serviços de streaming[14], comunicação instantânea, redes sociais e afins, poderão ser permitidos, em regime de exceção, quando formalmente autorizados pelo secretário municipal.

XV. É proibido o uso de quaisquer equipamentos aqui abrangidos e das redes de comunicação da administração pública nos âmbitos da administração direta e indireta, por qualquer colaborador, para fins eleitorais.

XVI. A intranet será alimentada por informações produzidas pela administração direta e indireta seguindo, no que couber, os mesmos critérios aplicados acima para a internet.

Política de Senhas

I. Os dispositivos de identificação com senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a PREFEITURA ou terceiros

II. O uso de acessos, com identificação de outra pessoa, constitui crime tipificado no Código Penal Brasileiro (art. 307 – Falsidade Ideológica)

III. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

IV. Todo e qualquer sistema de identificação pessoal, em hipótese alguma, poderá ser compartilhado com outras pessoas.

V. A Secretaria de Administração (através do Departamento de Recursos Humanos e Gestão de Pessoal) é a responsável pelo controle e guarda dos documentos de identidade dos colaboradores. O DTI responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

VI. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas no ato de criação das credenciais de acesso.

VII. Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 10 (dez) caracteres, sem partes do nome do usuário e contendo 3 (três) das quatro categorias de caracteres abaixo:

a. Caracteres alfabéticos minúsculos

b. Caracteres alfabéticos maiúsculos

c. Caracteres numéricos

d. Caracteres especiais (!, @, #, $, %, &, *, (,), , -, +, etc.)

VIII. Os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de, no mínimo, 14 (quatorze) caracteres, alfanumérica, com caracteres especiais e contendo caracteres alfabéticos maiúsculos e minúsculos, obrigatoriamente.

IX. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

X. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.), compreensíveis por linguagem humana (não criptografados) e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, “q1w2e3r4” entre outras.

XI. Após 5 (cinco) tentativas de acesso sem sucesso, a conta do usuário será bloqueada, caso o ambiente acessado permita esse procedimento. Para o desbloqueio é necessário que o usuário entre em contato com o Departamento de Tecnologia da Informação (através do sistema de abertura de chamados). Em alguns casos o bloqueio poderá ser temporário (por exemplo, 15 minutos), e após esse tempo o usuário será desbloqueado automaticamente.

XII. Em caso de bloqueio da credencial por esquecimento, deverá ser estabelecido processo para a renovação de senha, após a confirmação de identidade. Será fornecida senha temporária, que deverá ser alterada no primeiro acesso, seguindo o estabelecido nos itens VII, VIII e X.

XIII. Em caso de bloqueio de credenciais por comprometimento de segurança, o incidente será relatado ao CSGI. Deverá ser estabelecido processo para alteração da credencial, que só será possível após confirmação de identidade e identificação dos riscos e danos ocorridos em consequência do comprometimento das credenciais.

XIV. Os usuários devem alterar sua senha imediatamente em caso de suspeita de que terceiros tenham obtido acesso à sua conta, e comunicar ao DTI.

XV. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Acesso Remoto Externo

Objetivo

Estabelecer critérios para a disponibilização do serviço de acesso remoto externo à rede corporativa da PREFEITURA, bem como as regras para sua utilização, visando a prevenção do acesso não autorizado às informações.

Diretrizes Gerais

I. O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos colaboradores que, oficialmente, executem atividade vinculada à atuação institucional da PREFEITURA e que necessitem desse serviço para execução de suas atividades institucionais, desde que autorizados.

II. A liberação de acesso remoto só será efetivada após avaliação e verificação de viabilidade técnica por parte do DTI e aprovação pelo CGSI (ou por membro definido por este), para que se evitem ameaças à integridade e sigilo das informações contidas na rede corporativa da PREFEITURA. Será feita uma análise criteriosa, podendo ser negado o acesso remoto caso comprometa a segurança do ambiente.

III. A solicitação do acesso remoto deve conter, no mínimo:

a. data da solicitação
b. tipo de solicitação
c. tempo de validade do acesso remoto
d. Justificativa
e. dados do solicitante
f. dados do usuário
g. dados do superior imediato
h. dados do Secretário Municipal.

IV. A solicitação deverá ser realizada através do sistema de chamados.

V. A disponibilização de acesso remoto à rede corporativa da PREFEITURA para outras organizações deve obedecer às seguintes regras:

a. Direitos de acesso definidos por contrato formal entre as partes;
b. Acesso temporário e limitado às necessidades do negócio;
c. Revisão periódica dos direitos de acesso;
d. Utilização de solução que permita a implementação e controle de regras de acesso.

VI. O serviço de acesso remoto deve ser cancelado sob as seguintes condições:

a. Finalização do período especificado na solicitação ou no contrato;
b. Perda da necessidade de utilização do serviço;
c. Transferência do usuário para outras unidades;
d. Identificação de vulnerabilidade, risco ou uso indevido no acesso concedido. A revogação do acesso remoto não eximirá a apuração do uso indevido realizado e suas possíveis implicações administrativas, cíveis e penais.

VII. As conexões remotas à rede corporativa da PREFEITURA devem ocorrer da seguinte maneira:

a. Utilização de autenticação;
b. As senhas e as informações que trafegam entre a estação remota e a rede corporativa da PREFEITURA devem estar criptografadas;
c. Todas as conexões e acessos serão registrados em log, para posterior auditoria.
d. Caso disponível, a autenticação em dois fatores (2FA) deve ser habilitada.

VIII. Cada usuário deve manter suas credenciais de acesso (login e senha) em sigilo absoluto e não o fornecer a outra pessoa.

IX. É vedada a utilização de acesso remoto para fins não relacionados às atividades da prefeitura.

Computadores, Dispositivos Portáteis e Recursos Tecnológicos

I. A PREFEITURA é detentora dos equipamentos fornecidos, cabendo aos usuários a correta utilização e manuseio para as atividades de interesse da prefeitura, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis;

II. A PREFEITURA reserva-se o direito de inspecionar qualquer equipamento a qualquer momento;

III. É proibido qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento do DTI, ou de quem este determinar.

IV. Os equipamentos de rede (comutadores, roteadores, pontos de acesso) disponibilizados pelo DTI seguem padronização visando à disponibilização de

cobertura de rede suficiente às atividades realizadas pelas unidades da PREFEITURA. A alteração de configuração, mudança, desconexão e remoção não realizadas pelo DTI poderão ser passíveis de abertura de procedimento disciplinar.

V. A contratação de link de internet deve ser realizada com a anuência expressa do DTI e segundo suas orientações. A instalação de roteadores e/ou pontos de acesso fica condicionada à realização de estudo de interferência entre equipamentos pelo DTI. A não observância dessa orientação faculta ao DTI a retirada dos equipamentos não homologados e/ou instalados sem sua autorização, além da possibilidade de abertura de procedimento disciplinar pela não observância das normas.

VI. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos deverão ser aplicadas, entretanto, somente após suas disponibilizações oficiais, em versão estável, do fabricante ou fornecedor;

VII. Os computadores e dispositivos portáteis deverão ter versões do software antivírus instalados e ativados permanentemente, mantendo-os atualizados. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o DTI mediante registro de chamado;

VIII. A transferência ou divulgação de qualquer informação, software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a identificação positiva do solicitante junto ao Gestor responsável por esta informação, e estando de acordo com a classificação dessa informação[15] e a pertinente necessidade do destinatário.

IX. O transporte de computador ou dispositivo portátil[16] em veículos motorizados, deverá ser realizado no interior do porta-malas, onde não ficará visível, não devendo ser deixado no interior do veículo quando ele estiver estacionado.

Uso dos Equipamentos

I. No uso dos computadores, dispositivos móveis, equipamentos e recursos de informática, as regras constantes deste tópico devem ser atendidas.

II. Não serão autorizados equipamentos pessoais para utilização na rede corporativa da PREFEITURA.

III. Todos os computadores de uso individual deverão ter a BIOS[17] protegida por meio de senha, com o objetivo de restringir o acesso de pessoas não autorizadas. Tais senhas serão definidas pelo DTI, que terá acesso a elas para manutenção dos equipamentos.

IV. Os colaboradores devem informar ao DTI qualquer identificação de dispositivo estranho conectado ao seu computador.

V. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do DTI ou por terceiros devidamente contratados para o serviço e expressamente autorizados pelo DTI.

VI. O colaborador deverá manter a configuração do equipamento disponibilizado pela PREFEITURA, seguindo os devidos controles de segurança exigidos pela PSI e pelas normas específicas da instituição, assumindo a responsabilidade das informações e utilização.

VII. Todos os recursos tecnológicos adquiridos pela PREFEITURA devem ter imediatamente suas senhas padrão alteradas.

VIII. Os equipamentos deverão manter os registros de eventos preservados em modo seguro, constando identificação dos usuários, datas e horários de acesso.

IX. É proibido o uso de computadores e recursos tecnológicos da PREFEITURA para:

a. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

b. Burlar quaisquer sistemas de segurança;

c. Acessar informações confidenciais sem explícita autorização do proprietário ou de seu guardião;

d. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (Sniffers);

e. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

f. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio, constrangimento, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

g. Hospedar pornografia, material contendo perseguição baseada em sexo, raça, incapacidade física ou mental, relacionada a outras situações protegidas ou qualquer outro que viole a legislação vigente no país, a moral, os bons costumes e a ordem pública.

Dispositivos Portáteis

I. Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados do dispositivo móvel pertencente a PREFEITURA sob sua guarda. Deverá, também, manter esses backups em local diferente de sua fonte de origem.

II. Os dispositivos móveis que permanecerem em qualquer área física da PREFEITURA deverão estar em locais de acesso restrito e seguros, quando não estiverem sendo utilizados pelo usuário.

III. Ao viajar com um computador portátil, o usuário deve:

a. manter o equipamento sempre consigo;

b. ao utilizar todo e qualquer meio de transporte público no deslocamento em função de atividade de trabalho (ônibus, avião, carros através de aplicativos, táxis, ou outros enquadramentos), dentro ou fora do município, desde que autorizado, certificar-se de que retirou toda a sua bagagem, inclusive o computador e demais equipamentos, quando chegar em seu destino.

IV. O transporte do equipamento nas ruas é bastante observado pelos criminosos, portanto, é aconselhável

discrição e atenção no ambiente e seus arredores no trajeto até seu destino.

V. Em caso de perda de acessório (mala, capa, mouse etc.) o colaborador será responsável pelo seu ressarcimento, em igual ou superior especificação, qualidade ou finalidade.

VI. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela PREFEITURA, notificar imediatamente seu gestor direto e o DTI. Também deverá procurar ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

VII. O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel não é permitido, e, caso haja conclusão de que houve uso indevido, este será responsabilizado conforme legislação vigente.

Uso da Rede

I. Arquivos pessoais ou não pertinentes aos assuntos da PREFEITURA (fotos, músicas, vídeos etc.) não poderão ser copiados ou movidos para a rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles serão excluídos definitivamente, sem aviso prévio.

II. Diretórios ou pastas de acesso público não deverão ser utilizados para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza específica. Devem ser utilizados apenas para armazenar informações de interesses gerais.

III. Arquivos em geral (textos, planilhas, imagens, vídeos e outros) que estejam duplicados na rede, e os que não forem de interesse da administração, poderão ser excluídos por auditoria periódica na rede.

IV. Documentos imprescindíveis para as atividades dos colaboradores na PREFEITURA deverão ser salvos nos compartilhamentos de rede.

V. Os colaboradores da PREFEITURA no âmbito da administração direta e indireta e detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que possa sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação, autorização e agendamento pelo DTI.

Engenharia Social

I. A engenharia social é qualquer método usado para enganar ou explorar a confiança das pessoas para a obtenção de informações sigilosas e importantes, tanto da prefeitura como do colaborador em questão. Para isso, alguém pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área etc.

II. Para evitar esse método, todos os colaboradores devem estar cientes das seguintes regras:

a. Nenhum colaborador da prefeitura está autorizado a passar informação às pessoas ou agentes estranhos dentro da prefeitura;

b. Caso alguém entre em contato por telefone, e-mail, softwares de comunicação, solicitando informações sigilosas da prefeitura ou do usuário, o colaborador abordado deverá entrar em contato com o responsável da rede interna e com seu superior hierárquico informando tais situações.

Certificação e Assinatura Digital

I. A utilização de certificados digitais, assim como a assinatura digital deverá ser incentivada sempre que possível;

II. A adoção de certificados digitais não onerosos deverá ser incentivada, exceto em casos em que não seja possível sua adoção;

III. A responsabilidade pelo uso, manuseio, guarda de assinatura de certificados digitais corporativos será definida para cada certificado gerado, através de documento próprio.

IV. A responsabilidade pelo uso, manuseio, guarda de assinatura de certificados digitais individuais será de responsabilidade de seus respectivos portadores.

CONCLUSÃO

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura da PREFEITURA. Ou seja, qualquer incidente de segurança entender-se-á como alguém agindo contra a ética e os bons costumes adotados pela prefeitura. O não cumprimento desta PSI e demais instrumentos normativos que complementam o processo de segurança constitui falta grave e o colaborador estará sujeito às penalidades administrativas, contratuais, cíveis e criminais, conforme a legislação vigente.

ANEXO II

TERMO DE RESPONSABILIDADE DE UTILIZAÇÃO DA REDE DA PREFEITURA DE AVARÉ

Funcionário: **( ) Estatutário**	**( ) Contrato prazo determinado**	**( )Comissionado**	**( ) Estagiário**
Caso não seja estatutário, informar a data de término do contrato:			**___/___/____**
Matrícula:		**Nome completo:**	
Telefone:	**( ) _____-_____**	**Cargo:**	
E-mail pessoal:			

Devo me comprometer a:

a. Manter minha conta de acesso à rede de computadores e e-mail exclusivamente para meu uso, não disponibilizando ou facilitando o uso das contas a qualquer pessoa, funcionário ou não, ainda que hierarquicamente superior;

b. Utilizar a rede corporativa da Prefeitura da Estância Turística de Avaré, adiante denominada PREFEITURA, unicamente para desempenhar minhas atribuições e atividades diárias no interesse da organização;

c. Não acessar ou tentar ganhar acesso a qualquer computador, rede ou arquivos sem autorização explícita e adequada. Comprometo-me ainda a informar imediatamente o Departamento de Tecnologia da Informação se tornar-me ciente de que tal acesso ocorreu;

d. Entendo que programas e dados existentes nos arquivos que tenho ou possa vir a ter acesso são protegidos

por direitos autorais, leis, licenças e/ou outros acordos contratuais, portanto, não violarei tais restrições;

e. Não utilizarei a estrutura tecnológica da PREFEITURA para obter, fazer, executar ou distribuir cópias não autorizadas de software;

f. Guardar o mais absoluto sigilo em relação aos softwares/sistemas utilizados pela PREFEITURA bem como os licenciados para seu uso;

g. Manter total sigilo sobre dados ou informações que venha a ter conhecimento em razão do acesso ao ambiente computacional e sistemas de informação da PREFEITURA;

h. Não instalar e/ou utilizar, sem a devida homologação e expressa autorização pelo DTI, softwares no ambiente tecnológico da PREFEITURA;

i. Utilizar os recursos de internet somente para fins voltados aos interesses da instituição, portanto, jamais tentarei burlar as regras de segurança que impeçam acessos indevidos ou busquem proteger a estrutura tecnológica da instituição;

j. Caso venha a receber permissão para acesso de dispositivos móveis de armazenamento de dados, estarei ciente de que deverei mantê-los protegidos com senha;

k. Caso me seja destinado algum certificado digital para utilização, comprometo-me a manter sua guarda e sigilo, tomando ciência de que, em caso de utilização indevida, será de minha exclusiva responsabilidade e poderei sofrer as sanções cabíveis;

l. Tenho ciência de que a conta corporativa será mantida pelo tempo de duração do contrato de trabalho, não me sendo disponibilizada após meu desligamento;

Diante dos fatos acima, **DECLARO** sob as penas da lei, verdadeiras as informações neste ato prestadas, fazendo parte dos registros e arquivos da PREFEITURA, tendo ciência do que estabelecem os artigos 153, 313-A, 313-B, 299, 325 e 327 do Código Penal Brasileiro, a legislação aplicada e demais normas complementares, aquiescendo com todas as responsabilidade inerentes ao uso dos recursos tecnológicos do órgão, bem como das implicações legais decorrentes do seu uso indevido, seja qual for a circunstância, constituindo o usuário e senha disponibilizados para acesso (e-mail e/ou rede corporativa), propriedade da PREFEITURA e portanto, sujeitos ao monitoramento e controle das ações realizadas no seu âmbito. Declaro ainda que, estou ciente de que a PREFEITURA concede contas de acesso à rede de computadores e e-mail para utilização exclusiva do usuário, portanto, não disponibilizarei nem facilitarei o uso das minhas referidas contas para qualquer pessoa, funcionário ou não, ainda que hierarquicamente superior.

Estância Turística de Avaré, ____ de _____ de 20____

_____ Assinatura do compromissado

DRHGP	Departamento de Tecnologia da Informação	
_____ Assinatura do validador	Criada por:	
	Data:	a
	Nome atribuído ao usuário:	

ANEXO III

TERMO DE RESPONSABILIDADE DE UTILIZAÇÃO DA REDE DA PREFEITURA DE AVARÉ PARA PRESTADORES DE SERVIÇOS

Empresa:			
Contrato:			
Nome:		CPF:	
Cargo:		Lotação:	
E-mail		Telefone:	

Pelo presente termo, declaro ter conhecimento da Política de Segurança da Informação da Prefeitura da Estância Turística de Avaré - adiante denominada apenas PREFEITURA, disponível para consulta em {URL}, e concordo em aceitar suas regras.

Com autorização superior, estou recebendo uma conta com privilégios adequados ao exercício das atividades que aqui executo, a qual deverá ser utilizada somente para tal fim.

Declaro estar ciente de que minhas ações serão monitoradas de acordo com a Política de Segurança da Informação da PREFEITURA e de que qualquer alteração feita sob minha identificação, advinda de minha autenticação e autorização, é de minha responsabilidade.

Estou ciente também de que não deverei proceder com quaisquer instalações de programas e aplicações protegidos por direitos autorais sem o devido licenciamento registrado em nome da PREFEITURA (para os casos de hardware pertencentes a esta) ou à empresa contratada (para os casos de hardware de propriedade de empresa terceirizada e cedidas para utilização no ambiente da PREFEITURA), devendo consultar o DTI sobre os locais de instalação e obter instruções expressas sobre locais de instalação, portas, serviços, etc.

Estou ciente, ainda, de minha responsabilidade pelo dano que possa causar por descumprimento da Política de Segurança da Informação da PREFEITURA ao realizar uma ação de iniciativa própria de tentativa de modificação de configuração, física ou lógica, dos recursos computacionais sem a permissão expressa do Departamento de Tecnologia da Informação. Declaro também, ter o conhecimento de que qualquer operação de alteração de configurações que exijam reinício de aplicativos ou equipamentos deverá ser agendada previamente com o DTI, e, exceto em situações emergenciais, esse agendamento se dará fora do horário de expediente visando minimizar os transtornos gerados pela falta de acesso aos serviços.

Estância Turística de Avaré, _____ de _____ de 20____

_____

Assinatura do Prestador de Serviço

.....