IGEPREV

PORTARIA Nº 366, DE 15 DE FEVEREIRO DE 2021.

Institui a Política de Segurança da Informação e estabelece critérios relativos ao acesso, uso, armazenamento, procedimento, segurança e responsabilidade na utilização da tecnologia da informação do Instituto de Gestão Previdenciária do Estado do Tocantins - IGEPREV-TO.

O PRESIDENTE DO INSTITUTO DE GESTÃO PREVIDENCIÁRIA DO ESTADO DO TOCANTINS, no uso das atribuições legais que lhe confere o art. 20, X, da Lei nº 1.940, de 1º de julho de 2008, e;

CONSIDERANDO o disposto no Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios (Portaria MPS nº 185/2015), item 3.1.5 - Política de Segurança da Informação;

CONSIDERANDO que a efetividade da tecnologia da informação no âmbito do Instituto de Gestão Previdenciária do Estado do Tocantins - IGEPREV, é condição essencial para o pleno exercício das atividades institucionais de seus integrantes;

CONSIDERANDO imprescindível garantir a segurança das informações e dados que trafegam nos recursos computacionais e tecnológicos desta Autarquia, assegurando os atributos de confidencialidade, integridade, disponibilidade, autenticidade e sigilosidade;

CONSIDERANDO premente racionalizar e operacionalizar adequadamente o uso dos recursos e serviços relativos à tecnologia da informação disponibilizada nesta Autarquia;

CONSIDERANDO a necessidade de definir padrões técnicos e procedimentos para uso dos recursos e serviços disponíveis, bem como alinhar as ações de Tecnologia da Informação no âmbito interno aos objetivos estratégicos da Autarquia;

CONSIDERANDO a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018;

CONSIDERANDO a celeridade processual proporcionada pelo uso das ferramentas de tecnologia da informação, bem como a economicidade pela diminuição do fluxo de correspondências físicas e demais documentos oficiais, deslocamentos desnecessários de servidores, além do melhor controle dos atos e ações institucionais e a prestação de serviços à sociedade;

CONSIDERANDO a aprovação pelo Conselho Deliberativo do IGEPREV-TO em Reunião Ordinária realizada no dia xx de novembro de 2020.

RESOLVE:

Art. 1º Instituir a Política da Segurança da Informação e estabelecer critérios relativos ao acesso, uso, armazenamento, procedimento, segurança e responsabilidade na utilização da tecnologia da informação do Instituto de Gestão Previdenciária do Estado do Tocantins - IGEPREV-TO.

Art. 2º Este regulamento, conforme disposto no Anexo Único, aplica-se a toda estrutura desta Autarquia, bem como as unidades administrativas e usuários autorizados que utilizam a tecnologia da informação disponibilizada pelo Instituto de Gestão Previdenciária do Estado do Tocantins - IGEPREV-TO, na realização das atividades de interesse exclusivamente institucional.

Art. 3º Esta Portaria entra em vigor a partir da data da publicação.

SHARLLES FERNANDO BEZERRA LIMA
Presidente

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Diretrizes e Normas Administrativas
Versão 1.0 - Válida a partir da publicação

CRÉDITOS

Presidência
Sharlles Fernando Bezerra Lima

Vice-Presidência
Ana Cláudia Perreira da Cunha

Tecnologia da Informação
Kennypher Brito de Queiroz
Analista de Redes e Segurança

Tecnologia da Informação
José Maria Teixeira
Contador

Tecnologia da Informação
Fernando Coelho Moreira
Analista de Sistemas

Gerencia Geral de Administração
Júlio Soares Lacerda
Gerente Geral

CAPÍTULO I
SEGURANÇA DA INFORMAÇÃO

Seção I
Política da Segurança da Informação

Art. 1º A Política de Segurança da Informação no âmbito do Instituto de Gestão Previdenciária do Estado do Tocantins - IGEPREV-TO tem como pressupostos básicos:

I. Preservação da credibilidade e do prestígio da Autarquia;

II. Proteção das informações e/ou dados judiciais e extrajudiciais que circulam no âmbito do IGEPREV;

III. Efetivação de medidas de conscientização dos recursos humanos sobre a importância das informações processadas e sobre o risco da vulnerabilidade e integridade;

IV. Armazenamento e proteção de acesso ao uso adequado das informações.

Art. 2º Para efeitos da Política da Segurança da Informação ficam estabelecidas as seguintes conceituações:

I. Confiabilidade: princípio de Segurança da Informação pelo qual se garante que o acesso à informação seja obtido somente por pessoas autorizadas;

II. Criticidade: grau de importância da informação para a continuidade das atividades do IGEPREV;

III. Disponibilidade: princípio de Segurança da Informação pelo qual se estabelece que as informações e os recursos estarão disponíveis sempre que necessário;

IV. Integridade: princípio de Segurança da Informação por meio do qual é garantida que a informação não será alterada sem a devida autorização;

V. Recurso: além da própria informação, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

VI. Usuário: é toda pessoa física ou jurídica que utiliza quaisquer recursos computacionais do IGEPREV de forma autorizada por quem de direito;

VII. Tecnologia da Informação: conjunto de recursos tecnológicos e computacionais para geração e uso da informação;

VIII. Política da Segurança da Informação: normas que visam estabelecer procedimentos de proteção das informações e dados que circulam no âmbito do IGEPREV, com adoção de medidas para dar efetividade ao uso racional e adequado da tecnologia da informação disponibilizada;

IX. Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como a intrusão, a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

X. Departamento de Tecnologia da Informação - DTI: unidade vinculada à Diretoria Executiva do IGEPREV responsável pelo planejamento, coordenação, organização, controle e supervisão dos recursos computacionais da Autarquia;

XI. Recursos Computacionais: são todos os equipamentos, instalações, programas de computador e bancos de dados, direta ou indiretamente administrados e operados pelo Departamento de Tecnologia da Informação do IGEPREV para armazenar, processar, transmitir e disseminar informações de interesse da Autarquia, dentre eles:

a) computadores, tablets, notebooks, ultrabooks, smartphones e terminais de qualquer espécie, incluídos acessórios;

b) impressoras, multifuncionais, Leitores de código de barras e escanares de qualquer espécie;

c) servidores de arquivos, de impressão, de correio eletrônico, WEB, aplicação e outros tipos de servidores de redes;

d) modens, roteadores, switches, hubs, redes de dados, soluções de segurança e demais equipamentos de conexão e comunicação de dados;

e) sistemas operacionais e aplicativos;

f) intranet, internet e correio eletrônico;

g) softwares adquiridos ou desenvolvidos pelo Departamento de Tecnologia da Informação do IGEPREV;

h) banco de dados ou documentos residentes em servidor de rede, disco, fita e outros meios;

i) salas de computadores e laboratórios de informática;

j) site ou homepage do IGEPREV;

k) manuais técnicos.

XII. Material de Consumo de Informática: utilizados, direta ou indiretamente, para armazenar, processar, transmitir e disseminar informações na área de informática, consistindo em HD externos, pendrives, toner para impressora, CD, DVD, fita magnética e outros;

XIII. Conta de Acesso Pessoal: pertence ao usuário e lhe permite acessar à rede, o correio eletrônico, a intranet e os softwares do IGEPREV;

XIV. Serviço de Correio Eletrônico Institucional: serviço de envio e recebimento de mensagens eletrônicas (e-mails) do IGEPREV, implementado e gerenciado pelo DMTI;

XV. Serviço Externo de Correio Eletrônico: qualquer serviço de correio eletrônico disponibilizado por terceiros;

XVI. Webmail: serviço de correio eletrônico disponível por meio de um sítio;

XVII. Login: processo de identificação e autenticação de usuários em programas computacionais e serviços de e-mail;

XVIII. Spam: mensagem geralmente destinada à realização de propaganda e marketing de produtos e serviços disponíveis no mercado, bem como veicular outros tipos de conteúdos indevidos;

XIX. Corrente: mensagem enviada com o objetivo de propagar um boato ou determinado assunto sem relação com as atividades da Instituição;

XX. Scam: mensagem enviada com o objetivo de obter informações sensíveis, tais como senhas e números de cartão de crédito para utilização em fraudes;

XXI. Código Malicioso: termo genérico que se refere a todos os tipos de *software* que executam ações maliciosas em um computador, como: vírus, worms, bots, cavalos de troia e rootkits;

XXII. *Software*: qualquer programa, aplicativo ou sistema desenvolvido para utilização em computadores ou em outros dispositivos eletroeletrônicos;

XXIII. Cliente de Correio Eletrônico: *software* no qual o usuário pode receber e enviar e-mails;

XXIV. Grupo ou Lista de e-mails: é um grupo de endereços eletrônicos organizados para fins de recebimento conjunto de mensagens.

Art. 3º São objetivos da Política de Segurança da Informação:

I. dotar o IGEPREV de instrumentos jurídicos, normativos e organizacionais que o capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, integridade e a disponibilidade dos dados e/ou informações tratadas, classificadas e sensíveis;

II. eliminar a dependência extrema em relação a sistemas, equipamentos, dispositivos e atividades vinculadas a segurança dos sistemas de informação;

III. promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;

IV. estabelecer normas jurídicas necessárias para a efetiva implementação da segurança da informação;

V. promover as ações necessárias à implementação e manutenção da segurança da informação;

VI. promover o intercâmbio científico e tecnológico com outros órgãos estaduais ou federais sobre as atividades de segurança da informação;

VII. assegurar a operatividade dos sistemas de segurança da informação.

Art. 4º Compete à Diretoria Executiva

I. estabelecer políticas e diretrizes de tecnologia de informação, alinhadas aos objetivos estratégicos da Autarquia;

II. aprovar o Plano Diretor de Tecnologia da Informação do IGEPREV;

III. definir as prioridades dos investimentos em tecnologia da informação;

IV. estabelecer as prioridades para execução de projetos de tecnologia da informação;

V. definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de tecnologia da informação.

CAPÍTULO II
DAS NORMAS DE USO E SEGURANÇA DA INFORMAÇÃO

Seção I
Dos Direitos e Obrigações dos Usuários

Art. 5º São direitos dos usuários autorizados:

I. fazer uso dos recursos computacionais da Autarquia para a realização de atividades profissionais relacionadas aos serviços de interesse do IGEPREV;

II. ter conta de acesso pessoal à rede de computadores e aplicativos mediante a liberação automática de senha pelo Departamento de Gestão de Pessoas, após os devidos registros em seus sistemas e caso tenha problema de acesso e permissões, ter suporte do Departamento de Tecnologia da Informação;

III. ter conta de acesso pessoal ao correio eletrônico mediante a liberação automática de senha pelo Departamento de Gestão de Pessoas, após os devidos registros em seus sistemas e caso tenha problema de acesso e permissões, ter suporte do Departamento de Tecnologia da Informação;

IV. acessar Internet, pelo navegador (browser) indicado pelo Departamento de Tecnologia da Informação, e a Intranet por meio da senha pessoal liberada pelo Departamento de Gestão de Pessoas, encaminhada para e-mail não institucional cadastrado em sistema próprio, com auxílio e suporte do Departamento de Tecnologia da Informação, caso necessário;

V. o acesso a quaisquer serviços ou sistemas providos pelo IGEPREV ou por outros órgãos da administração direta deverá ser solicitado ao RH pelo chefe do departamento onde o usuário está lotado;

VI. ter restrita e/ou limitada privacidade das informações na sua área de armazenamento;

VII. solicitar atendimento técnico do Departamento de Tecnologia da Informação por meio do link "Help", constante na página da Intranet;

VIII. receber o adequado atendimento do suporte técnico.

IX. acessar a rede da Instituição por meio de computadores e/ou notebook pessoais quando devidamente autorizado pela Diretoria Executiva, sem nenhum ônus para a Administração;

X. inserir e/ou executar *pendrive* ou outro dispositivo similar nos recursos computacionais do IGEPREV somente quando proceder prévia varredura do antivírus disponível na rede no respectivo dispositivo.

Art. 6º São obrigações dos usuários autorizados:

I. zelar pela integridade e segurança dos equipamentos e pelas informações processadas e armazenadas nos recursos computacionais sob sua responsabilidade de uso;

II. utilizar dos recursos computacionais exclusivamente para os serviços do IGEPREV;

III. antes de ausentar-se do local de trabalho, o usuário deverá fechar todos os programas em uso, efetuar o logoff da rede ou fazer o bloqueio do computador através do comando Ctrl + Alt + Del, evitando o uso dos recursos computacionais por pessoas não autorizadas;

IV. manter, nos locais onde não tiver disponível servidor de rede, em especial nas unidades de atendimento do IGEPREV nas cidades do interior, cópia de segurança de seus dados e/ou informações, evitando a interrupção do serviço;

V. manter sigilo, integridade e segurança de todos os dados e/ou informações que tiverem acesso;

VI. não autorizar que pessoas estranhas ao quadro do IGEPREV tenham acesso físico aos equipamentos sob sua responsabilidade;

VII. manter constante cuidado de proteção contra vírus, principalmente quando do recebimento de mensagens pelo correio eletrônico, acesso à internet, download de arquivos com extensão que apresentem perigo de inserção ou execução de dispositivos nos recursos computacionais desta Instituição;

VIII. cientificar-se de que todo arquivo em mídia proveniente de entidade externa ao IGEPREV deve ser verificado por programa antivírus. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho;

IX. fazer uso racional do material de consumo do IGEPREV, combatendo o desperdício em todas as formas;

X. manter o bom uso, a limpeza e a conservação dos equipamentos de informática colocados à sua disposição;

XI. manter o Departamento de Tecnologia da Informação informado sobre qualquer mudança efetuada nos recursos computacionais colocados à sua disposição;

XII. respeitar e seguir as normas e procedimentos definidos pela Diretoria Executiva e pelo Departamento de Tecnologia da Informação.

Seção II
Das Proibições aos Usuários

Art. 7º Fica proibido aos usuários:

I. a utilização nas dependências do IGEPREV de sistemas, aplicativos ou de qualquer *software* que não tiver sua respectiva licença de uso;

II. usar, instalar, executar, copiar ou armazenar aplicativos, programas ou qualquer outro material que não esteja devidamente autorizado pelo Departamento de Tecnologia da Informação do IGEPREV;

III. fazer a instalação ou remoção de softwares que não forem devidamente acompanhados pelo Departamento de Tecnologia da Informação, através de solicitação que deve conter o ciente do responsável pelo departamento do solicitante;

IV. instalar ou utilizar outros programas de mensagens instantâneas que não aquele indicado pelo IGEPREV;

V. copiar, transferir ou emprestar *software* para finalidade ou pessoa estranha aos serviços do IGEPREV;

VI. fazer alterações nas configurações na rede de computadores do IGEPREV sem a prévia anuência do Departamento de Tecnologia da Informação, assim como alterar o modo de inicialização ou modificações outras no computador à sua disposição que possa acarretar algum problema ou abrir vulnerabilidade a ataques por hackers;

VII. executar ou configurar os recursos computacionais ou tecnológicos com a intenção de facilitar o acesso a usuários não autorizados;

VIII. utilizar programas de rádio, videoconferência, filmes, vídeos ou outros que trafegam dados que não sejam textos, sem a prévia autorização do Departamento de Tecnologia da Informação;

IX. compartilhar com terceiros contas de acesso pessoal à rede computacional do IGEPREV, aos softwares de aplicativos e qualquer outra espécie de autorização de uso individual e intransferível;

X. obter por terceiros, acesso não autorizado aos sistemas, recursos computacionais e tecnológicos do IGEPREV;

XI. violar o sistema de segurança dos recursos computacionais, por exemplo: identificação de usuários, senhas de acesso, fechaduras automáticas, catracas, sistemas antivírus ou outros;

XII. remover, copiar, emprestar ou divulgar documento confidencial e sigiloso, bem como endereços residenciais e eletrônicos de usuários, de propriedade do IGEPREV;

XIII. destruir, estragar ou desconfigurar intencionalmente os equipamentos, softwares ou dados pertencentes ao IGEPREV;

XIV. utilizar os recursos e materiais de informática para trabalhos particulares ou que não tenham ligação com a finalidade do IGEPREV;

XV. remover, transferir, emprestar, modificar ou proceder qualquer alteração nas características físicas ou técnicas dos equipamentos, sem a prévia autorização do Departamento de Tecnologia da Informação;

XVI. retirar qualquer recurso computacional do local destinado sem prévia autorização da Diretoria Executiva ou Departamento por ela autorizado;

XVII. conectar qualquer equipamento particular à rede local do IGEPREV sem o conhecimento prévio e anuência da Diretoria Executiva e, em especial, sem que o Departamento de Tecnologia da Informação retire o serviço DHCP para esse equipamento e libere o acesso à rede Institucional através do registro do endereço MAC;

XVIII. utilizar qualquer recurso computacional do IGEPREV para constranger, assediar, ofender, caluniar ou ameaçar qualquer pessoa ou instituição.

Seção III
Do Acesso à Internet

Art. 8º Todos os usuários autorizados terão direito ao acesso à Internet para realização das atividades relacionadas ao serviço da Instituição, por meio do browser indicado pelo Departamento de Tecnologia da Informação.

Art. 9. É proibida a utilização da internet nos equipamentos do IGEPREV para:

I. participar de salas de bate-papo e comunicação instantânea, como Google Talk, Skype e similares, exceto aquelas de exclusivo interesse das atividades do IGEPREV e quando previamente autorizado por quem de direito;

II. engajar-se em atividades comerciais ou político partidárias;

III. copiar arquivos que ofereçam risco potenciais à segurança do ambiente computacional do IGEPREV, tais como os arquivos com as extensões exe, src, bat, pif, vbc e outros de mesma natureza;

IV. copiar arquivos (download) que contenham som, vídeo ou animação, que não sejam de interesse das atividades do IGEPREV;

V. acessar sites de redes sociais como Facebook, Facebook Messenger, Youtube, WhatsApp, Instagram, Wechat, Tumblr, QQ, QZone, Sina Weibo, Reddit, Twitter, ou outros similares que venham a existir, que não sejam de interesse das atividades do IGEPREV ou que provoquem sobrecarga na estrutura computacional desta Autarquia;

VI. participar de qualquer ação que comprometa a segurança do site e das informações e/ou dados que circulam no IGEPREV;

VII. exibição, veiculação ou armazenamento de páginas com conteúdo pornográfico, erótico, jogos de qualquer espécie, comercial, político partidário, ofensivo ao decoro pessoal e ao princípio de urbanidade.

Art. 10. O uso da internet será monitorado pelo Departamento de Tecnologia da Informação mediante emprego de ferramentas específicas, com a possibilidade de geração de relatórios e estatísticas dos sites visitados, serviços utilizados e usuários com maior acesso.

Art. 11. O bloqueio de sítios eletrônicos estranhos à atividade institucional, com base na Política da Segurança da Informação, ficará a cargo do Departamento de Tecnologia da Informação, principalmente quando se tratar de arquivos de vídeos, áudios, executáveis, batches, scripts, macros e qualquer outro que porventura possam comprometer a segurança e estrutura da rede do IGEPREV.

§1º Cabe à Diretoria Executiva verificar a necessidade de bloqueio de outras espécies de sítios eletrônicos.

§2º Se houver imprescindível necessidade, em razão de serviço, de acessar sítio eletrônico ou documento previamente bloqueado pelo Departamento de Tecnologia da Informação, deverá o pedido de liberação ser autorizado pela Diretoria Executiva, de forma temporária ou definitiva, para que o servidor execute o trabalho.

§3º Todo arquivo recebido/obtido através do ambiente de Internet deve ser verificado por programa antivírus. O usuário não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Art. 12. Incumbe Diretoria Executiva a análise prévia das matérias a serem publicadas no site eletrônico do IGEPREV, que após deferimento encaminhará ao departamento competente para divulgação.

Seção IV
Do Uso da Intranet

Art. 13. O acesso à intranet do IGEPREV é restrito aos usuários autorizados.

Art. 14. O acesso à intranet será monitorado e auditado por meio de login e senha pessoal.

Art. 15. O "Servidor de Arquivos" do IGEPREV deve ser utilizado seguindo as seguintes normas:

a) os usuários devem receber acesso "Servidor de Arquivos" somente dos serviços que tenham sido especificamente autorizados a usar, em formulário específico assinado pelo gestor;

b) é obrigatório armazenar os arquivos inerentes ao IGEPREV no "Servidor de Arquivos", em pastas compartilhadas, para garantir a cópia de segurança dos mesmos;

c) é vedado o uso do "Servidor de Arquivos" para armazenar informações de cunho pessoal, como fotos, arquivos de áudio, etc. Tais arquivos devem ser salvos no disco rígido da estação de trabalho utilizada pelo usuário;

d) os arquivos gravados em diretórios temporários públicos no "Servidor de Arquivos" e nas estações de trabalho, podem ser acessados por todos os usuários que utilizam a rede interna do IGEPREV, portanto não se pode garantir sua integridade e disponibilidade. Por estarem tais arquivos gravados em diretórios temporários públicos, poderão ser alterados ou excluídos sem prévio aviso e por qualquer usuário, conforme previsto no item "e";

e) os arquivos gravados em diretórios temporários públicos no "Servidor de Arquivos" e nas estações de trabalho, serão excluídos pelo Departamento de Tecnologia da Informação todo 5º dia útil de cada mês, com aviso prévio via aplicativo pandion/spark;

f) não é permitido criar e/ou remover arquivo fora da área previamente alocada ao usuário no "Servidor de Arquivos", bem assim criar e/ou remover arquivos que venham a comprometer o desempenho e funcionamento da estrutura tecnológica do IGEPREV;

g) o usuário deve fazer manutenções periódicas no diretório pessoal no "Servidor de Arquivos", evitando acúmulo de arquivos desnecessários ou duplicados;

h) o Departamento de Tecnologia da Informação não se responsabiliza por documentos, programas e relatórios armazenados em pasta de caráter pessoal do usuário no "Servidor de Arquivos" ou por documentos, programas e relatórios armazenados em pasta de caráter pessoal ou mesmo institucional na estação de trabalho do usuário. Cabe ao usuário a tarefa de resguardar a segurança de documentos, programas e relatórios armazenados em pasta de caráter pessoal ou outra de qualquer que esteja armazenada em sua estação de trabalho;

i) é de responsabilidade do usuário os documentos, programas e relatórios armazenados em seu diretório pessoal, devendo evitar o acúmulo de arquivos desnecessários;

j) o Departamento de Tecnologia da Informação poderá monitorar os diretórios pessoais dos usuários, com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos;

k) a utilização de equipamento particular de informática na rede do IGEPREV só será liberada mediante autorização por quem de direito e após vistoria no equipamento pelo Departamento de Tecnologia da Informação, objetivando aferir se o mesmo atende aos requisitos mínimos de segurança exigidos;

l) quando um servidor efetivo ou comissionado, um terceirizado ou estagiário for transferido entre departamentos no IGEPREV, o responsável pelo departamento deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança serão necessários na sua nova função, e informar ao Departamento de Gestão de Pessoas e Folha de Pagamento qualquer modificação necessária través de formulário específico;

m) quando ocorrer a nomeação/contratação/exoneração/demissão/aposentadoria do servidor, o Departamento de Gestão de Pessoas deverá informar à TI para providenciar a ativação/desativação dos acessos do usuário a qualquer recurso da rede do IGEPREV. Deve-se informar ao Departamento de Tecnologia da Informação a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações privadas do setor.

Seção V
Do Uso do Correio Eletrônico

Art. 16. O correio eletrônico institucional deve ser utilizado somente em atividades estritamente relacionadas às funções institucionais e será para comunicação e troca de documentos internos, evitando-se, tanto quanto possível, a impressão do conteúdo de mensagens.

Art. 17. É garantido a cada integrante do IGEPREV o uso de uma conta de correio eletrônico da Autarquia, criada pelo Departamento de Tecnologia da Informação, desde que possua identificação de acesso para utilização do serviço.

§1º Servidores cedidos, prestadores de serviços terceirizados, consultores e estagiários poderão ter acesso ao correio eletrônico institucional durante o período de cessão, de prestação dos serviços, consultoria ou estágio, observando as normas aqui enumeradas, mediante cadastro realizado pelo Departamento de Gestão de Pessoas;

§2º Solicitações para criação ou exclusão serão realizadas de forma automática após os devidos cadastros ou bloqueios pelo Departamento de Gestão de Pessoas;

§3º As unidades administrativas poderão ter endereço de correio eletrônico, devendo ser encaminhado o pedido formal ao Departamento de Tecnologia da Informação, com a justificativa do chefe ou responsável da unidade.

§4º A caixa postal de uma unidade administrativa poderá ser acessada pelo gestor da unidade e pelos servidores por ele designados.

§5º É permitida a criação de listas de correio eletrônico, com o objetivo de atender necessidades específicas de determinados grupos de usuários, com gerenciamento pelo Departamento de Tecnologia da Informação;

§6º Será mantida a conta de e-mail pelo prazo máximo de 180 (cento e oitenta) dias, do servidor exonerado ou aposentado, bem assim do comissionado exonerado e do terceirizado ou estagiário que tiveram seu vínculo rompido com o IGEPREV, a contar da publicação do respectivo ato no Diário de Oficial do Estado do Tocantins, porém, apenas para cópia das informações necessárias e envio de informações, mas sem possibilidade de recebimento de novos e-mails. Após o prazo a conta deverá ser bloqueada totalmente, porém, não será excluída seguindo as recomendações do §7º;

§7º A conta de e-mail desativada terá seu conteúdo preservado pelo Departamento de Tecnologia da Informação por um período de 05 (cinco) anos, com exclusão após o decurso desse prazo. Por se tratar de e-mail funcional e Institucional, após o desligamento do servidor a Administração terá pleno direito a todas as informações e conta, podendo acessar o conteúdo para análise ou interesse do serviço público.

Art. 18. O endereço de correio eletrônico institucional será composto pelo sufixo "@igeprev.to.gov.br".

Art. 19. Constitui uso indevido do serviço de correio eletrônico institucional:

I. enviar qualquer tipo de spam, scam ou "corrente";

II. enviar mensagens com vírus ou códigos maliciosos anexados;

III. enviar material protegido por Leis de propriedade intelectual;

IV. enviar mensagens com conteúdo considerado ofensivo, obsceno, discriminatório, antiético, ilegal ou impróprio, como: pornografia, pedofilia, racismo, apologia ao crime, calúnia, difamação, injúria, entre outros;

V. enviar mensagens com conteúdos, arquivos, fotos, imagens, sons ou vídeos não relacionados às funções institucionais;

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

VII. assuntos que provoquem assédio, constrangimento ou que prejudiquem a imagem do IGEPREV;

VIII. utilizar clientes de correio eletrônico não homologados pelo Departamento de Tecnologia da Informação;

IX. participar de lista de e-mails cujo tema não esteja relacionado às atividades institucionais;

X. enviar mensagens que representem riscos de segurança, ou que afetem o desempenho dos recursos de tecnologia da informação, ou, ainda, que possam comprometer, de alguma forma, a integridade, a confidencialidade ou a disponibilidade das informações institucionais;

XI. o redirecionamento automático de mensagens para serviços externos de correio eletrônico;

XII. enviar listas contendo o endereço eletrônico institucional (e-mails) de servidores do IGEPREV para fins não relacionados às funções institucionais.

Art. 20. Os anexos e/ou hiperlinks das mensagens do correio eletrônico institucional poderão ser bloqueados quando oferecerem riscos à segurança da informação e comunicação.

Parágrafo único. A abertura de mensagens de remetentes desconhecidos, externos ao IGEPREV, deve ser avaliada, especialmente no caso de dúvidas quanto à natureza do seu conteúdo, como arquivos anexados não esperados ou hiperlinks para endereços externos não relacionados às atividades profissionais em curso.

Art. 21. O uso indevido do correio eletrônico das unidades administrativas na capital e interior é de responsabilidade do respectivo gestor e dos servidores por ele eventualmente designados para acessá-lo, na medida de suas culpabilidades.

Art. 22. Compete ao Departamento de Tecnologia da Informação a gestão das funcionalidades e a segurança do serviço de correio eletrônico institucional do IGEPREV, para garantir o cumprimento desta Política.

§1º O Departamento de Tecnologia da Informação é responsável pela implementação, configuração e gerenciamento dos recursos de tecnologia da informação relacionados aos serviços de correio eletrônico institucional;

§2º O Departamento de Tecnologia da Informação manterá os registros de envio e recebimento de mensagens, resguardado o sigilo das correspondências;

§3º O Departamento de Tecnologia da Informação estabelecerá os limites de tamanho das caixas postais e das mensagens enviadas e recebidas pelos usuários, de acordo com a capacidade técnica dos servidores de armazenamento de dados;

§4º A quantidade de destinatários deve ser limitada por mensagem, com o objetivo de coibir a prática de spam, cabendo ao Departamento de Tecnologia da Informação estabelecer tal limite, bem como acordar com as demais áreas as eventuais exceções, de acordo com os interesses do IGEPREV.

Art. 23. São deveres dos usuários:

I. utilizar o correio eletrônico institucional para os objetivos e funções próprias e inerentes às atribuições funcionais;

II. verificar diariamente o conteúdo da conta pessoal, eliminando periodicamente as mensagens contidas nas caixas postais;

III. manter em sigilo sua senha de acesso ao correio eletrônico, visto que esta é de uso pessoal e intransferível, substituindo-a em caso de suspeita de violação;

IV. não permitir acesso de terceiros ao correio eletrônico por meio da senha pessoal;

V. responsabilizar-se pelas mensagens e anexos enviados e/ou recebidos;

VI. sair do acesso do e-mail institucional toda vez que se ausentar da estação de trabalho, evitando o uso indevido por terceiros;

VII. comunicar o recebimento de mensagens com os conteúdos indevidos ao Departamento de Tecnologia da Informação;

VIII. efetuar a exclusão de e-mails da pasta Lixeira e de e-mails desnecessários, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo;

IX. notificar ao Departamento de Tecnologia da Informação a ocorrência de alterações que afetem o cadastro do usuário de e-mail;

X. incluir no recurso "assinatura de e-mail" a identificação, contendo pelo menos os seguintes dizeres referente ao remetente: nome do usuário, função que exerce no IGEPREV e setor a que pertence, além de um aviso legal, referenciando a confidencialidade da informação, quando for o caso;

Art. 24. São deveres dos usuários dos grupos de e-mail:

I. utilizar a ferramenta de distribuição de mensagens exclusivamente para troca de mensagens que sejam de interesse institucional ou do grupo;

II. não permitir acesso de terceiros às listas de distribuição de e-mail;

III. guardar sigilo funcional das discussões travadas nos respectivos grupos;

IV. notificar ao Departamento de Tecnologia da Informação quando do recebimento de mensagens que contrariem o disposto nesta Política.

Art. 25. O Departamento de Tecnologia da Informação comunicará à Diretoria Executiva as irregularidades constatadas, a fim de que sejam tomadas as providências cabíveis.

Art. 26. Quaisquer violações às normas de segurança da informação e comunicação do IGEPREV ensejarão sanções administrativas, cíveis e criminais, caso aplicáveis.

Art. 27. A caixa postal de correio eletrônico terá o valor inicial de 100MB, podendo ser ampliada conforme disponibilidade de espaço, ficando o controle sob responsabilidade do Departamento de Tecnologia da Informação.

Seção VI
Da Utilização do Mensageiro Corporativo

Art. 28. O mensageiro corporativo é um sistema de acesso voluntário dos usuários da rede, destinado à troca de mensagens instantâneas entre seus usuários.

§1º O acesso ao mensageiro corporativo do IGEPREV é restrito aos usuários cadastrados na rede de informática da Instituição.

§2º O Departamento de Tecnologia da Informação é responsável pela instalação, manutenção e armazenamento das informações que circulam no mensageiro corporativo.

§3º As reclamações pertinentes ao conteúdo de mensagens veiculadas no mensageiro corporativo deverão ser encaminhadas à Diretoria Executiva, para eventual provocação da suspensão do acesso e/ou apuração de eventuais faltas funcionais.

CAPÍTULO III
DOS EQUIPAMENTOS DE INFORMÁTICA, MANUTENÇÃO E SOFTWARES

Seção I
Da Instalação e Manutenção dos Equipamentos

Art. 29. A instalação e desinstalação de equipamentos de informática nas dependências do IGEPREV, incluindo as unidades do interior, é de responsabilidade do Departamento de Tecnologia da Informação, mediante prévio agendamento pelo usuário de, no mínimo, 02 (dois) dias.

§1º Havendo necessidade de mudança do local dos recursos computacionais, o chefe do departamento fará solicitação, por meio dos canais de atendimentos disponibilizados pelo Departamento de Tecnologia da Informação, informando o motivo, o número do patrimônio, a nova localização e quem é o responsável pelo equipamento.

§2º No caso de efetiva mudança do equipamento, deverá o Departamento de Tecnologia da Informação informar a Área de Patrimônio sobre a alteração.

Art. 30. A manutenção preventiva e corretiva dos equipamentos de informática do IGEPREV é de responsabilidade exclusiva do Departamento de Tecnologia da Informação, e será realizada por técnicos de informática próprios da Autarquia ou por empresa terceirizada, conforme o caso.

§1º Havendo necessidade de manutenção em equipamentos de informática, deverá o usuário comunicar o Departamento de Tecnologia da Informação por meio do link link, constante na página da Intranet.

§2º O usuário deverá especificar detalhadamente o defeito apresentado nos recursos computacionais ou tecnológicos na ocasião da solicitação do suporte técnico ao Departamento de Tecnologia da Informação;

§3º A permanência dos equipamentos de informática para manutenção no Departamento de Tecnologia da Informação deverá observar que:

a) o Departamento de Tecnologia da Informação tem o prazo de até 04 (quatro) horas para informar ao usuário sobre a situação do equipamento, o diagnóstico e a previsão para devolução;

b) no caso do equipamento estar na garantia, será aberto um chamado junto à autorizada para adoção das providências de acordo com prazo de garantia de cada fabricante, que será repassado ao usuário do equipamento;

c) no caso das estações de trabalho e servidores de redes serem enviados para manutenção externa, recomenda-se a retenção das mídias de armazenamento, de modo a preservar os dados contidos.

Art. 31. É vedada a manutenção de equipamentos de informática particulares, incluindo *hardware* e *software*, por técnicos do Departamento de Tecnologia da Informação no âmbito do IGEPREV.

Art. 32. Todo computador é entregue lacrado e cabe ao respectivo usuário responsável pelo equipamento mantê-lo íntegro, de forma a garantir a inviolabilidade e segurança.

Seção II
Da Cópia de Segurança (Backup)

Art. 33. O IGEPREV possui sistema de backup que armazena cópia das informações e/ou dados que circulam na rede institucional em meio digital para assegurar recuperação, quando se fizer necessário.

Art. 34. O Departamento de Tecnologia da Informação do IGEPREV é responsável pelo backup das informações que trafegam na rede da Instituição.

Parágrafo único. O backup é realizado diariamente no horário compreendido entre 20h e 06h.

Art. 35. O IGEPREV conta com um servidor de rede situado no prédio sede, para armazenar as informações e/ou dados institucionais que trafegam na rede da Instituição.

§1º É vedada a gravação no servidor de rede, de arquivos que não contenham relação com as atividades desenvolvidas pelo IGEPREV, tais como, músicas, fotos, vídeos e outros, exceto em caso de imprescindível necessidade, a qual deve ser previamente comunicada ao Departamento de Tecnologia da Informação, com a devida motivação e justificativa.

§2º É de responsabilidade exclusiva do Departamento de Tecnologia da Informação a realização de backups diários e, quando necessário, as respectivas restaurações.

§3º É de responsabilidade dos servidores, principalmente àqueles que atuam no Interior do Estado, quando não houver servidor de rede, salvar os arquivos armazenados no disco rígido - HD (winchester) do computador em que trabalham em outro meio, a fim de preservar a informação no caso de erro ou defeitos nos equipamentos.

CAPÍTULO IV
DAS SENHAS DE ACESSOS

Art. 36. A senha de acesso é pessoal e intransferível, cabendo ao detentor sua guarda, sigilo e responsabilidade pelo uso.

§1º o usuário é o único responsável pelo uso da sua identificação (login e senha), pelo que quaisquer ações praticadas durante a utilização desta identificação será de sua inteira responsabilidade.

§2º caso o usuário perceba que outra pessoa possa estar utilizando seu login e senha de acesso aos recursos computacionais do IGEPREV, deverá informar imediatamente ao seu superior hierárquico que, após as medidas cabíveis, solicitará ao Departamento de Tecnologia da Informação para efetuar a troca da senha e auditoria das atividades executadas com o login e senha em questão.

Art. 37. Preferencialmente a senha deverá possuir no mínimo 08 (oito) caracteres, contendo letras maiúsculas, minúsculas, números e caracteres especiais.

Parágrafo único. O usuário deverá alterar sua senha de acesso à rede e aplicativos a cada 60 (sessenta) dias, evitando repetição e obedecendo aos critérios de segurança conforme descrito no *caput* deste artigo.

CAPÍTULO V
DOS SERVIDORES DE PRODUÇÃO E BANCO DE DADOS

Art. 38. Recomenda-se que o acesso ao servidor (equipamento) de produção pela equipe do Departamento de Tecnologia da Informação seja realizado através de autenticação por usuário e chave pública, onde cada integrante deverá possuir seu usuário exclusivo.

Art. 39. Toda operação realizada no servidor de produção deverá ser registrada em logs.

Art. 40. Recomenda-se que cada integrante da equipe técnica que desempenhe atividades no banco de dados possua seu usuário de acesso exclusivo e não um usuário padrão disponível para todos.

Art. 41. Recomenda-se que sejam registrados os logs de conexões e operações no banco de dados, bem como as provenientes a partir de qualquer cliente web, aplicativos desktops e terminal/shell.

Art. 42. Recomenda-se a definição de estratégia de individualização das ações executadas por cada membro da equipe do Departamento de Tecnologia da Informação, principalmente em relação ao acesso de informações sensíveis da base de dados do IGEPREV.

CAPÍTULO VI
COMITÊ DA POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

Art. 43. Para atender às demandas da Política da Segurança da Informação fica instituído o "Comitê da Política da Segurança da Informação" que será composto, no mínimo, pelos seguintes integrantes:

I. pelo Presidente do IGEPREV ou um integrante por ele indicado;

II. pelo Vice-Presidente do Instituto;

III. pelo Gerente Geral de Administração;

IV. um integrante do Departamento de Tecnologia da Informação; e

V. um integrante da Assessoria de Planejamento.

§1º O "Comitê da Política da Segurança da Informação" terá como Presidente o Presidente do IGEPREV ou um integrante por ele indicado e como Secretário o Gerente Geral de Administração.

§2º Em caso de ausência, afastamento ou impedimento, os integrantes do "Comitê da Política da Segurança da Informação", se necessário, indicarão seus substitutos.

§3º O "Comitê da Política da Segurança da Informação" reunir-se-á, ordinariamente, uma vez a cada trimestre e, extraordinariamente, por convocação de seu Presidente.

§4º Por deliberação do "Comitê da Política da Segurança da Informação" ou de seu Presidente, poderão ser convidados a participar de reuniões pessoas físicas ou jurídicas que possam contribuir para o esclarecimento das matérias a serem apreciadas.

§5º Ao Presidente do "Comitê da Política da Segurança da Informação" compete instituir comissões para auxiliar a tomada de decisão sobre assuntos de natureza técnica, definindo, no ato de constituição, seus objetivos específicos, sua composição e prazo para a conclusão dos trabalhos.

Art. 44. Compete ao "Comitê da Política da Segurança da Informação":

I. elaborar e aprovar o seu regimento interno;

II. estabelecer políticas e diretrizes da Política da Segurança da Informação, alinhadas aos objetivos estratégicos do IGEPREV;

III. definir as prioridades dos investimentos em Segurança da Informação;

IV. estabelecer as prioridades para execução de projetos da Segurança da Informação;

V. definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de Segurança da Informação;

VI. administrar e gerenciar a implantação, manutenção e aperfeiçoamento dos serviços e sistemas de Segurança da Informação.

CAPÍTULO VI
DAS DISPOSIÇÕES GERAIS

Art. 45. Compete à Diretoria Executiva deliberar sobre a contratação de empresa especializada em auditoria da segurança da informação ou solicitar auditoria do órgão de Tecnologia da Informação da estrutura administrativa do Poder Executivo Estadual.

Art. 46. A autorização para utilizar os recursos computacionais do IGEPREV é facultada a servidor, seja efetivo, comissionado ou à disposição, estagiário, colaborador ou prestador de serviço e demais servidores de instituições conveniadas, mediante abertura de conta pessoal junto ao Departamento de Gestão de Pessoas.

Art. 47. Todos os usuários autorizados têm o dever de noticiar ao Departamento de Tecnologia da Informação tentativa de acesso não autorizado, uso indevido ou qualquer ocorrência que evidencie desrespeito a esta Política, devendo tomar imediatamente as providências necessárias que estiverem ao seu alcance para garantir a segurança, integridade e a conservação dos recursos computacionais do IGEPREV.

Art. 48. O Departamento de Tecnologia da Informação deverá adotar uma política de limpeza de mídias de armazenamentos para estações de trabalho e servidores de rede, utilizando-se de ferramentas para sobrescrita de dados, de modo a reduzir a possibilidade de recuperação dos arquivos, e em caso de impossibilidade de realizar a ação, recomenda-se a retenção e posterior destruição da mídia de armazenamento.

Art. 49. Quanto aos colaboradores do Departamento de Tecnologia da Informação com vínculo externo (estagiário, terceirizado etc), recomenda-se a supervisão de um profissional do quadro do IGEPREV em relação a acesso a dados sensíveis e nos atendimentos *in loco*.

Art. 50. O Departamento de Tecnologia da Informação deverá criar políticas complementares a Esta, quando for necessário, não sobrepondo as diretrizes aqui estabelecidas e submetendo-as ao crivo da Diretoria Executiva, a fim de preservar os interesses Institucionais, acompanhando as atualizações tecnológicas e novas políticas de segurança e boas práticas.

Parágrafo único. As políticas do Departamento de Tecnologia da Informação aprovadas pela Diretoria Executiva deverão ser publicadas na intranet para conhecimento de todos.

Art. 51. A violação das normas descritas nesta Política implicará em responsabilização disciplinar, independentemente da responsabilidade civil e penal.

Art. 52. Serão alcançados por esta Política os estagiários do IGEPREV, funcionários terceirizados, colaboradores, prestador de serviço, voluntários e demais servidores de instituições conveniadas que, para o exercício de suas funções, possuam credenciamento de acesso aos sistemas de informações do IGEPREV.

Art. 53. Os casos omissos serão decididos pela Diretoria Executiva.

SHARLLES FERNANDO BEZERRA LIMA
Presidente

RURALTINS

PORTARIA DE FISCAL Nº 23/2021/GABPRES - RURALTINS.

O PRESIDENTE DO INSTITUTO DE DESENVOLVIMENTO RURAL DO ESTADO DO TOCANTINS - RURALTINS, no uso das suas atribuições que lhe confere o Regimento Interno aprovado pelo Decreto nº 10.643, de 11 de julho de 1994, Ato de Nomeação nº 1.132 - NM, de 16 de Novembro de 2020, publicado no DOE Nº 5.726, página 01,

CONSIDERANDO a necessidade de acompanhamento de fiscal para todos os contratos públicos;

CONSIDERANDO que os gastos devem sempre ser fiscalizados;

R E S O L V E:

Art. 1º Designar os servidores abaixo relacionados para sem prejuízo de suas atribuições, exercerem o encargo de Fiscal de Contrato, bem como seu respectivo substituto, para os casos de impedimentos e afastamentos legais do titular do contrato elencado a seguir:

Número do Contrato	Número do Processo	Fiscal do Contrato	Fiscal Substituto	Contratado e Objeto do Contrato
009/2021	2019/34490/000334	Celio Cota De Andrade Matricula nº 957309-2	Luciléia Cheyla Karvat Matricula nº 961027-5	TICKET SOLUCOES HDFGT S/A, referente a prestação de serviços de gerenciamento de abastecimento, implantação e operação de sistema informatizado/integrado com utilização de cartão magnético via WEB, que permita o fornecimento de combustíveis (gasolina comum e diesel S10) e aditivos através de rede de postos credenciados pela Contratada para atender à frota de veículos do Instituto de Desenvolvimento Rural do Estado do Tocantins - RURALTINS