PORTARIA Nº 026/2020 - IPREF

Institui e disciplina a Política de Segurança da Informação do Instituto de Previdência dos Funcionários Públicos Municipais de Guarulhos

O Presidente do Instituto de Previdência dos Funcionários Públicos Municipais de Guarulhos, **Eduardo Augusto Reichert**, no uso de suas atribuições legais, considerando o que lhe é facultado pelo artigo 11, inciso X, da Lei nº 6.056, de 24 de fevereiro de 2005;

Considerando a necessidade de regulamentar a Política de Segurança da Informação no âmbito do Instituto de Previdência dos Funcionários Públicos Municipais de Guarulhos;

Embasado no disposto pelo caput do artigo 1º do decreto municipal nº 27.168 de 14 de janeiro de 2010, que regulamentou a Lei 6.065/2005, que estabelece, entre outros, *a obrigatoriedade de atendimento a padronização e uniformização das tecnologias da informação e telecomunicação de todos os órgãos e entidades da administração direta e na administração indireta*;

Atendendo ao estabelecido pelo decreto municipal 36.140, de 15 de agosto de 2019, que regulamenta no âmbito do Poder Executivo Municipal a Lei Federal, nº 12.527, de 18 de novembro de 2011, estabelecendo procedimentos e outras providências correlatas para garantir o direito de acesso à informação, conforme especifica;

Atendendo, ainda, ao que preceitua a Legislação Federal ordenado pela Lei 13.709, de 14 de agosto de 2018, e a Lei nº 13.853, de 08 de julho de 2019;

Considerando a importância em minimizar riscos e diminuir a vulnerabilidade dos sistemas de dados no Instituto de Previdência dos Servidores Públicos Municipais de Guarulhos- IPREF;

Considerando que o Instituto busca disponibilizar para seus servidores e segurados, soluções sistêmicas corporativas com dados íntegros e integrados, definindo e implantando hardware e software, para garantir a disponibilidade e qualidade da infraestrutura tecnológica; e,

Atendendo ao estabelecido pela adesão do Instituto de Previdência dos Funcionários Públicos Municipais de Guarulhos – IPREF ao Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios “Programa Pró-Gestão”;

RESOLVE:

Art. 1º Estabelecer a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IPREF** aplicável aos servidores diretos e indiretos do IPREF, beneficiários e segurados, aos membros dos Conselhos Administrativo e Fiscal, membros do Comitê de Investimentos e a outros que por ventura sejam criados, Empresas Contratadas e Prestadores de Serviços, todos denominados na presente Política como usuários, aplicam-se as disposições legais vigentes nesta Portaria.

Art. 2º Fica aprovada e estabelecida a Política de Segurança da Informação do Instituto de Previdência dos Servidores Públicos Municipais de Guarulhos – IPREF, disciplinada na forma do Anexo Único da presente Portaria;

Art. 3° Será realizada revisão dessa Política de Segurança da Informação a qualquer prazo em que a gestão julgar oportuno por alteração de norma pertinente ou necessidade interna.

ANEXO ÚNICO DA PORTARIA 026/2020-IPREF

CAPÍTULO I
DOS OBJETIVOS

Art. 4º A **Política de Segurança da Informação**, também referida como **PSI**, é o documento que orienta e estabelece as diretrizes corporativas do IPREF para a proteção dos ativos de informação e a responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da Autarquia e por todos os usuários que tenham acesso às informações de propriedade do Instituto.

A presente PSI está baseada nas recomendações propostas pela nova lei de proteção de dados LGPD - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm que entrará em vigor em 2020, bem como pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação e demais leis vigentes em nosso país.

Art. 5º Constitui objetivos e princípios da Política de Segurança da Informação – PSI:

I – Estabelecer diretrizes que permitam aos usuários do IPREF seguirem padrões de comportamento relacionados à segurança e correta utilização da informação e dos equipamentos, adequados às necessidades de negócio e de proteção legal da Autarquia e do indivíduo;

II – Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento;

III – Preservar as informações do IPREF quanto à:

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;
b. **confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

c. **disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

d. **autenticidade**: qualidade da informação produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

e. **primariedade**: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações; e

f. **informação atualizada**: informação que reúne os dados mais recentes sobre o tema, de acordo com sua natureza, com os prazos previstos em normas específicas ou conforme a periodicidade estabelecida nos sistemas informatizados que a organizam.

IV – Prover mecanismos de transparência e gestão das informações; e

V – Definir papéis e responsabilidades.

CAPÍTULO II
DISPOSIÇÕES GERAIS

Art. 6º Para efeitos de aplicação dessa Política – PSI, entende-se:

I – **Informação**: dados, processados ou não, que possam ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II – **Segurança da Informação**: proteção contra uso ou acesso não autorizado à Informação, garantindo a proteção permanente aos ativos tecnológicos que permitem a sua armazenagem, a sua distribuição e o seu processamento seguro;

III – **Governança Digital**: é a utilização, pelo setor público, de recursos de Tecnologia da Informação com o objetivo de melhorar a informação e a prestação de serviços por meio digital, aprimorando os níveis de responsabilidade, transparência e efetividade de governo;

IV – **Dados processados**: aqueles submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

V – **Documento**: unidade de registro de informação, qualquer que seja o suporte ou formato;

VI – **Informação sigilosa**: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, bem assim aquelas abrangidas pelas demais hipóteses de sigilo;

VII – **Informação pessoal**: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

VIII – **Tratamento da informação**: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 7º Para os fins desta Portaria, consideramos na caracterização desta PSI os itens listados a seguir com os seguintes termos e seus significados:

a – Bancos de dados: um agrupamento de arquivos de dados relacionados da organização;

b – Extranet: é a conexão das redes de computadores (Intranets) de duas ou mais organizações públicas e/ou privadas, por meio da tecnologia da Internet;

c – Hardware: é o conjunto de dispositivos como computadores servidores, computadores clientes, monitores, impressoras, periféricos das mais diversas categorias, infraestrutura de comunicação de dados e redes de computadores, e tudo mais que a evolução de diversas áreas da engenharia da informática permitir disponibilizar para as tarefas de coleta, transmissão, armazenagem, recuperação, manipulação e apresentação de dados e informações processadas pelos sistemas de informação;

d – Internet: é a rede formada pela integração de outras redes de computadores. É a super rede, com extensão geográfica mundial. Utiliza tecnologia e

protocolos próprios. Foi projetada para continuar funcionando mesmo que partes desta super rede não estejam em operacionalização. A rede das redes que interconecta computadores de empresas, consumidores, órgãos dos governos municipais, estaduais, federais, escolas e outras organizações no mundo todo, que trocam informações habitualmente;

e – Intranet: é o termo usado para caracterizar uma rede de computadores, restrita a uma determinada área, prédio ou organização, que utiliza a mesma tecnologia desenvolvida para a Internet. Uma Intranet tem as mesmas capacidades de uma Internet, sendo que a diferença entre elas se encontra no fato de que a Intranet é usada dentro das Organizações. Uma rede de uma organização que utiliza o software e os protocolos TCP/IP da Internet; basicamente, uma Internet Privada ou grupo de segmentos privados da rede Internet pública;

f – Programa aplicativo: uma parte de um sistema de informação, geralmente um programa de software, desenvolvido para um propósito específico, como por exemplo, executar uma folha de pagamento, ou gerar a prestação de contas da Lei de Responsabilidade Fiscal;

g – Redes de computadores: um sistema de conectividade que viabiliza o compartilhamento de recursos e a comunicação entre computadores diferentes;

h – Sistema integrado de gestão corporativa: é sinônimo de ERP (Enterprise Resource Planing), um processo integrado para planejar e gerenciar todos os principais processos da organização, com uma única arquitetura baseada em cliente/servidor, em tempo real, incluindo em alguns casos a integração com parceiros de negócios e com clientes especiais;

i – Software: conjunto de programas de apoio, incluindo, sistemas operacionais, sistemas de segurança, sistemas de bancos de dados, entre inúmeros outros que formam a plataforma para desenvolvimento e processamento dos sistemas de informação. É o conjunto de programas de computador que permite o processamento de dados no hardware;

j – Software aplicativo: conjunto de programas que orienta os computadores a executar atividades de processamento de informações com propósitos específicos e disponibilizar funções para escolha dos usuários;

k – Tecnologia da Informação e Comunicação (TIC): conjunto de recursos de infraestrutura de hardware e de software que dá todo o suporte ao funcionamento de sistemas baseados em computadores e na comunicação entre eles. Sistemas Aplicativos;

l – Web: sistema com padrões aceitos mundialmente para armazenar, recuperar, formatar e exibir informações por meio de uma arquitetura baseada em cliente/servidor. A web lida com todos os tipos de informações digitais, incluindo texto, hipermídia, gráficos e som. Usa interfaces gráficas de usuário, de modo que é muito fácil utilizá-la;

m – www: é o acrônimo para world wide web, e constitui o coração da Internet. É a parte gráfica que permite distribuir documentos, gráficos, fotos, sons e outras mídias, de maneira unificada e eficiente via Internet, acessível via hiperlinks;

n – Hiperlinks: sinônimo de link, hiperlink consiste em links que vão de uma página da web ou arquivo para outro(a), o ponto de partida para os links é denominado de hiperlinks; e

o – Website ou site: todas as páginas do site de uma determinada organização ou pessoa física.

CAPÍTULO III
APLICAÇÕES DA PSI

Art. 8º As diretrizes aqui estabelecidas deverão ser seguidas por todos os usuários e se aplicam à informação em qualquer meio ou suporte.

***Parágrafo único*:** é obrigação de cada usuário se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação

sempre que não estiver absolutamente seguro quanto ao uso e/ou descarte de informações.

Art. 9º É de inteira responsabilidade da área de Tecnologia da Informação do IPREF a configuração de todos os equipamentos, ferramentas e sistemas para que fiquem de acordo com as normas estabelecidas pela Política de Segurança da Informação aqui estabelecida.

Art. 10° É de responsabilidade da área de Tecnologia da Informação do Instituto publicar e promover atualizações, sempre que necessárias, referente a Política de Segurança da Informação – PSI, bem como conscientizar os colaboradores em relação à relevância da Segurança da Informação.

Art. 11° O cumprimento das regras estabelecidas pela PSI é obrigatória e sua não observância poderá acarretar aplicação de sanções administrativas, penalidades civis ou criminal a quem der causa, bem como não serão permitidas visitas a site de conteúdos adultos ou impróprios, de cunho sexual, pedofilia e/ou ilícitos o que é expressamente proibido.

***Parágrafo único**:* é proibido a todos os usuários acesso a sites com códigos maliciosos, utilização de softwares desatualizados, bem como instalações de softwares piratas ou suspeitos.

Art. 12º São consideradas violações, além daquelas previstas na legislação municipal própria, as seguintes condutas:

I – Uso ilegal de software;

II – Introdução, intencional ou não de malwares;

III – Tentativas de acesso não autorizado a dados e sistemas do Instituto;

IV – Divulgação de informações de servidores, beneficiários, dependentes, fornecedores e das operações contratadas, fora daquelas autorizadas pela Lei da Transparência;

V – Instalação de software sem a devida homologação da área responsável;

VI – Atualização de software sem o devido acompanhamento da área responsável.

Art. 13º O uso de quaisquer recursos da Autarquia para atividades ilícitas poderá acarretar em ações administrativas e penalidades de acordo com o previsto no ordenamento jurídico que rege o Instituto, seja em âmbito administrativo, civil e/ou criminal.

Art. 14° A alteração de qualquer parâmetro ou regra presente na PSI sem a devida autorização será considerada ilegal.

Art. 15° Dispositivos móveis ou mídias digitais devem ser conectados com cautela aos computadores, vez que podem conter arquivos maliciosos ou as mais variadas espécies de vírus.

Art. 16º O usuário deverá conhecer a origem dos arquivos digitais utilizados e caso ocorra download de algum arquivo, de forma inesperada, independente da extensão, o mesmo não deverá ser executado.

Art. 17° Arquivos em geral, mesmo aqueles deletados, ocupam espaço em disco, motivo pelo qual deverão ser evitadas a criação de cópias desnecessárias ou pessoais em ambiente de trabalho, pois podem comprometer o desempenho do computador.

Art. 18º Cada usuário deverá possuir sua própria senha com os devidos privilégios, composta, preferencialmente, por oito dígitos com ao menos um caractere maiúsculo e um especial, caso a senha seja compartilhada, a responsabilidade por eventuais alterações, inclusões ou qualquer outra atividade efetivada com a mesma será do detentor original da senha.

Art. 19º A senha do administrador do sistema só deverá ser utilizada quando estritamente necessária, como no caso, por exemplo, de downloads, manutenção, atualização ou instalação de programas essenciais à elaboração de tarefas, bem como os privilégios de administrador só serão aceitos e fornecidos, após análise e validação da área de Tecnologia da Informação.

Art. 20º O acesso e o uso de todos os sistemas de informação, diretórios de rede, banco de dados e demais recursos devem ser restritos a pessoas autorizadas e de acordo com a necessidade para o cumprimento de suas atividades e funções.

Parágrafo único: A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

Art. 21º A padronização deverá ser utilizada com o fim de garantir integridade, melhor acessibilidade e facilidade em todos os processos envolvendo Tecnologia da Informação.

Art. 22º Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do Instituto, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Art. 23° Equipamentos particulares/privados, como notebook ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o Instituto, nem devem ser conectados às redes da Autarquia.

Art. 24º É obrigatória a realização de backup ou cópias de segurança de arquivos e trabalhos realizados, independentemente do tamanho dos arquivos.

Art. 25º As regras da Política de Segurança da Informação – PSI estabelecidas pelo IPREF têm o objetivo de estimular o desenvolvimento de um comportamento ético e profissional do uso da internet.

Art. 26° A presente Política de Segurança da Informação deve ser observada e respeitada como parte da cultura interna do IPREF, e, assim, quaisquer incidentes que caracterize infringência a essas normas será ato contra as normas e regulamentos do Instituto.

CAPÍTULO IV
DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Art. 27º A utilização da informação deve ser conduzida em conformidade com essa Política de Segurança da Informação, visando obedecer às seguintes diretrizes:

I – A liberação de acessos deve seguir o critério de menor privilégio, no qual os usuários têm acesso somente a recursos necessários para o desempenho de suas atividades;

II – A informação deve ser utilizada de forma transparente e apenas para a qual foi determinada;

III – O acesso a informação e recursos só poderá ser permitido se devidamente autorizado;

IV – As responsabilidades quanto à segurança da informação devem ser divulgadas aos usuários que devem entender e assegurar essas diretrizes;

V – Garantir que cada usuário possua sua identificação, sendo ela única, pessoal e intransferível, o que o qualifica como responsável pelas ações realizadas;

VI – Os riscos às informações do IPREF devem ser comunicados à área de TI imediatamente;

VII – A senha é considerada como assinatura eletrônica, e deve ser mantida sob sigilo, sendo proibido o seu compartilhamento.

CAPÍTULO V
DAS RESPONSABILIDADES ESPECÍFICAS

Art. 28º Será de inteira responsabilidade de cada usuário todo prejuízo ou dano que vier a sofrer ou causar ao IPREF ou a seus parceiros ou fornecedores, em decorrência da não obediência às diretrizes e normas aqui referidas.

Art. 29º Todos os usuários têm responsabilidades quanto à segurança da informação e deverão:

I – No geral:

a – Manter sigilo das informações do IPREF;

b – Zelar pelos ativos de informação do IPREF, sejam eles físicos (processos, documentos, outros) ou digitais (arquivos, sistemas, etc);

c – Seguir as diretrizes e recomendações do Instituto quanto ao uso, divulgação e descarte de dados e informações;

d – Utilizar as informações e recursos disponibilizados pelo IPREF somente para fins profissionais;

e – Comunicar ao responsável pela área de Tecnologia da Informação ou ao superior falhas ou violações de segurança da informação;

f – Armazenar informações confidenciais ou críticas à atividade do IPREF de forma protegida;

g – Restringir a utilização de equipamentos aos fins autorizados pelo IPREF;

h – Manter sua senha em sigilo e diante de suspeita da perda efetuar a troca da mesma, informando imediatamente à área de TI e a chefia imediata;

i – Adotar senhas com seis ou mais caracteres alfanuméricos, misturando maiúsculas e minúsculas e evitando palavras conhecidas, datas, etc.;

j – Realizar o descarte de informações críticas ou confidenciais com destruição irrecuperável das mesmas;

k – Informar imediatamente à área de TI em caso de ocorrência de vírus;

l – Usar somente programas licenciados e homologados pela área de TI do IPREF;

m – Acompanhar o atendimento do técnico de informática quando ocorrer manutenção corretiva ou quando for solicitada a presença do usuário;

II. Em seu local de trabalho ou afastado dele:

a – Não se alimentar ou fumar próximo aos equipamentos de informática.

b – Ao sair de sua mesa guarde as informações em gavetas ou dentro de pastas;

c – Certifique-se de que as impressoras e copiadoras não permaneçam com documentos expostos;

d – Evite manusear documentos do IPREF na presença de estranhos ou em locais públicos;

e – Fique atento para não deixar documentos e informações nas salas de reunião;

f – Seja no seu PC ou notebook bloqueie sempre o equipamento ao se ausentar, para impedir que pessoas não autorizadas tenham acesso à estação. Ao término de expediente desligue o equipamento;

g – Em caso de mau uso dos equipamentos e/ou uso em desacordo com as instruções desta norma, o usuário poderá ser responsabilizado

h – Armazene os arquivos que dizem respeito ao IPREF nos Servidores Corporativos, assim, os dados serão salvos periodicamente (backups), evitando sua perda;

i – Evite a exposição do notebook durante o transporte, ao transportá-lo utilize uma pasta ou mochila que não chame a atenção;

j – Em caso de roubos, extravios, danos ou quaisquer outras irregularidades comunique imediatamente à sua chefia imediata;

CAPÍTULO VI
DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art. 30º Para garantir as regras mencionadas nesta PSI, o Instituto poderá:

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 poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II – Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação do superior hierárquico;

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

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

Parágrafo Único: O IPREF faz uso de uma solução que monitora os dados sensíveis, registra acessos e registra todas as ações realizadas pelo usuário.

Art. 31º A Segurança da Informação é um ciclo, temos que estar sempre atentos, conscientes e atualizados, portanto:

I – A informação deve receber proteção adequada em todo o seu ciclo de vida: geração, manuseio, transporte e descarte, a partir do momento em que você cria uma informação, seja e-mails ou documentos, a manuseia (consulta ou alteração), a armazena (em HD, gaveta, pastas) envia para alguém (e-mail, correio, motoboy, pessoalmente) até o ponto em que você decide descartá-la (apagar um arquivo ou jogar um relatório no lixo), a informação passa por várias fases.

II – Não existe ambiente cem por cento seguro, existe ambiente com menor risco. Colabore para isso.

CAPÍTULO VII
ENGENHARIA SOCIAL

Art. 32º Seja zeloso até mesmo com aquelas informações casuais, pois engenharia social consiste na obtenção de informações importantes do usuário ou ambiente, através de uma conversa informal, ingenuidade ou confiança. O Indivíduo mal-intencionado geralmente usa telefone, e-mail ou redes sociais para conseguir informações que procura. Portanto, atente-se para:

I – Não ceda à pressão psicológica ou às técnicas de persuasão de pessoas que tentam obter informações, seja, pessoalmente, por telefone ou internet;

II – Verifique a necessidade de levar informações dentro da bolsa ou pastas. Pessoas mal-intencionadas podem manipular e utilizar informações de forma inadequada ou criminosa;

III – Muito cuidado, desconfie de abordagens de pessoas que ligam e se identificam como técnicos ou funcionários de determinada firma e pedem dados sobre o Instituto, ambiente, você, seu superior;

IV – Jamais forneça sua senha a outrem.

V – Evite falar de assuntos profissionais na presença de pessoas estranhas (elevador, telefone celular, cafés, restaurantes, metrô, táxi, Uber, ônibus, etc). Essas pessoas poderão fazer mau uso das informações.

VI – Não dê informações por telefone ou e-mail sem a confirmação da identidade do interlocutor;

VII – Não discuta assuntos profissionais em sites de relacionamentos;

VIII – Seja um multiplicador de atitudes e conduta segura, cobre de si mesmo essas ações e respeite seus colegas que também o fazem.

CAPÍTULO VIII
CORREIO ELETRÔNICO

Art. 33º O uso do correio eletrônico do IPREF é permitido tanto para uso de trabalho quanto pessoal, sendo este último permitido desde que não entre em conflito com o ordenamento do IPREF, ou cause qualquer tipo de prejuízo ou constrangimento ao Órgão, sendo terminantemente proibido:

I – Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a usos legítimos do Instituto;

II – Enviar mensagens por correio eletrônico pelo endereço de seu setor ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não seja autorizado a utilizar;

III – Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o IPREF vulneráveis a ações civis ou criminais;

IV – Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

V – Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

VI – Apagar mensagens pertinentes de correio eletrônico quando o IPREF estiver sujeito a algum tipo de investigação ou sanções;

VII – Enviar informações privadas do Instituto, sem autorização;

VIII – Envio de spam;

IX – Divulgação de informações falsas;

X – Envio de executáveis maliciosos;

XI – Envio de conteúdo pornográfico, ilegal ou obsceno;

XII – Envio de mensagem com caráter ofensivo, desrespeitoso, ameaçador, entre outros;

XIII – Envio ou instalação de softwares pirateados, sem a devida licença.

CAPÍTULO IX
INTERNET

Art. 34º Exige-se dos usuários comportamento ético e profissional com o uso da internet disponibilizada pelo IPREF

Art. 35º Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do Instituto, que pode analisar e, julgando necessário, bloquear quaisquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, sempre visando assegurar o cumprimento de sua Política de Segurança da Informação. O atendimento a tais requisitos é possível pois o Instituto realizou a implementação de servidor Firewall/Proxy.

§ 1º. Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria, tendo o IPREF, em total conformidade legal, o direito de monitorar e registrar todos os acessos a ela.

§ 2º Qualquer alteração dos parâmetros de segurança realizado por qualquer usuário sem o devido credenciamento e autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e respectivo superior hierárquico para as medidas cabíveis.

§ 3º O uso de quaisquer recursos para atividades ilícitas poderá acarretar em ações administrativas e penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Autarquia cooperará ativamente com as autoridades competentes.

§ 4º O uso de sites de notícias ou de serviços, por exemplo, é aceitável desde que pertinentes ao desenvolvimento de suas atividades profissionais e que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom

andamento dos trabalhos nem implique em conflitos de interesse com seus objetivos de negócio.

Art. 36º Somente os usuários que estão devidamente autorizados a falar em nome do IPREF para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevistas on-line, podcast entre outros

Art. 37º Apenas usuários autorizados pelo Instituto 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.

Art. 38º Os usuários com acesso à internet poderão fazer Download (baixa) somente de programas ligados diretamente às suas atividades no IPREF, e, deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo Instituto.

§ 1º O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

§ 2º Os usuários não poderão, em nenhuma hipótese, utilizar os recursos do IPREF para fazer download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Art. 39º É proibido o acesso, exposição, armazenamento, distribuição, edição, impressão ou gravação por meio de qualquer recurso, de materiais de cunho sexual.

Art. 40º Os usuários não poderão utilizar recursos do IPREF para deliberadamente propagar quaisquer tipos de vírus, worn, cavalo de tróia, spam, assedio, perturbação ou programas de controle de outros computadores.

Art. 41º As regras expostas neste capítulo se aplicam ao uso de computadores e outros dispositivos de propriedade do IPREF, bem como dispositivos particulares dos usuários que estiverem conectados à internet do Instituto (cabeada ou sem fio).

CAPÍTULO X
IDENTIFICAÇÃO E CONTROLE DE ACESSO

Art. 42º Para o acesso aos recursos tecnológicos do IPREF será exigido, sempre que possível, identificação e senha exclusiva de cada usuário, permitindo assim o controle e acesso.

§ 1º É proibido o compartilhamento de login entre os usuários.

§ 2º Recomenda-se como boa prática de segurança que, ao realizar o primeiro acesso ao ambiente de rede local, o usuário seja direcionado a trocar imediatamente sua senha.

§ 3º 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 consignados e/ou designados.

§ 4° Os usuários podem alterar a própria senha, e, devem ser orientados a fazê-lo caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

CAPÍTULO XI
CONTROLE DE ACESSO FÍSICO E PATRIMONIAL

Art. 43º Para o gerenciamento do acesso físico dos usuários às dependências do IPREF o órgão toma medidas de controle de acesso pessoal e biométrico, por meio de:

I. Recepção central, com profissional na portaria, que controla o acesso à única entrada do prédio;

II. Fornecimento de crachá de identificação aos funcionários do Instituto no momento da admissão;

III. Controle de entrada e saída dos funcionários com uso de biometria;

IV. Catracas para permissão de acesso de visitantes ao prédio após triagem e identificação.

CAPÍTULO XII
DAS DISPOSIÇÕES FINAIS

Art. 44º Tanto a PSI quanto as normas de segurança deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da área de Tecnologia da Informação da Autarquia.

Art. 45º Assim como a Ética, a Segurança deve ser entendida como parte fundamental da cultura interna do IPREF. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pelo Instituto.

Art. 46º Esta portaria entrará em vigor na data de sua publicação.

EDUARDO AUGUSTO REICHERT
Presidente

Publicado no Diário Oficial de Guarulhos nº028/2020 de 21 de fevereiro de 2020 pág.64
Disponível em https://www.guarulhos.sp.gov.br/uploads/pdf/420321229.pdf