

PSI – Política de Segurança da Informação

Documentos de Diretrizes e Normas

A Política de Segurança da Informação (PSI), orienta e estabelece as diretrizes e Normas Administrativas para a proteção dos ativos de Informação e a prevenção de responsabilidade legal para todos os usuários e funcionários da Prefeitura Municipal de Florínea. Portanto deverá ser cumprida e aplicado em todos setores da Administração Pública.

PSI – Política de Segurança da Informação está baseada nas recomendações propostas pela norma ABNT NBR ISSO 27002:2005/IEC, LGPD Lei Federal 13709/2018, Lei Governo Digital 14129/2021 e Lei de Acesso à Informação (LAI) 12527/2011, se ajustando com código de prática para a gestão da segurança da informação e está de acordo com outras leis vigentes em nosso país.

Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao uso do órgão público, visando a orientação de nossos usuários e funcionários para a utilização dos ativos de tecnologia da informação disponibilizados em suas tarefas. O mesmo encontra-se disponíveis no site da Prefeitura Municipal de Florínea (<https://www.florinea.sp.gov.br/plano-municipal>).



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



OBJETIVOS.....	3
DIREITOS.....	3
REQUISITOS.....	4
DAS RESPONSABILIDADES ESPECÍFICAS.....	5
1 - Dos Funcionários em Geral.....	5
2 - Dos Gestores de Pessoas ou Processos.....	5
3 - Dos Custos diante da Informação.....	5
3.1 - Da Área de Tecnologia da Informação.....	5
3.1.1 - Das Secretárias e Diretorias.....	7
4 - Monitoramento de Rede.....	7
5 - Correio Eletrônico.....	8
6 – Internet.....	9
7 – Identificação.....	11
8 - Computadores e Recursos Tecnológicos.....	12
9 - Dispositivos Móveis.....	14
10 - Datacenter e Servidores.....	15
11 - Monitoramento de Segurança.....	16
12 - Sistemas de Ponto Eletrônico.....	17
13 – Backup.....	17
14 – Anexos.....	17
14.1 Anexo I.....	17
14.2 Anexo II.....	19
DAS DISPOSIÇÕES FINAIS.....	20



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



OBJETIVOS

Estabelecer diretrizes que permitam aos usuários e funcionários seguirem padrões de comportamento relacionados à segurança da informação adequando- se às necessidades da Administração Municipal, proteção legal de dados, equipamentos da Prefeitura Municipal de Florínea e os direitos do cidadão.

Estabelecer a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento em pleno âmbito.

Preservar as informações da administração Municipal e Cidadãos quanto a:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

DIREITOS

Toda informação produzida ou recebida pelos usuários e funcionários como resultado da atividade profissional, artísticas, educacionais e administrativas pertencem à Prefeitura Municipal de Florínea em seu âmbito. As exceções devem ser explícitas e formalizadas em contrato ou documento formal a Administração Municipal.

Os equipamentos de informática, comunicação, áudio, segurança, sistemas e informações que são utilizados pelos funcionários para a realização das atividades profissionais pertencem a Administração Municipal. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços, assim o responsável do setor deve avaliar este uso, ficando de responsabilidade do usuário qualquer dano causado ao patrimônio público e a sua responsabilidade conforme lei.

A Administração Municipal e o setor responsável poderão registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



REQUISITOS

Para a uniformidade da informação, a Política de Segurança da Informação (PSI) deverá ser comunicada a todos os Usuários e Funcionários da Prefeitura a fim de que a política seja cumprida dentro e fora dos Órgãos Públicos.

Tanto a Política de Segurança da Informação (PSI) quanto as normas poderão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação de funcionários. Todos os funcionários e prestadores de serviço (efetivos, temporários, prestadores de serviços, pessoa física ou jurídica), devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos equipamentos disponíveis, a fim de reduzir possíveis riscos. Eles devem assinar o Termo de Responsabilidade (Anexo I) e Termo de Confidencialidade (Anexo II).

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Setor de TI e, se julgar necessário, deverá encaminhar posteriormente ao responsável superior.

Poderão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades digitais, em todos os pontos e sistemas em que o órgão público julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, acessos à internet (WIFIs), correio eletrônico, sistemas comerciais e financeiros desenvolvidos pela Prefeitura ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A Prefeitura Municipal de Florínea exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus usuários e funcionários, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta Política de Segurança da Informação (PSI) será implementada por meio de procedimentos específicos, obrigatórios para todos os funcionários, independentemente do nível hierárquico ou função no órgão público, bem como de vínculo empregatício ou prestação de serviço.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



O não cumprimento dos requisitos previstos nesta Política de Segurança da Informação (PSI), acarretará violação às regras internas administrativas e sujeitará o usuário ou funcionários às medidas administrativas legais cabíveis.

DAS RESPONSABILIDADES ESPECÍFICAS

1 - Dos Funcionários em Geral

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

2 - Dos Gestores de Pessoas ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os funcionários sob a sua gestão.

Exigir a assinatura do Termo de Responsabilidade e Confidencialidade por todos os funcionários e prestadores de serviços com vínculo de qualquer natureza. Ao assinar, o indivíduo assume o dever de seguir as normas estabelecidas e cumprir integralmente a Política de Segurança da Informação (PSI). Este compromisso inclui manter o sigilo sobre todos os ativos de informação da Prefeitura, mesmo após o término do vínculo (desligamento ou rescisão contratual).

3 - Dos Custos diante da Informação

3.1 - Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos funcionários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança da Informação (PSI).



Selo Município
Amigo da Família



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



Os administradores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, troca de arquivos entre setores a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente Cloud (Computação em nuvem), fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Manter cópia de todos os backups de sistemas, software e banco de dados em local predeterminado sobre guarda da administração Municipal.

O Setor de TI deve ser previamente informado sobre o fim do prazo de contratos de serviços de informação, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo prestador.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irreversível antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas administrativas.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação e internet a um responsável identificável como pessoa física, sendo que:

Os dados de acesso (logins) individuais de funcionários ou terceiros serão de responsabilidade do próprio funcionário.

Proteger continuamente todos os ativos de informação da Administração Pública contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de uso após estarem livres de código malicioso e outras ameaças relacionadas.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente administrativo.

Garantir que todos os equipamentos com acesso à rede de internet, bem como os ambientes de rede e demais sistemas, operem sincronizados ao horário de Brasília.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



Monitorar o ambiente de TI para gerar indicadores e históricos de:

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos;
- Períodos de indisponibilidade no acesso à internet e aos sistemas;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos);
- Atividade de todos os Funcionários durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);
- A permissão de acesso a redes Wifi e locais, fica de responsabilidade do setor de TI bem como, o fornecimento de senhas de acesso à internet e uso dos equipamentos de tecnologia de informação.

3.1.1 Das Secretárias e Diretorias

As Secretarias e Diretorias se responsabilizam pelo uso correto, manuseio, guarda de assinatura, certificados digitais e equipamentos específicos disponíveis para execução de suas atividades.

Garantir, de forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Prefeitura, incidente, investigação ou outra situação que exija medida restritiva para fins de proteger informações inerentes a Administração pública.

4 - Monitoramento de Rede

Para garantir o cumprimento das regras mencionadas na Política de Segurança da Informação (PSI), a Prefeitura poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação da Administração pública ou órgão de Controle Externo.



Selo Município
Amigo da Família



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção preventivos, para garantir a segurança das informações de posse da Administração Pública.

5 - Correio Eletrônico

O uso do correio eletrônico da Prefeitura é para fins corporativos e relacionados às atividades do funcionário ou usuário dentro da Administração Pública. A utilização desse serviço para fins pessoais é proibida a qualquer usuário.

Acrescentamos que é proibido aos usuários e funcionários o uso do correio eletrônico da Prefeitura nas seguintes hipóteses:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente ou a Prefeitura vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo ou informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens de correio eletrônico quando qualquer uma das unidades da Prefeitura estiver sujeita a algum tipo de investigação.
- Enviar ameaças eletrônicas, como: vírus, spyware, ou qualquer outro tipo de software malicioso que possa infectar outros dispositivos;
- Enviar arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Visar obter acesso não autorizado a outro computador, servidor ou rede;



- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Tenha conteúdo considerado impróprio, ilegal ou de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, preconceituoso, entre outros;
- Tenha fins políticos locais ou do país (propaganda política);
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir dados com o seguinte formato:

- Nome do colaborador
- Gerência ou departamento
- Nome da Prefeitura
- Telefone (s)

6 - Internet

Todas as regras atuais da Prefeitura visam basicamente o desenvolvimento de um comportamento ético e profissional quanto a utilização dos recursos disponíveis. Embora a conexão direta e permanente da rede corporativa da Administração Pública com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação acessada, transmitida, recebida ou produzida utilizando os recursos de internet da Prefeitura está sujeita a monitoramento e auditoria, pois a instituição,



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



em total conformidade legal, reserva-se o direito de registrar e analisar todos os acessos ocorridos para garantir a segurança e a integridade de seus sistemas

Os equipamentos, tecnologias e serviços fornecidos 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 e internet, estejam eles em disco local, na estação, em áreas privadas da rede ou em nuvem visando assegurar o cumprimento de sua Política de Segurança da Informação.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer funcionário, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao funcionário e ao respectivo gestor da pasta. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a administração cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela Administração Pública aos seus funcionários, independentemente de sua relação contratual, poderá ser utilizada para fins pessoais, desde que seja autorizada, não prejudique o andamento dos trabalhos nas unidades e tarefas diárias.

Como é do interesse da Prefeitura que seus funcionários estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com suas respectivas funções.

Apenas os funcionários autorizados pela administração poderão copiar, receber, imprimir ou enviar documentos para terceiros, devendo atender, à Lei de Direitos Autorais e demais dispositivos legais.

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

Os funcionários com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades na Prefeitura e deverão providenciar sua instalação e demais procedimentos necessários para o correto funcionamento ao Setor de TI, desde que autorizados pela Administração Pública.

O uso, instalação, cópia ou distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

Qualquer software não autorizado baixado será excluído pelo Setor de TI, e seu superior informado da irregularidade.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



Os funcionários não poderão em hipótese alguma utilizar os recursos da Prefeitura para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias mediante solicitação e aprovação do setor responsável. O uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza relacionada às atividades educacionais e de desenvolvimento pedagógico.

Como regra geral, materiais de cunho sexual não poderão ser acessados, armazenados, distribuídos, editados, impressos e gravados por qualquer meio ou recurso disponível ao usuário.

Funcionários com acesso à internet não poderão efetuar upload (postagem) de qualquer software ou documento, licenciado a Prefeitura ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização da Administração Pública.

É proibido aos funcionários utilizar os recursos da Prefeitura para disseminar vírus, worms, cavalos de troia, spam, ou qualquer outro tipo de software malicioso que cause assédio, perturbação ou permita o controle de outros dispositivos.

O acesso a softwares peer-to-peer (P2P) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a usuários específicos quando necessários para o desenvolvimento de suas atividades.

O uso de serviços de comunicação instantânea (Facebook, WhatsApp e outros) é permitido apenas se for estritamente necessário para o trabalho ou se houver autorização da Administração Pública. Em ambos os casos, a liberação do acesso deve ser informada por um superior ao Setor de TI.

Não é permitido acesso a sites de proxy que não seja certificado com o Setor de TI.

7 - Identificação

Os dispositivos de identificação e senhas protegem a identidade dos usuários e funcionários, evitando e prevenindo que uma pessoa se faça passar por outra utilizando equipamentos da Prefeitura.

O uso de dispositivos ou senhas de identificação de outra pessoa é considerado um crime de falsa identidade, conforme o artigo 307 do Código Penal Brasileiro. Essa norma tem o objetivo de estabelecer critérios claros de responsabilidade sobre o uso dos equipamentos de Tecnologia, e deve ser aplicada a todos os usuários e funcionários



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



Todos os dispositivos de identificação utilizados na Prefeitura, como o número de registro dos funcionários, crachá, identificações de acesso aos sistemas, certificados, assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação vigente (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

É proibido o compartilhamento de login para funções de administração de sistemas.

O Setor de TI fica responsável pela criação de dados de acesso a sistemas, computadores e internet dos colaboradores na Administração Municipal.

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.

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.

Caso um usuário tenha alguma senha de utilização bloqueada, o mesmo deverá entrar em contato com o Setor de TI ou superior de seu departamento para providenciar medidas necessárias de correção para correta utilização.

Se o usuário suspeitar de acesso indevido a um sistema ou dado sob sua responsabilidade, o mesmo deve primeiramente alterar suas senhas. Caso não consiga fazer a alteração, deverá entrar em contato com o Setor de TI.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for desligado permanente de suas atividades por qualquer ocasião, o Setor de Recursos Humanos deverá imediatamente comunicar tal fato ao Setor de TI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado.

8 - Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos Funcionários são de propriedade da Prefeitura, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da administração municipal, bem como cumprir as recomendações constantes nos procedimentos operacionais contidos nessa PSI.



Selo Município
Amigo da Família



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



É proibido todo procedimento de manutenção, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico Setor de TI, ou de quem este determinar.

Os setores que necessitarem fazer testes deverão solicitá-los previamente ao Setor de TI.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor do sistema.

Os sistemas e computadores devem ter versões do software antivírus instalados, e atualizados permanentemente. O usuário, em caso de suspeita de vírus ou problemas de uso, deverá comunicar o Setor de TI mediante registro de chamado por e-mail ou outro meio formal disponível afim de solucionar o ocorrido.

A transferência ou a divulgação de qualquer software, programa ou instrução de computador para terceiros, por qualquer meio (físico ou digital), somente será permitida após a devida identificação do solicitante, verificação da real necessidade do destinatário, conformidade com a classificação da informação, autorização do superior imediato, solicitação judicial ou por órgãos de controle externo.

Arquivos pessoais ou não pertinentes a administração pública (fotos, músicas, vídeos, etc..) não deverão ser copiados e movidos para os drives de rede ou em cloud, pois podem sobrecarregar o armazenamento dos servidores. Caso identificada a existência desses arquivos, os mesmos poderão ser excluídos definitivamente sem que haja comunicação prévia ao usuário

Documentos imprescindíveis para as atividades dos funcionários da Prefeitura deverão ser salvos em drives de backups. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os funcionários da Prefeitura ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do Setor de TI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Todos os computadores de uso individual deverão ter senha para restringir o acesso de colaboradores não autorizados. Tais senhas serão enviadas pelo Setor de TI quando solicitadas, que terá acesso a elas para manutenção dos equipamentos.
- Os colaboradores devem informar ao Setor de TI qualquer identificação de dispositivo estranho conectado ao seu computador.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de Informática e tecnologia para qualquer tipo de reparo que não seja realizado por um técnico do Setor de TI ou por terceiros devidamente contratados para execução do serviço.
- O Funcionário deverá manter a configuração do equipamento disponibilizado pela Prefeitura, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da Administração Pública, assumindo a responsabilidade do uso do equipamento disponibilizado.
- Todos os recursos tecnológicos adquiridos pela Prefeitura devem ter imediatamente suas senhas padrões (default) alteradas.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Prefeitura, a saber:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário e administração pública.
- Vigiatar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers) sem ser para uso de registro e pela administração Municipal.
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação, supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular.
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

9 - Dispositivos Móveis

Estende-se como dispositivo móvel aparelhos como, Tablets, Smartphones, Notebooks, Netbooks e qualquer outro equipamento de uso portátil.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os usuários e funcionários que utilizem tais equipamentos.

A Prefeitura, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar manutenções de segurança.

O Funcionário, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo direto ou indireto, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo funcionário deverá em necessidade de ausência, efetuar o bloqueio do uso do dispositivo móvel concedido à execução de suas atividades.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, sem a devida comunicação e a autorização da área responsável e auxílio ou presença de um técnico do Setor de TI.

O funcionário deverá responsabilizar-se em não manter ou utilizar quaisquer programas ou aplicativos que não tenham sido instalados ou autorizados por um técnico do Setor de TI.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela administração pública constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

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

O Funcionário deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros.

O Funcionário que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios para utilização durante suas atividades na Prefeitura e outros setores da instituição, deverá submeter previamente tais equipamentos ao processo de autorização da Administração juntamente com o setor de TI.

10 - Datacenter e Servidores



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



Para agilizar a resolução de problemas, uma cópia da chave da sala que abriga o servidor e demais equipamentos de informática deverá permanecer sob a guarda do responsável pelo Setor de TI.

O responsável pelo Setor de TI poderá autorizar e acompanhar a entrada de técnicos externos, prestadores de serviço ou demais colaboradores quando necessário, desde que devidamente identificados e justificados.

O responsável pelo setor de TI terá acesso total às dependências, equipamentos, sistemas e documentos relacionados à área, garantindo a manutenção, segurança e o pleno funcionamento dos serviços.

É proibido a entrada de pessoas portando qualquer tipo de alimentos ou bebidas na sala do servidor, a fim de prevenir riscos acidentais que possam danificar qualquer equipamento presente no local.

11 - Monitoramento de Segurança

Para garantir o cumprimento das regras definidas na Política de Segurança da Informação (PSI), a Prefeitura poderá:

- Implantar sistemas de monitoramento como câmeras, alarmes e outros dispositivos, visando a segurança dos patrimônios públicos e segurança interna de seus imóveis e funcionários.
- Os dados gerados por esses sistemas poderão ser utilizados para identificação de usuários e visitantes durante seus acessos a prédios e setores públicos.
- A Prefeitura poderá tornar públicas as informações obtidas pelos sistemas de monitoramento, no caso de exigência judicial.
- As imagens geradas poderão ser utilizadas como provas para comprovação de atos gerados dentro ou fora dos ambientes monitorados em fatos que constituam algum tipo de crime previsto na legislação atual vigente.
- Qualquer solicitação para fornecimento de imagens deverá conter identificação do solicitante, data, hora de referências e o fato ocorrido para busca das mesmas.
- Realizar a qualquer tempo, inspeção física nos equipamentos de sua propriedade.
- Instalar sistemas de proteção preventivos para garantir a segurança das informações e dos perímetros de acesso monitorados.
- O acesso a Central de Monitoramento por terceiros, somente poderá ser realizado com acompanhamento de funcionários autorizados.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



12 - Sistemas de Ponto Eletrônico

Para garantir a Política de Segurança da Informação (PSI), a Prefeitura poderá:

- Implantar sistemas de Ponto Eletrônico, para coleta e monitoramento das atividades desenvolvidas por seus funcionários.
- A informação gerada por esses sistemas poderá ser usada para identificar funcionários em respectivo controle de frequência no trabalho.
- As informações obtidas pelos sistemas de ponto Eletrônico, somente poderão ser fornecidas a terceiros em casos de exigência judicial ou solicitação por órgãos de controle externo.

13 - Backup

Todos os backups devem ser realizados preferencialmente por sistemas de agendamento automatizado fora do horário comercial.

- Os Funcionários responsáveis pela gestão dos sistemas de backup deverão realizar cópias frequentes.
- A Administração deverá fornecer os recursos necessários ao Setor de TI para que sejam armazenados de forma segura os backups dos sistemas atualmente em uso afim de garantir o correto funcionamento dos mesmos.
- Os backups poderão ser realizados em nuvem (cloud) ou dispositivos físicos. Em caso de backup em dispositivos físicos, os mesmos deverão estar em locais separados dos aparelhos geradores de tais cópias. Essas medidas se fazem necessárias para fornecer mais segurança aos dados gerados.

14 – ANEXOS

14.1 – Anexo I

Termo de Responsabilidade PSI



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



Eu, _____,
portador do RG nº _____ e do CPF nº _____,
declaro, para todos os fins de direito, ter lido e compreendido a ****Política de Segurança da Informação (PSI)** da Prefeitura Municipal de Florínea, disponível no site da Prefeitura no endereço <https://www.florinea.sp.gov.br/plano-municipal>.

Por este termo, concordo e me comprometo a cumprir integralmente todas as diretrizes, normas e procedimentos estabelecidos para a proteção dos ativos de informação da Administração Municipal, em conformidade com as leis vigentes, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD) e o conteúdo presente na Política de Segurança da Informação (PSI), disponível no site da Prefeitura de Florínea no seguinte endereço; <https://www.florinea.sp.gov.br/plano-municipal>.

Estou ciente de que a Prefeitura Municipal de Florínea, como proprietária dos equipamentos, sistemas e informações, pode monitorar e auditar todas as minhas atividades na rede, sistemas, correio eletrônico e outros dispositivos, visando garantir a segurança e a disponibilidade das informações.

Comprometo-me a seguir as seguintes responsabilidades, entre outras previstas na PSI:

Utilizar os equipamentos de informática e comunicação, bem como os sistemas e informações, exclusivamente para fins profissionais e relacionados às minhas atividades na Prefeitura Municipal, conforme as normas estabelecidas.

Proteger minha identidade e senhas, que são de minha responsabilidade exclusiva, e não as compartilhar com nenhuma outra pessoa.

Comunicar imediatamente ao setor de Tecnologia da Informação (TI) qualquer incidente que possa afetar a segurança da informação.

Não realizar qualquer procedimento de manutenção, instalação ou modificação nos equipamentos sem a autorização e o acompanhamento de um técnico de TI.

Não utilizar os recursos da Prefeitura Municipal para atividades ilícitas, como a obtenção de acesso não autorizado, a violação de direitos autorais ou a disseminação de material impróprio, sob pena de sanções administrativas, civis e criminais.

Reconheço que qualquer prejuízo ou dano causado à Prefeitura ou a terceiros em decorrência do não cumprimento das diretrizes e normas será de minha inteira responsabilidade. Além disso, estou ciente de que o não cumprimento dos requisitos da PSI poderá resultar em medidas administrativas e legais cabíveis.

Comprometo-me a manter a confidencialidade de todas as informações da Prefeitura, mesmo após o término do meu vínculo de trabalho.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



Florínea, _____ de _____ de _____.

Nome do funcionário

14.2 – Anexo II

Termo de Confidencialidade

Eu, _____,
portador do RG nº _____ e do CPF nº _____,
declaro que, em razão da minha função ou prestação de
serviços na Prefeitura Municipal de Florínea, tenho ou terei acesso a informações confidenciais,
proprietárias e estratégicas da Administração Pública e dos cidadãos.

Por este termo, comprometo-me a manter total sigilo e a não utilizar, revelar ou
divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de
terceiros, qualquer informação, confidencial ou não, da qual eu venha a ter conhecimento,
respeitando além deste, todo conteúdo disponível na Política de Segurança da Informação (PSI)
disponível no site da Prefeitura de Florínea no seguinte endereço;
<https://www.florinea.sp.gov.br/plano-municipal>.

Minhas obrigações de confidencialidade incluem, mas não se limitam a:

- 1 - Manter o sigilo sobre todos os ativos de informações da Prefeitura, mesmo após o meu desligamento.
- 2 - Não divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem permissão expressa e formal.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024



3 - Não fazer upload de qualquer software ou documento licenciado da Prefeitura, nem de dados de sua propriedade, para terceiros, sem autorização do responsável.

4 - Não reproduzir ou compartilhar indevidamente informações da área administrativa em listas de discussão, sites, comunidades de relacionamento ou qualquer outro meio de comunicação digital ou não.

Estou ciente de que a utilização dos recursos tecnológicos para acessar informações confidenciais sem a autorização explícita do proprietário e da Administração Pública é proibida. A violação deste termo pode acarretar em medidas administrativas e legais cabíveis, podendo a Administração Municipal cooperar ativamente com as autoridades competentes em casos de uso ilícito.

Florínea, _____ de _____ de _____.

Nome _____

DAS DISPOSIÇÕES FINAIS

É essencial que a segurança seja vista como parte intrínseca da cultura da Prefeitura, da mesma forma que a ética. Um incidente de segurança não é apenas uma falha técnica; ele sugere uma ação contrária à ética e aos bons costumes que regem a Administração Municipal.



PRÊMIO
PREFEITO AMIGO
DA CRIANÇA
GESTÃO 2021 - 2024

