ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DOS DADOS

DISPÕE SOBRE A REGULAMENTAÇÃO DA UTILIZAÇÃO DOS RECURSOS DE INFORMÁTICA E REDES DA PREFEITURA MUNICIPAL DE ESTEIO, VISANDO ESTABELECER UMA POLÍTICA DE SEGURANÇA DOS DADOS, INFORMAÇÕES, PRIVACIDADE E PROTEÇÃO DOS DADOS DA PREFEITURA MUNICIPAL E ENTES DA ADMINISTRAÇÃO INDIRETA.

A Política de Segurança da Informação e Proteção de Dados descreverá as normas de utilização e boas práticas dentro do ambiente de tecnologia da informação e comunicação.

Tendo como objetivo principal, instruir sobre as regras no uso das ferramentas tecnológicas e consequentemente oferecer serviços de forma segura e com a maior disponibilidade possível.

Estas diretrizes também visam proteger informações, sistemas, equipamentos e ativos de rede, sendo estes itens de uso exclusivo da Prefeitura de Esteio.

As normas descritas nesta política podem ser alteradas a qualquer momento, desde que discutidas de forma prévia com as partes envolvidas.

1. Abrangência

Todos os secretários, diretores, empregados, servidores, estagiários, aprendizes, fornecedores e prestadores de serviços, bem como toda pessoa física ou jurídica que, de alguma forma, executem atividades funcionais amparadas por contratos ou instrumentos jurídicos e que, para tanto, venham a utilizar ou ter acesso às informações de propriedade da Prefeitura Municipal, Secretarias Municipais ou entes da Administração Indireta sob sua custódia, em qualquer meio, especialmente, físico ou eletrônico.

2. Aplicação

Aplicam-se estas regras a todos os usuários e terceiros que venham utilizar o ambiente de tecnologia e quaisquer equipamentos da rede interna ou externa, observando-se a legislação aplicável, notadamente a Lei Federal 12.527/2011 e a Lei Complementar 5.231/2011 (Estatuto dos Servidores Municipais).

3. Responsabilidades

As definições de configurações e melhor uso das tecnologias são de responsabilidade da área de Tecnologia da Informação e Comunicação (TIC), sendo também participante fundamental na confecção das políticas em conjunto com as demais áreas.

Também a consideramos a participação da área de gestão de pessoas na colaboração do repasse destas informações na nomeação de servidores para ciência e pleno conhecimento deste documento.

Também terão responsabilidades os gestores, no repasse de informações sobre permissões e no controle destas regras.

Avaliações sobre o uso incorreto ou o não cumprimento destas regras serão discutidas pelos gestores e demais superiores.

3.1 Dos Usuários

- Respeitar esta Política de Segurança da Informação;
- Respeitar a Política de Privacidade e Proteção de Dados Pessoais da Prefeitura Municipal, de forma a garantir a segurança e inviolabilidade dos cidadãos;
- Respeitar todas as normas da LGPD (Lei Geral de Proteção de Dados Pessoais);
- Responder pelo descumprimento dos procedimentos de tratamento de Dados dos Cidadãos, pacientes e alunos previsto na Política de Proteção de Dados Pessoais;
- Responder pela guarda e proteção dos recursos computacionais colocados a sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional, sob a orientação da Tecnologia da Informação e Comunicação (TIC);
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;
- Relatar prontamente à área de TIC qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc;

- Assegurar que as informações e dados de propriedade da Prefeitura Municipal, inclusive, os dados dos cidadãos, pacientes ou alunos não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico;
- Comprometer-se em não auxiliar terceiro ou não provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro;
- Relatar para o seu responsável hierárquico e à Tecnologia da Informação e Comunicação (TIC) o surgimento da necessidade de um novo software para suas atividades;
- Responder pelo prejuízo ou dano que vier a provocar a Prefeitura Municipal ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

3.2 Da Área de Tecnologia da Informação e Comunicação (TIC):

- Configurar os equipamentos e sistemas para cumprir os requerimentos desta Política;
- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
- Restringir a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;
- Garantir segurança do acesso público e manter evidências que permitam a rastreabilidade para auditoria ou investigação;
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;
- Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da Prefeitura Municipal;
- Gerenciar o descarte de informações a pedido dos custodiantes;
- Garantir que as informações de um usuário sejam removidas antes do descarte ou mudança de usuário;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Criar a identidade lógica dos colaboradores na empresa;
- Atribuir contas e senhas identificáveis à pessoa física para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação;
- Proteger todos os ativos de informação da empresa contra códigos maliciosos e ou vírus;
- Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção;
- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da empresa;
- Realizar inspeções periódicas de configurações técnicas e análise de riscos;
- Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais;
- Garantir, assim que solicitado, o bloqueio de acesso de usuários por motivo de desligamento;
- Propor as metodologias de desenvolvimento e processos específicos que visem aumentar a segurança da informação;
- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação;
- Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços;
- Buscar alinhamento com as diretrizes corporativas da Prefeitura e de suas respectivas Secretarias;

- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Monitorar o ambiente de TIC, a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos Prefeitura Municipal, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos e assim por diante); atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do superior hierárquico;
- Realizar, a qualquer tempo, inspeção física nas máquinas sob sua responsabilidade.

4. Definições

4.1 Comitê de Segurança da Informação e Proteção de Dados Pessoais

A criação deste comitê visa deliberar, coordenar, orientar, avaliar e implantar as ações, atividades e projetos relativos à Segurança da Informação na Prefeitura Municipal de Esteio.

4.2 Informação

Conjunto organizado de dados, processados eletronicamente ou não, que podem ser utilizados para produção e transmissão de conhecimento. A informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio pelo qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida.

4.3 Tratamento

Toda operação realizada com qualquer tipo de informação, com dados da Prefeitura Municipal de Esteio ou de terceiros, desde coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

4.4 Segurança da Informação

É a proteção da informação contra vários tipos de ameaças, a fim de garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

4.5 Comitê de Segurança da Informação e Proteção de Dados Pessoais(CSIPD)

Grupo multidisciplinar composto por técnicos de diversas unidades organizacionais da Prefeitura Municipal de Esteio, que atua como ponto central para notificações de incidentes de segurança, provendo a coordenação e o apoio no processo de resposta a incidentes. A indicação de seus membros deve ser feita pelo Comitê de Segurança da Informação e Proteção de Dados Pessoais .

Em sua composição deve necessariamente contar com pelo menos um representante das áreas de Segurança da Informação, Infraestrutura, Negócios, Jurídico e Comunicação, além do Encarregado de Proteção de Dados (DPO) e eventuais indicações da Diretoria. Os membros deverão exercer a função sem prejuízo das suas atribuições e sem gratificação.

4.6 Termo De Responsabilidade Com A Política De Uso Dos Sistemas De Tecnologia

Da Informação Da Prefeitura Municipal De Esteio

O Termo de Responsabilidade é um formulário que tem como objetivo comprovar a ciência do usuário/agente público sobre a Política de Segurança da Informação e de suas respectivas normas de apoio, bem como sobre as regras a serem observadas para acesso aos recursos de Tecnologia da Informação e Comunicação (TIC) e da Rede Corporativa, assim como as informações da Prefeitura sob sua custódia, armazenadas ou registradas em qualquer meio, físico ou eletrônico, visando principalmente à manutenção da integridade, confidencialidade e disponibilidade das informações.

4.7 Termo de Ciência, Responsabilidade e Compromisso Para Empresas Contratadas

Deve ser elaborado um modelo específico de Termo para ser assinado pelos responsáveis legais por empresas contratadas para prestação de serviços no ambiente da Prefeitura, Secretarias Municipais e Administração Indireta ou que precisem ter acesso a informações internas ou confidenciais.

5. Diretrizes

5.1 Princípios

As diretrizes desta política estão apoiadas nos seguintes princípios:

Integridade – É vedada a manipulação das informações, portanto, são proibidas alterações, supressões e adições de conteúdo nas informações, salvo se expressamente autorizadas pela Empresa.

Confidencialidade – Somente pessoas devidamente autorizadas pela Empresa devem ter acesso à informação.

Disponibilidade – A informação deve estar disponível para as pessoas autorizadas, sempre que necessário ou demandado.

Rastreabilidade – Possibilita acompanhar ou identificar o percurso de um dado ou informação durante um processo: saber onde, como, por quem e quando o dado foi manipulado.

5.2 Programas Ilegais

A Prefeitura respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não autorizando o uso de programas não licenciados nos computadores da Prefeitura e nas demais Secretarias. É terminantemente proibido o uso de programas ilegais (sem licenciamento) na Prefeitura e nas suas Secretarias. A instalação de softwares ilegais constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98.

5.3 Proteção da Informação

a) Todas as informações e sistemas de propriedade da Prefeitura Municipal, Secretarias e Administração Indireta ou sob sua custódia devem ser mantidos em locais protegidos.

b) Deve ser mantido sigilo sobre toda e qualquer informação ou dado a que tiver acesso, não se valendo desse privilégio em benefício próprio ou de terceiros, mesmo depois de findo o vínculo contratual.

c) Não é permitido manter acessíveis ou permitir acesso a pessoas não autorizadas, documentos e informações em qualquer tipo de mídia (eletrônica, impressa ou outros).

d) Todos os dados armazenados em banco de dados em produção somente poderão ser reproduzidos com autorização formal, conforme Instrução Normativa vigente.

e) Todo tráfego de informações entre aplicação e banco de dados deve ser criptografado sempre que possível, e esta regra deve ser prevista durante o desenvolvimento das aplicações.

f) Toda informação pertencente à Prefeitura Municipal, Secretarias e Administração Indireta ou sob sua custódia deverá possuir mecanismos de proteção e classificação.

g) A classificação dos dados é sempre realizada pelo proprietário da informação, seja ele interno ou externo, levando-se em consideração o disposto na Lei Federal no 12.527/2011 - Lei de Acesso à Informação (LAI) e Lei Federal no 13.709/2018 - Lei Geral de Proteção aos Dados Pessoais (LGPD).

h) No mesmo sentido, as informações pertencentes à Prefeitura Municipal, Secretarias e Administração Indireta ou sob sua custódia serão classificadas segundo grau de sigilo, a ser tratado em política própria.

i) Toda informação de dados pessoais será tratada de acordo com os princípios legais aplicáveis, em especial a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico.

j) O acesso às bases de dados dos sistemas em produção deve ser realizado somente pelas aplicações de produção ou pelos técnicos responsáveis pela manutenção dos bancos de dados, de acordo com os termos vigentes definidos em Instrução Normativa.

k) Todo acesso físico às dependências da Prefeitura Municipal, Secretarias e Administração Indireta deverá ser previamente autorizado, controlado e monitorado.

l) Para acessar os sistemas da Prefeitura Municipal, Secretarias e Administração Indireta, os usuários devem fazer uso de senhas/credenciais atribuídas para tal finalidade. Toda senha ou credencial de acesso é pessoal e intransferível e não deve ser divulgada e/ou compartilhada com terceiros.

5.4 Antivírus

A Prefeitura Municipal, por intermédio do setor de TIC(Tecnologia da Informação e Comunicação), disponibiliza software corporativo de antivírus instalado para todos os usuários.

O antivírus é atualizado automaticamente na estação de trabalho do usuário sempre que uma nova versão é disponibilizada pelo fabricante através do aplicativo servidor.

O setor de TIC não permite que o usuário remova ou altere as configurações do antivírus a fim de não comprometer a segurança dos dados que o fabricante do software proporciona.

As checagens periódicas do disco rígido (HD) e da estação de trabalho estão programadas para execução periódica automática conforme definições da área de TIC no aplicativo servidor.

5.5 Utilização, guarda e descarte de documentos

Documentos que contenham informações classificadas como uso interno, restrito e confidencial não podem ficar expostos na estação de trabalho, em impressoras, fax, scanner, telas de computadores, áreas comuns, locais de trânsito de pessoas, refeitório e nas salas de reunião. Documentos que contenham informações classificadas como restrita ou confidencial devem ser acondicionados em armários de acesso controlado, sua destruição, quando for o caso, deverá ser feita conforme orientação do Arquivo Municipal.

5.6 CDs e DVDs

Os dispositivos devem ser quebrados após ser considerado inutilizável.

5.7 Discos rígidos, pendrives e outras mídias físicas

Para a eliminação das informações deverá ser utilizado o método de “desmagnetização”.

5.8 Mesa limpa e tela limpa

Essa prática tem como objetivo a redução dos riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente.

A adoção dessa prática “mesas limpas” para os papéis e mídias de armazenamento removível e, igualmente, uma política de “telas limpas”, contra, por exemplo, o perigo de ter um usuário já autenticado/registrado, porém ausente e com sua sessão de trabalho aberta.

A prática de Mesa Limpa/Tela Limpa busca resguardar a Prefeitura Municipal bem como o próprio usuário contra o acesso não autorizado a informações.

Assim, sinteticamente, entre outros:

a) Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidos sempre que possível fora da superfície da mesa (mesa limpa);

b) Informações restritas ou confidenciais devem ser trancadas em local separado (idealmente em um arquivo, armário e gaveteiro) quando não necessárias, especialmente quando o ambiente fica vazio;

c) Computadores e notebooks não devem ser deixados autenticados/ registrados quando não houver um colaborador (operador) junto e devem ser protegidos por senhas e outros controles quando não estiverem em uso. (Tela limpa);

d) Informações restritas ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;

e) Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho;

f) Papéis, livros ou qualquer informação restrita ou confidencial não devem ser deixados na mesa;

g) Um protetor de tela que solicite uma senha para acesso deve ser usado;

h) Todos os documentos e meios eletrônicos no final do dia de trabalho devem ser devidamente guardados/organizados, com proteção adequada;

i) Documentos contendo informações pessoais devem ser mantidos trancados.

5.9 Revogação de acessos

O acesso de usuários desligados da Prefeitura Municipal deverá ser revogado imediatamente no momento da comunicação do desligamento realizado pelo setor Recursos Humanos/Folha de Pagamento.

A revogação de acesso deve ser registrada de modo que seja possível determinar a data da ocorrência, os usuários afetados, assim como os privilégios revogados.

As credenciais de acesso dos usuários que encerraram suas atividades na Prefeitura Municipal não devem ser removidas das bases cadastrais, mas devem ser bloqueadas de forma que não seja possível utilizá-las.

Devem ser mantidos registros que permitam identificar os usuários responsáveis pelas ações realizadas por meio das credenciais de acesso, mesmo depois de bloqueadas.

6. Direitos e Acessos de Usuários

Cada agente público ao iniciar suas atividades na administração pública para poder fazer o uso de equipamentos e sistemas, deverá receber e assinar o Termo de Responsabilidade (Anexo I), assim tendo ciência das Políticas de Segurança da Informação.

É parte fundamental desta política, a colaboração do setor de Gestão de Pessoas e dos gestores de cada área, repassando as informações sobre mudanças no quadro de servidores e os direitos de acesso que o mesmo poderá ter.

A. Ao iniciar o processo de admissão, o setor de Gestão de Pessoas deve incluir em seu processo a tarefa de informar/solicitar os dados para o novo servidor e incluir no sistema.
B. No caso de exoneração, a TIC deverá ser informada o mais breve possível para eventuais restrições e bloqueios.
C. É tarefa dos gestores de cada área informar ao setor de TIC os direitos e níveis de acesso dos servidores aos sistemas e acessos da rede.
D. Acessos a sistemas de gestão e que tenham informações confidenciais, assim como gráficos e relatórios também serão definidos pelos gestores das áreas, e devem ser autorizados de forma registrada via memorando.

E. Terceiros podem utilizar o ambiente, seja para acesso à rede ou WEB, mas devem ser autorizados previamente e de forma temporária, sendo estes acessos revogados depois de período pré-determinado.

Não é permitido a usuários realizarem nenhum tipo de cópia de dados ao serem exonerados da Prefeitura de Esteio, toda e qualquer cópia deve ser informada e solicitada aos setores e deve ser realizada pelo setor de TIC ou pelo próprio usuário, desde que autorizado

7. Uso dos Ativos de TI

Os ativos de TI são todos os computadores, ativos de rede (impressoras, roteadores, switches, computadores) e quaisquer softwares(sistemas) que venham a ser ligados ao ambiente tecnológico.

Assim como o acesso às ferramentas e serviços que estes equipamentos proporcionam, eles são de uso exclusivo em serviço da Prefeitura de Esteio e só podem sofrer alterações do setor de Tecnologia da Informação. Não é permitido nenhuma intervenção de usuários ou terceiros em nenhum destes itens, somente com aviso prévio e acompanhamento do setor de Tecnologia da Informação e Comunicação.

A. Não é permitida a inclusão de equipamentos na rede, sejam eles de forma cabeada ou sem fio, sem o prévio aviso ao setor de TIC.
B. Não é permitida a mudança de equipamentos de local, sem o prévio aviso ao setor de TIC.
C. Não é permitida a instalação de softwares nos equipamentos da Prefeitura de Esteio, caso necessário deve ser solicitado ao setor de TIC.
D. Não é permitido aos agentes públicos do Município realizarem manutenções em nenhum equipamento da Prefeitura de Esteio, seja de software ou hardware.
E. Cópia de dados serão realizados somente no ambiente de Data Center, sejam dados de arquivos, diretórios e sistemas (GRP e E-mails). Estas cópias são direcionadas para armazenamentos controlados pelo setor de TIC e possuem formas e rotinas diversas. Nenhum dado salvo localmente (Nos discos internos de Computadores/Notebooks) pelos usuários é realizado backup. Para qualquer solicitação ou informações é necessário registrar a solicitação ao setor de TIC ao menor sinal de incidentes.

O uso da Internet é para fins de trabalho, apesar de o ambiente informático contar com controles, antivírus e filtros, a navegação de forma segura e responsável também é de responsabilidade do usuário, portanto acessos a sites indevidos se identificados devem ser registrados ao setor de Tecnologia da Informação.

7.1 Uso de impressoras

O uso de impressoras na Prefeitura e nas demais Secretarias deve seguir algumas regras:

1) É proibida a impressão e cópia de documentos de cunho pessoal e/ou ilegal;

2) A configuração e manutenção das impressoras só podem ser realizadas pela Equipe prestadora de Serviços contratada;

3) A instalação das impressoras deverá ser realizada através de abertura/registro de chamados

4) O responsável de cada setor / unidade será o responsável pela forma de utilização da impressora localizada na sala, inclusive para responder a questionamentos como impressões/cópias excessivas;

5) O responsável de cada setor / unidade será o responsável pela forma de utilização da impressora localizada na sala, inclusive para responder a questionamentos como impressões/cópias excessivas;

7.2 Uso das estações de trabalho

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

a) É de responsabilidade do colaborador do equipamento zelar por ele, mantendo-o em boas condições;

b) Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;

c) É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores.
Caso seja necessário, o reparo deverá ser feito pela equipe de suporte do setor de TIC(Tecnologia da Informação e Comunicação);

d) As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas.

e) É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários
finais. Este procedimento só poderá ser realizado pela equipe de suporte do setor de TIC(Tecnologia da Informação e Comunicação); após análise, mediante abertura de chamado;

f) É proibido copiar, modificar, enviar, encaminhar ou receber materiais protegidos por copyright, segredo industrial, sigilo financeiro ou quaisquer outros dispositivos a estes assemelhados, sem a autorização prévia e expressa do titular de direito, i.e, que não possuam licença e/ou não sejam homologados pela equipe da TIC;

g) As estações de trabalho devem permanecer bloqueadas nos períodos de ausência do colaborador;

h) Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre serem armazenados em local próprio no servidor da rede ou armazenamento em nuvem, indicado pelo setor de TIC, o qual possui rotinas de backup e controle de acesso adequado;

i) Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede local ou em armazenamento em nuvem, indicado pelo setor de TIC, nunca no disco local da máquina;

j) É proibido o uso de estações de trabalho para:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede; exceto com pedido do chefe do Executivo.
- Burlar quaisquer sistemas de segurança;
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Acessar ou hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

k) A TIC(Tecnologia da Informação e Comunicação) não se responsabiliza por prestar manutenção ou instalar softwares em computadores pessoais;

l) As estações de trabalho possuem códigos internos, os quais permitem que sejam identificadas na rede. Desta forma, toda informação que for salva ou transmitida pela estação de trabalho é de responsabilidade do agente político, a qual poderá ser acessada pela TIC(Tecnologia da Informação e Comunicação) a pedido do chefe do Executivo ou Secretário Municipais.

7.3 Uso do Correio Eletrônico (e-mail)

O serviço de correio eletrônico (e-mail corporativo) é permitido somente para as atividades profissionais e comunicação com o cidadão/munícipe, não sendo permitido enviar ou arquivar mensagens que não estejam relacionadas às atividades profissionais. O envio, recebimento ou armazenamento de conteúdo ilegal, ofensivo, difamatório, pornográfico ou discriminatório é estritamente proibido.

O uso de ferramentas de correio eletrônico, com exceção do meio disponibilizado pelo setor de Tecnologia da Informação para este fim, fica terminantemente proibido, sob a sujeição de penas impostas pelo presente regulamento.

Recomenda-se que toda mensagem enviada pelo usuário em função, contenha, ao seu final, uma assinatura padrão com: nome completo, cargo, função e telefone para contato.

As contas de e-mail particulares não terão suporte do Setor Tecnologia da Informação e Comunicação da Prefeitura de Esteio.

Qualquer mensagem utilizando o correio eletrônico da Prefeitura, seja seu destino interno ou externo, deve sempre priorizar pelo uso apropriado da ferramenta.

Considera-se uso inapropriado o envio de mensagens de correio eletrônico contendo:

I - materiais obscenos, ilegais ou antiéticos;

II - materiais preconceituosos ou discriminatórios;

III - materiais caluniosos ou difamatórios;

IV - propagandas com objetivos comerciais;

V - listas de endereços eletrônicos dos usuários do correio eletrônico do Tribunal;

VI - vírus ou qualquer programa danoso;

VII - material de natureza político-partidária ou sindical que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e
sindicatos;

VIII - material protegido por leis de propriedade intelectual;

IX - entretenimentos e “correntes”;

X - assuntos ofensivos;

XI - músicas, vídeos ou animações que não sejam de interesse específico do trabalho;

XII - SPAM.

O setor Tecnologia da Informação e Comunicação poderá registrar o envio e recebimento de mensagens eletrônicas no âmbito da Prefeitura, podendo, a qualquer momento, efetuar auditoria, conforme normas vigentes.

Mesmo existindo formas de restringir e eliminar fraudes, vírus e roubo de informações é importante o cuidado do usuário no uso destes serviços, por se tratarem de aplicações restritas aos servidores públicos da Prefeitura de Esteio.

A. O usuário não deve divulgar seus dados de usuário e senha de e-mail ou de serviços e aplicativos a terceiros.
B. O usuário deve ter cuidados ao abrir links de acesso, receber arquivos de remetentes desconhecidos e não encaminhar conteúdo que desconfiar ser malicioso ou de fonte que não seja fidedigna.
C. Estas ferramentas não devem ser utilizadas para disponibilizar conteúdo impróprio (cunho racista, religioso ou pornográfico), nocivo a terceiros ou informações sobre a Prefeitura de Esteio.
D. O usuário deve solicitar apoio técnico ao setor de TIC caso suspeite de acessos indevidos ou tenha dúvidas sobre quaisquer mensagens.

7.4 Uso de aplicativo de mensageria para fins profissionais

Aplicativos de mensagens não são oficiais para a utilização na Prefeitura. São apenas facilitadores para uma comunicação rápida, interna e externa,

7.5 Uso da telefonia móvel e plano de dados corporativos

7.5.1 A Administração Municipal poderá, conforme necessidade, disponibilizar aos servidores públicos, aparelhos de telefonia móvel com linha e ou/plano de dados, ficando o servidor responsável pelo seu uso e guarda, observando as seguintes instruções:

I- O uso do telefone celular corporativo deverá ser exclusivo para assuntos relacionados ao trabalho;

II- Mesmo nas ligações a serviço, o uso deverá ser rápido e objetivo.

7.5.2 A administração municipal poderá verificar, a qualquer tempo, o seu uso, por meio de do Gestor de cada Secretaria/Departamento, que controlará periodicamente a utilização e os limites contratados, sendo que as cotas serão pré-definidas de acordo com a demanda e necessidade de cada usuário incitando todos a contribuírem com a redução de custos.

7.5.3 O servidor público possuidor de um celular com plano corporativo será o responsável pela guarda e posse do bem relacionado, respondendo perante a Administração Municipal e operadora em caso de furto, roubo, extravio ou semelhante, bem como pela má utilização ou qualquer dano causado ao bem, comprometendo-se a ressarcir um equipamento igual ou de valor equivalente, na ocorrência de qualquer um dos eventos referidos.

7.5.4 Os planos corporativos de telefonia serão utilizados de forma estritamente funcional, no período em que exercer suas funções no âmbito do Município de Esteio, obrigando-se a devolvê-lo em condições de uso, nos casos de desligamento ou a pedido da autoridade responsável.

7.5.5 O usuário de telefones funcionais e planos corporativos de telefonia, deverá estar ciente que as ligações de longas distâncias (DDD/DDI) efetuadas nesta linha móvel deverão ser realizadas somente pela operadora com a qual a Prefeitura Municipal de Esteio possui contrato.

7.6 Uso da telefonia fixa corporativa

A. O uso do telefone fixo na Prefeitura Municipal, Secretarias Municipais ou entes da Administração Indireta é de uso exclusivo para execução de suas atividades diárias, sendo vetado o uso para fins próprios.
B. As chamadas telefônicas entre os ramais das diversas unidades, locais ou remotas, são realizadas utilizando a rede IP, portanto sem custos adicionais.
C. Informações sobre as chamadas realizadas contendo data e hora e número chamado são registradas e mantidas por tempo indeterminado.

7.7 Uso de plataformas de vídeo-conferências

O Meet é a plataforma adotada institucionalmente para as atividades síncronas profissionais. Trata-se de um serviço de videoconferência bastante inclusivo e, portanto, versão que temos acesso utilizando as contas de e-mails institucionais (@esteio.rs.gov.br) permitem a criação e a realização das chamadas.

1. Ao criar a sala pelo e-mail institucional garanta que sua Agenda Google não está pública;
2. Combine com os demais participantes o acesso sempre utilizando o email institucional da Prefeitura(@esteio.rs.gov.br), ou seja, não autorize o acesso de pessoas com nomes e/ou e-mails desconhecidos;
3. Ative a gravação da reunião desde o início; para isso, avise/solicite aos participantes;
4. Não torne públicas as salas de videoconferências; evite, portanto, o compartilhamento do endereço (link) da chamada em páginas web ou redes sociais;
5. Pesquise os recursos do Meet para silenciar ou remover um participante.

7.8 Uso de formulários eletrônicos

A ferramenta Google Forms é uma solução prática e eficiente para elaboração de pesquisas, coleta e análise de dados. Entretanto, quando se lida com dados pessoais e dados sensíveis de terceiros (munícipes, servidores públicos, etc...), é necessário que o responsável pela coleta de dados siga uma série de recomendações de uso e boas práticas a fim de evitar que esses dados sejam expostos e tenham uma destinação inadequada.

A Lei Geral de Proteção e Segurança de Dados (Lei 13.709/2018), popularmente conhecida como lei LGPD, regula as atividades de tratamento de dados pessoais e estabelece que deve-se coibir qualquer publicação de dados pessoais sensíveis através da pseudonimização ou sem anonimização (dado anônimo definitivo, sem possibilidade de identificação).

O formulário criado deve estar vinculado a uma conta de e-mail institucional (@esteio.rs.gov.br) e estar de acordo com as diretrizes publicadas na Política de privacidade do Município.

8. Senhas

As senhas são partes fundamentais na segurança do acesso, seja a rede de dados, e-mails ou sistemas. As senhas são de uso pessoal e intransferível, não devem ser divulgadas sem prévia autorização ou solicitação por parte dos superiores e ou titulares de pastas(Secretarias). Qualquer dúvida ou suspeita de vazamento da senha, deve ser comunicado ao setor de TIC para realização de troca da mesma, mediante confirmação de dados de cadastro.

A. Toda senha inicial será criada pelo sistema de forma automática ou pelo setor de Tecnologia da Informação, a partir da solicitação dos superiores, e somente será repassada ao próprio usuário.
B. As senhas deverão ser trocadas periodicamente. Preferencialmente a cada 60 dias, no máximo a cada 90 dias
C. Em caso de esquecimento ou bloqueio da senha, o usuário deve utilizar as ferramentas de cada sistema para troca de senha, caso o sistema não possua esta opção o usuário deverá entrar em contato com o setor de Tecnologia da Informação, via sistema de chamados ou telefone.
D. Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %).
E. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), não devem ser baseadas em informações pessoais, como o próprio nome, familiares, nascimento, endereço, placa de veículo, nome da empresa, e ou não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “123456”, entre outras.

F. Os agentes públicos do setor de TIC não possuem registro das senhas e não possuem formas de saber a senha atual do usuário.
G. A senha é de uso particular e intransferível do usuário.
H. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade será dos usuários que dele se utilizarem. Se for identificada solicitação do gestor para uso compartilhado ele deverá ser responsabilizado.
I. Qualquer ato realizado com o uso da senha pessoal é de responsabilidade do seu devido usuário.

10. Armazenamento Removível/Externos

É restrito o uso de mídias removíveis (pendrives, Smartphones ou HD's externos) a somente locais pré-determinados que necessitem seu uso, demais necessidades de usuários devem ser registradas via Portal de Chamados ao setor de Tecnologia da Informação. O uso de mídias removíveis deve ser tratado como exceção à regra, pois a porta USB(Universal Serial Bus) é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais.

11. Rede Sem Fio (WI-FI)

As redes corporativas sem fio somente serão acessíveis por agentes públicos, equipamentos e setores previamente autorizados pelos responsáveis da respectiva Secretaria.

Redes sem fio consideradas de uso livre, não tem seu acesso e/ou uso sob a responsabilidade da TIC, pois não fazem parte de nossa rede corporativa.

12. Datacenter

Definimos por datacenter todo o ambiente de servidores locais e virtuais, independente dos acessos a estes servidores sejam de forma lógica, física ou remota, obedecem a estas políticas:

A. O acesso físico ao ambiente de servidores é vedado aos técnicos do setor de Tecnologia da Informação ou terceiros em serviço, sendo estes identificados.
B. A mudança física dos servidores é autorizada somente ao setor de Tecnologia da Informação.
C. Terceiros somente podem realizar reparos aos servidores, seja de forma física ou lógica, sendo estes acessos informados.
D. Os acessos lógicos aos servidores, assim como senhas, informações de configurações e serviços, são processos e informações do setor de Tecnologia da Informação, e podem ser requisitados pelos seus gestores.
E. Acessos remotos a serviços obedecem às mesmas regras de utilização interna, e para uso específico de usuários identificados. Estes acessos devem ser solicitados por e-mail, registrando esta solicitação e deferida junto ao setor de Tecnologia da Informação.
F. Acessos remotos a serviços obedecem às mesmas regras de utilização interna, e para uso específico de usuários identificados. Estes acessos devem ser solicitados por e-mail, registrando esta solicitação e deferida junto ao setor de Tecnologia da Informação.

13. Auditoria

As políticas descritas anteriormente devem ser seguidas por todos agentes públicos municipais no uso das ferramentas ou equipamentos, estejam eles na Prefeitura de Esteio ou não. Estas políticas foram elaboradas para o bom uso e o funcionamento correto dos serviços, gerando segurança, confidencialidade e disponibilidade maior ao ambiente.

Por isso, a auditoria das práticas destas políticas será realizada pelo setor de TIC, de forma automática no dia a dia, por meio da coleta de dados, verificações periódicas em equipamentos e serviços utilizados. Também serão realizadas de forma agendadas rotinas de auditoria.

A colaboração dos usuários e gestores também é uma excelente prática de auditoria, visto que a tecnologia sofre atualizações constantes e de forma rápida, sendo assim, informações sobre incidentes ou mau uso de algum equipamento devem ser informados ao setor de TIC o quanto antes, para auxílio na resolução e otimização dos processos ou procedimentos a serem realizados.

14. Notificação de falhas e incidentes de segurança da informação e mau funcionamento

Devem ser estabelecidos procedimentos formais para a notificação de falhas e incidentes de segurança da informação e mau funcionamento de equipamentos ou aplicativos, bem como procedimentos de resposta a incidentes.

A inobservância das proibições acima indicadas poderá implicar em aplicação de medidas disciplinares, sanções contratuais ou mesmo rescisão do contrato vigente, além de responder administrativa, civil e criminalmente pelos prejuízos causados à Administração Municipal ou às Secretarias.

15. Segurança em pessoas

15.1 Novos Colaboradores, estagiários e prestadores de serviço

As responsabilidades de segurança da informação devem ser atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a permanência.

Todos que utilizam os ativos devem obedecer às regras de segurança da informação contidas neste Decreto e nas Normativas indicadas pelo setor de TIC.

15.2 Treinamento dos usuários

Deve ser elaborada uma política de capacitação em segurança da informação para usuários com o objetivo de assegurar que estejam cientes das ameaças e preocupações de segurança da informação e equipados para apoiar a política de segurança da instituição durante a execução normal do seu trabalho.

16. Adequações à Lei Geral de Proteção de Dados

Permitir que os dados sejam disponibilizados em formato interoperável para compartilhamento com outros órgãos públicos, quando isso for necessário para políticas e serviços públicos, descentralização da atividade pública, e para a disseminação e o acesso das informações pela sociedade.

Possibilitar a adaptação e revisão dos procedimentos e formulários, habilitando meios digitais, para atender ao cidadão, em demandas de solicitação e revogação do consentimento e outras mais sobre como seus dados estão sendo tratados.
Visando um maior controle e segurança dos dados, é solicitado que os dados pessoais sejam armazenados apenas em território nacional, assim como os servidores(nuvem).

17. Cláusulas obrigatórias em contratos com terceiros

a) Cláusulas de submissão à Política e Normas de Segurança da Informação.

Deve constar das propostas e/ou contratos com fornecedores e prestadores de serviços, cláusula de conformidade com a Política e Normas de Segurança da Informação.

b) Cláusulas de sigilo, proteção e contra espionagem.

Em todo contrato firmado com terceiros deverão constar cláusulas para proteção das informações da Prefeitura de Esteio - e das informações sob sua custódia - de forma padronizada, a fim de garantir que todos os softwares e hardwares fornecidos serão livres de programas de espionagem (backdoors).

c)Todos os contratos com terceiros deverão conter cláusulas referentes à proteção de dados pessoais, estabelecendo deveres e obrigações envolvendo a temática, e atestando o compromisso dos terceiros com as legislações de proteção de dados pessoais aplicáveis. Destaca-se, ainda, que as empresas contratadas que tratam dados pessoais sob as instruções da Prefeitura Municipal, estão sujeitas às obrigações impostas aos Operadores de acordo com a LGPD.

d)Todos os fornecedores e terceiros devem assinar o termo de aceite dessa Política, se aplicável, submetendo as atividades contratadas no âmbito da relação com a Prefeitura Municipal também a essas normativas.

18. Penalidades

As violações das Diretrizes, Normas ou Procedimentos, que juntas formam a Política de Segurança da Informação e Comunicação desta instituição, resultarão em sansões não só disciplinares, mas também cíveis e penais, tendo em vista que atos ilícitos praticados em desacordo com essa política podem ter também sanções definidas na legislação brasileira, como é o caso, por exemplo, da Lei no 9.610/98 (lei de proteção aos direitos autorais); dos artigos 153, §1o-A (divulgação de segredo), 154-A (Invasão de dispositivo informático), 168 (apropriação indébita), 266 (Interrupção ou perturbação de serviço informático), 313-A (inserção de dados falsos em sistemas de informação) e 313-B (modificação ou alteração não autorizada de sistema de informação), do Código Penal Brasileiro; e do art. 927 (ato ilícito e reparação de dano) do Código Civil Brasileiro de 2002.

As sanções disciplinares deverão ser previstas em documento normativo específico aprovado pelo Comitê de Segurança da Informação e Proteção de Dados Pessoais. Os casos não previstos deverão ser avaliados individualmente pelo mesmo Comitê.

Esteio, 04 de Agosto de 2023

LILIAN TERESINHA MARTINY HAIGERT
Secretária Municipal de Governança e Gestão

RAFAEL ANDRADE DOS SANTOS
Coordenador de TIC

15. TERMOS E DEFINIÇÕES

Agente público: Considera-se o agente político, o servidor público e todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública.
Ambiente Tecnológico: Compreende todos os sistemas, computadores e redes da Prefeitura.
Ameaça: qualquer fator ou ação capaz de interferir e causar danos à integridade, à confidencialidade, à autenticidade e à disponibilidades de dados e informações.
Antivírus: Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, assim como impede sua instalação e propagação.
Aplicativos de comunicação: Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de Whatsapp, Telegram, Skype etc.
Armazenamento em nuvem: é um serviço que permite armazenar dados ao transferi-los pela Internet ou por outra rede a um sistema de armazenamento externo mantido por terceiros.
Ativo: Qualquer coisa que tenha valor para a Prefeitura e precisa ser adequadamente protegida.
Ativo de informação: Podem ser tangíveis ou intangíveis. Ativos tangíveis são ativos físicos, como documentos em papel, servidores, discos rígidos, laptops, profissionais qualificados, dentre outros. Já os ativos intangíveis, são os ativos não físicos, como dados armazenados em computadores e banco de dados, arquivos de dados, informações pessoais, arquivos de áudio, imagens e vídeos digitalizados, dentre outros.
Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
E-mail corporativo: sistema de mensagens pertencente ao domínio @esteio.rs.gov.br e utilizado para criar, encaminhar, responder, transmitir, arquivar, manter, copiar, ler ou imprimir informações, com o propósito de estabelecer comunicações, entre os setores/departamentos, Secretarias, Administração indireta entre pessoas e entre grupo de pessoas.
E-mail particular: todo email que não está vinculado ao domínio @esteio.rs.gov.br .
Firewall: Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
Hardware: conjunto dos componentes físicos (material eletrônico, placas, monitor, equipamentos periféricos etc.) de um computador.
Informação: Conjunto de dados e conhecimentos organizados, que possam constituir referências sobre um determinado acontecimento, fato ou fenômeno.
Log: Registro de eventos em um sistema de computadores.
Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.
Perfil de Acesso: Grupo de acessos a um recurso tecnológico estratificado por função dentro da Prefeitura.
Proxy: Em redes de computadores, um proxy é um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.
Sites de proxy: Sites utilizados para acessar outros sites da web. Em redes corporativas que têm monitoramento ou bloqueio de sites, sites de proxy permitem a navegação anônima a sites proibidos.
Servidor: é um software ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, chamada de cliente.

Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores.
SPAM: Mensagem de e-mail publicada em massa com fins publicitários.
TIC: Tecnologia da Informação e Comunicação.
USB(Universal Serial Bus): É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.
VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por colaboradores autorizados em trânsito.
Wi-Fi: Abreviação de Wireless Fidelity - é uma tecnologia de comunicação que não faz uso de cabos e, geralmente, é transmitida através de frequências de rádio, infravermelhos etc.

Referências legais e normativas

- **Lei Federal 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)**

Dispõe sobre a proteção de dados pessoais;

- **Lei Federal 12.737 de 30 de novembro de 2012**

Tipifica crimes de delitos informáticos;

- **Lei Federal 12.965 de 23 de abril de 2014**

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil(Marco Civil da Internet);

- **Lei Federal 9.609 de 19 de fevereiro de 1998**

Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências;

- **Lei Federal 12.527 de 18 de novembro de 2011**

Lei de acesso à informação;

- **Norma ABNT NBR ISO/IEC 27001:2013**

Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos;

- **Norma ABNT NBR ISO/IEC 27002:2013**

Tecnologia da Informação – Técnicas de Segurança – Código de Prática e Controles de Segurança da Informação;

- **Norma ABNT NBR ISO/IEC 27005:2023**

Tecnologia da Informação – Gerenciamento de riscos à segurança da informação;

- **Norma ABNT NBR ISO/IEC 22313:2020**

Sistema de Gestão de Continuidade de Negócios.