Prefeitura de Goiânia
Instituto de Previdência dos Servidores do Município de Goiânia
Gabinete da Presidência

PORTARIA Nº 435, DE 25 DE MARÇO DE 2024

A PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE GOIÂNIA – GOIANIAPREV, no uso das atribuições legais que lhes são conferidas pelo Art. 7º do regimento interno do órgão, aprovado pelo Chefe do Executivo Municipal através do Decreto nº 304, de 19/01/2021, e a vista do que consta no processo SEI n.º 23.20.000000856-5,

CONSIDERANDO as exigências as exigências da Lei nº 9.609, de 19/02/1998, que dispõe sobre a proteção da propriedade intelectual de software, sua comercialização no País e dá outra providências, da Lei nº 12.527, de 18/11/2011, atualizada pela Lei nº 12.737, de 30/11/2012, que dispõe sobre a tipificação criminal de delitos informáticos, e da Lei nº 13.709, de 14/08/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que regula o acesso à informação;

CONSIDERANDO - A necessidade de produzir e propor normas, planos, procedimentos, mecanismos de proteção e instruções reguladoras específicas, reduzindo riscos de falhas, danos e prejuízos a informação;

CONSIDERANDO – O Objetivo de estabelecer estratégias, definir responsabilidades e competências que garantam a segurança das informações em acordo ao constante no Regime Próprio de Previdência Social - RPPS, reconhecidamente necessários ao desempenho das atribuições do GOIANIAPREV;

CONSIDERANDO a Portaria MPS 185, de 14/05/2015, atualizada até 02/01/2018, instituiu o Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios - "Pró-Gestão RPPS" na forma que estabelece o item 3.1.5 do manual (versão 3.5 com vigência e publicada em 17/01/2024),

RESOLVE:

Art. 1º Fica Instituída a Política de Segurança da informação do Instituto de Previdência dos Servidores do Município de Goiânia – GOIANIAPREV, tendo por objetivo o estabelecimento de diretrizes estratégicas, aplicada e restrita a todos os servidores públicos e prestadores de serviços que utilizem o ambiente de processamento de dados ou que tenha acessos às informações do Instituto.

Art. 2º Para fins desta Política, considera – se:

- **Informação:** São dados, processados ou não, que podem ser utilizados na produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato. A informação tem um valor altamente significativo e pode representar grande poder para quem a possui.

- **Segurança da Informação –** Conjunto de medidas que estabelece a **proteção de dados** contra ameaças diversas.

- **Gestão de segurança da informação** – é o resultado da sua aplicação planejada, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação, no uso da legislação e das normas PSI.

- **Classificação da informação -** a informação é um ativo essencial e precisa ser protegida quanto a eventuais ameaças observando os seguintes princípios básicos:

• **Confidencialidade**: Proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas.

• **Integridade**: Garantia da exatidão das informações e dos métodos de processamento.

• **Disponibilidade**: Garantia de que os usuários autorizados e os interessados tenham acesso às informações.

• **Autenticidade**: "Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações."

I. **As informações podem ser classificadas em:**

a) **Informações públicas -** É uma informação do GOIANIAPREV com linguagem e formato dedicado à divulgação ao público, sendo de natureza informativa. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

b) **Informações internas -** representam baixo nível de confidencialidade, são aquelas que não podem ser divulgadas, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação, quando o acesso externo às informações deve ser negado;

c) **Informações confidenciais -** é o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem do GOIANIAPREV. São protegidas contra tentativas de acesso externo;

d) **Informações restritas -** é o nível intermediário de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de Colaboradores, são protegidas por controle de acesso a módulos de sistemas e/ou diretórios em nuvem.

II. **Do Ciclo de vida*:***

a) O ciclo de vida da informação é composto por quatro etapas:

✓ **Manuseio,** este é o momento em que a informação é criada e manipulada.

✓ **Armazenamento** Nesta etapa a informação é tanto para o armazenamento quanto para a guarda (seguindo sempre uma tabela de classificação dos documentos).

✓ **Transporte** Será nesta fase em que a informação será transportada/encaminhada, (envio do documento físico ou eletrônico),

✓ **Descarte** Momento em que a informação é descartada, ou seja, eliminada como arquivo, no uso pleno de todas as normativas legais da PSI. (tabela de temporalidade)

b) Atingindo a sua segurança, usando seu tempo de vida nas três idades:

✓ Corrente (1ª **idade**)
✓ Intermediário (2ª **idade**)
✓ Permanente (3ª **idade**)

Art. 3º Produção/Transmissão/ Tratamento da Informação

I - Produção:

A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, nuvens, equipamentos portáteis (HD externo, pendrive, outros), e até mesmo por meio da comunicação oral. Toda informação relacionada às operações do GOIANIAPREV, gerada ou desenvolvida nas dependências da mesma, constitui ativo desta organização, sendo essencial à sua existência. Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

GOIANIAPREV defende a proteção da informação, a fim de evitar riscos e ameaças, tais como alterações, divulgação e destruição não autorizadas, provenientes de erros, fraudes, vandalismo, espionagem ou sabotagem, o que pode comprometer a confidencialidade, integridade ou disponibilidade dessas informações.

II (Transmissão) O acesso aos diversos serviços de informática, como sistemas, e-mail, rede local, WebService, entre outros, ocorre mediante autenticação do usuário através de seu nome de usuário (login) e senha (password). Tal processo visa garantir que o acesso à informação seja obtido apenas por pessoas autorizadas (garantia de confidencialidade). Cada usuário é responsável pela escolha de suas senhas pessoais.

Será disponibilizado em rede um diretório de arquivos por gerência para transferência e armazenamento de dados entre usuários com caráter temporário.

É de responsabilidade exclusiva dos usuários do setor manter, neste diretório, as informações produzidas a fim de facilitar as consultas e para que essas sejam preservadas através das rotinas de segurança e backup.

III - Tratamento - A informação deve receber proteção adequada em observância aos princípios e diretrizes da Política da Segurança da Informação do GOIANIAPREV em todo o seu ciclo de vida, que compreende:

- ✓ Coleta;
- ✓ Produção;
- ✓ Recepção;
- ✓ Classificação
- ✓ Utilização;
- ✓ Acesso;
- ✓ Reprodução;
- ✓ Transmissão;
- ✓ Distribuição;
- ✓ Processamento;
- ✓ Arquivamento;
- ✓ Armazenamento;
- ✓ Eliminação;
- ✓ Avaliação / controle da informação;
- ✓ Modificação;
- ✓ Comunicação;
- ✓ Transferência;
- ✓ Difusão ou extração.

Art. 4º Das Responsabilidades:

I. Gestão de Pessoas

- ✓ Apurar as sanções disciplinares e administrativas, indicadas pela Tecnologia da Informação em relação ao uso dos dados;
- ✓ Reportar via comunicação interna através do sistema SEI, à área de tecnologia da informação, ausência ou desligamento de funcionários para providências quanto ao controle de acesso aos sistemas de informação;
- ✓ Informar aos colaboradores e coletar assinatura do termo de Responsabilidade de Segurança da Informação, anexando ao dossiê;
- ✓ Apoiar em programas de treinamentos e educação para implementação e manutenção da política de segurança junto aos colaboradores;
- ✓ Informar a área de tecnologia da informação sobre os prestadores de serviços para serem assinados os termos de responsabilidade.

II. Usuários:

- ✓ Ler, entender, respeitar e fazer cumprir a política da segurança;
- ✓ Assinar os Termos de Responsabilidade de Segurança da Informação;
- ✓ Deverá solicitar os acessos aos sistemas e rede do GOIANIAPREV;

✓ Deverá possuir um código de acesso atrelado a uma senha previamente cadastrada, sendo esta pessoal e intransferível;

✓ As informações não devem ser obtidas sem as devidas proteções e autorizações do Presidente da Pasta;

✓ Somente softwares homologados e autorizados podem ser utilizados no ambiente computacional do GOIANIAPREV;

✓ Não usar, inspecionar, copiar ou armazenar programas de computadores, ou qualquer outro material não liberado, sob pena de violação da legislação de propriedade intelectual pertinente;

✓ Não é permitido compartilhar pastas de arquivos pessoais nos servidores da instituição. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;

✓ Prestadores de serviços contratados direta ou indiretamente pelo GOIANIAPREV e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais devem respeitar as obrigações previstas nos respectivos contratos de prestação de serviço, especialmente, para fins dessa Política, no que concerne à segurança da informação.

III. Setor de Tecnologia da Informação:

✓ Promover ações de conscientização sobre a Política de Segurança da Informação;

✓ Definir, implementar e revisar os controles da Política da Segurança da Informação;

✓ Elaborar programas de treinamento para capacitação de usuários;

✓ Definir requisitos e especificar instruções para utilização do teletrabalho (home office) quando for o caso;

✓ Prestar assessoramento técnico à Alta Direção à Lei Geral de Proteção de Dados;

✓ Desenvolver, implementar e manter planos de continuidade de TI os quais visam garantir as operações em casos de desastre e indisponibilidade dos sistemas de informação;

✓ Gestão de ativos de redes.

✓ O Setor de T.I é responsável pelos sistemas operacionais e aos demais programas de computadores instalados;

✓ Equipamentos pessoais somente poderão ser usados no âmbito do GOIANIAPREV com autorização prévia do Departamento de T.I e com as devidas justificativas da Chefia imediata.

✓ Quaisquer movimentações de equipamentos de informática deverão ser comunicadas com antecedência à área de T.I e informadas por escrito ao departamento de Patrimônio.

✓ Os recursos de Tecnologia da Informação pertencentes ao GOIANIAPREV que estão disponíveis para os usuários devem ser utilizados em atividades estritamente relacionadas às funções institucionais desempenhadas pela Autarquia.

IV. Alta Gestão:

✓ Prover a orientação e o apoio necessário às ações de segurança da informação, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes, tendo como responsabilidades:

✓ Aprovar a política e as normas de segurança da informação e suas revisões;

✓ Tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação, mediante a apresentação de propostas da T.I.

V. Gestores:

Secretário Executivo, Chefe de gabinete, Diretores, Gerentes, e demais cargos de chefia, administrando pessoas e/ou processos.

Compete ao Gestor da Informação:

✓ Classificar a informação sob sua responsabilidade e gerada por servidores, fornecedores ou outras entidades externas, que devem participar do processo de definição do nível de sigilo da informação;

✓ Inventariar todos os ativos de informação sob sua responsabilidade;

✓ Manter um controle efetivo da informação estabelecendo e documentando os Perfis de acesso;

✓ Reavaliar periodicamente, fiscalizando o acesso da informação, solicitando o cancelamento quando necessário;

✓ Participar da investigação dos incidentes de segurança relacionados às informações sob sua responsabilidade.

VI. Comitê Gestor de Segurança da Informação

✓ Estabelecer um Comitê para a Política da Segurança da Informação, devendo ser multidisciplinar;

✓ O Comitê Gestor da Política de Segurança da Informação é o órgão colegiado consultivo e propositivo que tem a finalidade de colaborar com o Setor de TI para o desenvolvimento das políticas e ações do GOIANIAPREV na área de Tecnologia da Informação;

✓ Analisar, definir, coordenar, executar e avaliar ações de segurança da informação relativas aos objetivos estabelecidos na Política de Segurança da Informação do GOIANIAPREV;

✓ Elaborar e implementar a manutenção da melhoria de gestão da segurança da informação;

Da composição

✓ Deve ser composto obrigatoriamente pelos membros:

Diretoria Administrativa, Diretoria Previdenciária, Gerencia de cálculos e folha de pagamento de Benefícios Previdenciários, Diretoria de Benefícios Previdenciários, Controladoria Especial Previdenciária, Secretaria Executiva, Chefe de Gabinete.

Das atribuições do Comitê

✓ Sugerir ações visando o alinhamento do plano de desenvolvimento de tecnologia da informação com o planejamento estratégico do Instituto;

✓ Aprovar e revisar anualmente ou sempre que necessário a política de gestão de continuidade, a estratégia de continuidade e o processo de gerenciamento de continuidade de serviços essenciais de T.I do Instituto;

✓ Aprovar o processo de classificação e tratamento da informação, revisar anualmente e aperfeiçoá-lo sempre que necessário;

✓ Aprovar e manter o plano de continuidade dos serviços essenciais de TI;

✓ Garantir que o plano seja testado periodicamente e solicitar atualizações necessárias;

✓ Definir as funções de negócio vitais para as áreas judiciárias e administrativas do Instituto;

✓ Definir os serviços de TI mais relevantes para o Instituto;

✓ Apreciar os relatórios dos testes de recuperação de falhas, previstos no plano de continuidade;

✓ Aprovar ações periódicas de conscientização, educação e capacitação em segurança da informação em todas as áreas do Instituto;

✓ Definir as diretrizes para gestão de riscos de TI com impacto na prestação previdenciária, a estratégia institucional, a imagem do órgão e os serviços das áreas meio e fim do Instituto. E ainda a segurança da informação dos ativos críticos de TI;

✓ Acompanhar e avaliar periodicamente os relatórios de riscos, contendo as informações sobre sua identificação, avaliação e tratamento;

✓ Aprimorar continuamente propostas de normas e políticas de uso dos recursos da TI referentes à segurança da informação, tais como:

✓ Gerenciamento de identidade e controle de acesso lógico;

✓ Controle de acesso físico;

✓ Controle de acesso à Internet;

✓ Utilização do correio eletrônico;

✓ Utilização de equipamentos e aplicações de TI de forma segura, em observância a Política de Segurança da Informação;

✓ Tomar decisões sobre questões de segurança da informação e gestão de riscos não contempladas na política de segurança da informação e normas relacionadas;

✓ Propor e acompanhar planos de ação para aplicação da Política de Segurança da Informação, assim como campanhas de conscientização dos usuários;

✓ Receber e analisar as comunicações de descumprimento das normas referentes à Política de Segurança da Informação deste Instituto, apresentando parecer à autoridade/órgão competente para sua apreciação;

✓ Uniformizar as políticas de Tecnologia da Informação do Instituto;

✓ Elaborar o Plano de Desenvolvimento de Tecnologia da Informação - PDTI, e o Plano de Metas;
✓ Analisar e emitir parecer sobre as propostas encaminhadas à comissão pela TI;
✓ Apreciar e emitir parecer sobre os relatórios das atividades desenvolvidas;
✓ Subsidiar a Tecnologia da Informação no tocante às políticas de sua área de atuação;
✓ Promover a integração entre os setores de TI e os outros setores;
✓ Aprovar o plano de capacitação de pessoal da área de TI;
✓ A classificação da informação obedecerá às diretrizes estabelecidas pela Lei de Acesso à Informação – LAI – regulamentada pelo Decreto n.º 7.724/2012, do Governo Federal, visando minimizar os riscos aos serviços e atividades, bem como preservar a imagem institucional.
✓ O Modelo de Gestão deve contemplar, no mínimo, os seguintes processos:

- O Planejamento Estratégico da Segurança da Informação;
- A Gestão da Política de Segurança, das **Normas** e dos **Procedimento**s;
- A Classificação da Informação;
- A Tabela Temporalidade;
- O Controle de Acesso;
- A Gestão de Riscos;
- A Gestão da Continuidade do Negócio;
- A Gestão de Resposta a Incidentes;
- A Gestão de Mudanças;
- A Divulgação e Conscientização;
- A Auditoria e Conformidade;

VII. Gerência de Atendimento, Cadastro e Protocolo e Arquivo - GERACA

✓ Implementar procedimentos que garantam a confidencialidade de documentos/processos físicos, digitais e híbridos, produzidos ou recebidos pelo GOIANIAPREV, desde sua entrada até o seu arquivamento e acondicionamento.

Art. 5º A política de mesa limpa:

✓ Consiste em não deixar informações confidenciais ou bens do GOIANIAPREV, incluindo, mas não se limitando, a papéis, pen-drives ou quaisquer outros tipos de mídias removíveis, acessíveis a outras pessoas sem a devida proteção, quando o funcionário estiver fora de sua estação de trabalho.
✓ Ao final do dia de trabalho, computadores portáteis devem ser devidamente trancados em gaveta ou armário, ou serem presos a cabos de segurança, ou levados pelo seu responsável, conforme estabelecido pelo respectivo gestor.
✓ O GOIANIAPREV tem direito de acesso a qualquer informação salva em formato eletrônico em seus equipamentos de rede ou “nuvem”, que se encontrem fisicamente no mobiliário do Instituto, como, por exemplo, em mesas, estantes, gaveteiros, armários, etc. Dessa forma, ainda que o Colaborador possa se utilizar da estrutura de tecnologia da organização para algum uso particular não conflitante, tais informações podem ser acessadas pelo GOIANIAPREV mesmo sem o prévio consentimento do respectivo Colaborador.

Art. 6º Utilização do telefone fixo, e-mails, teleconferências, videoconferências.

✓ O uso do telefone fixo deve ser para fins profissionais, sendo permitido para fins pessoais mediante autorização, desde que não sejam conflitantes com as atividades, nem prejudiquem qualquer lei, regulação ou regulamento e políticas internas do GOIANIAPREV.
✓ Deve-se sempre priorizar fazer ligações dentro do GOIANIAPREV, ou pelos meios eletrônicos de telefonia e comunicação disponibilizados pela empresa via computador e/ou aplicativos aprovados pela Diretoria Administrativa (Departamento de T.I).
✓ Não se deve deixar mensagens confidenciais em secretárias eletrônicas, pois essas podem ser resgatadas por pessoas não autorizadas;
✓ Ao coordenar uma teleconferência ou videoconferência, deve-se garantir que todos os participantes foram devidamente autorizados antes de começar a reunião.

Art.7º Integram o patrimônio físico e intangível.

✓ Imóveis, instalações, veículos, equipamentos, estoques, valores, planos, produtos, tecnologia, estratégia de negócio e de comercialização, informações, pesquisas e dados;

✓ Não podem ser utilizados equipamentos ou outros recursos do GOIANIAPREV para fins particulares, salvo se previamente autorizado pelo gestor de área, sendo a referida aprovação vetada nos casos em que interfira no seu trabalho, ou se ainda:

- Interferir ou concorrer com os negócios do GOIANIAPREV;
- Fornecer informações a terceiros;
- Envolver solicitação comercial ou outra solicitação não apropriada ao negócio;
- Envolver custo adicional para o GOIANIAPREV.

Art.8º O uso dos recursos de Internet e e-mail deve obedecer às seguintes regras:

✓ Em acordo com as diretrizes da Secretaria Municipal de Inovação, Ciência e Tecnologia – SICTEC, a Política de uso da internet foi norteada por 04 (quatro) diretivas, duas de caráter técnico e duas de caráter ético profissional:

➢ **Diretivas Técnicas:**

1. **Segurança dos dados e sistemas**: O acesso à internet não pode comprometer a segurança de dados e sistemas, ou seja, evitar que atitudes do usuário durante o acesso à Internet comprometam a segurança.
2. **Uso do Link de Internet**: Evitar que um ou alguns usuários aloquem todo, ou grande parte do link de Internet, prejudicando assim o desempenho do restante dos acessos.

➢ **Diretivas Éticas**:

1. **Comportamentos ilegais, imorais e não éticos**. Evitar que o acesso à Internet seja utilizado para efetuar atos ilegais, imorais, profissionalmente não éticos ou ainda que denigrem a imagem da Prefeitura de Goiânia/GOIANIAPREV.
2. **Produtividade no trabalho**: Como a Internet é extremamente diversa e possui vários entretenimentos, ela pode se tornar um grande consumidor de tempo e consequentemente um redutor da produtividade. Esta diretiva vem evitar que a Internet interfira negativamente na produtividade dos funcionários.

➢ **Estrutura**

Baseadas nas quatro diretivas, as normas e políticas foram estruturadas em seis partes:

1. Condições gerais: O acesso à Internet é franqueado prioritariamente objetivando a pesquisa, educação, suporte e aprendizado de assuntos do interesse da Prefeitura de Goiânia/GOIANIAPREV, entretanto será permitida a utilização moderada para o uso de caráter pessoal.

✓ O usuário é o único responsável pelo conteúdo das transmissões feitas através do e-mail a partir de sua conta e senha;

✓ O uso da conta de e-mail corporativo da Prefeitura de Goiânia/ GOIANIAPREV é para fins profissionais, sendo permitido seu uso pessoal com bom-senso, para assuntos que não sejam conflitantes com as atividades da PREFEITURA DE GOIÂNIA/ GOIANIAPREV nem que prejudiquem qualquer lei, regulação ou regulamento e políticas internas da PREFEITURA DE GOIÂNIA/ GOIANIAPREV.

✓ As mensagens de e-mail são confidenciais, somente podendo ser acessadas pelo remetente e seu(s) destinatário(s). É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela;

✓ Não devem ser abertos arquivos ou executados programas anexados aos e-mails sem antes ter certeza de sua procedência e existência de prévia expectativa do recebimento da mensagem;

✓ Dentro do aplicativo ou visualizador de e-mails, devem sempre estar desabilitadas as opções que permitam abrir ou executar automaticamente arquivos ou programas anexados às mensagens;

✓ Não deve ser utilizado e-mail para fins ilegais;

✓ Não devem ser transmitidos quaisquer materiais ilegais ou de qualquer forma censuráveis através deste serviço;

✓ Não devem ser transmitidos quaisquer materiais que violem direitos de terceiros, incluindo, mas sem limitação, direitos de propriedade intelectual;

✓ Não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis;

✓ O Colaborador não pode obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço;

✓ Não devem ser utilizados os serviços de e-mail para transmitir quaisquer materiais que contenham vírus, arquivos do tipo "Cavalo de Troia" ou outro programa prejudicial;

✓ Não devem ser transmitidas mensagens não-solicitadas, conhecidas como spam ou junk mail, correntes, chain letters ou distribuição em massa de mensagens não-solicitadas, salvo mensagens informativas de produtos e serviços da PREFEITURA DE GOIÂNIA/GOIANIAPREV, aprovada por um Diretor, por lista controlada e via ferramentas oficiais contratas pela PREFEITURA DE GOIÂNIA/GOIANIAPREV. Quando este envio ocorrer, deve contar com sistema de cancelamento de cadastramento na própria mensagem;

✓ Mensagens com assuntos confidenciais não devem ser impressas em impressoras usadas por outros usuários, sem que se esteja cuidando para retirar a impressão antes do acesso físico ao conteúdo impresso, de forma inadvertida, pelos demais usuários;

✓ O e-mail deve estar ativo sempre que o usuário estiver trabalhando no microcomputador. Quando este se afastar de sua estação de trabalho, deve encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal;

✓ É proibido aos administradores de rede ou e-mail ler mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte, salvo por necessidade de apuração de eventos que tenham causado danos, ou tenham sido classificados como potencialmente danosos à PREFEITURA DE GOIÂNIA/GOIANIAPREV ou a terceiros ou por determinações Diretoria de Administrativo Financeiro, desde que devidamente justificado, ou, ainda, de Reguladores ou Autoridades para apuração de eventos de infração de alguma regulação, ou legislação;

✓ Não é permitido enviar músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura de rede local ou que violem as leis de direitos autorais.

✓ É permitido o uso de serviços de mensagens ou chat (WhatsApp, Hangouts, Skype, Messenger, etc.) desde que para fins profissionais. O uso pessoal desses aplicativos deve ser limitado e com bom senso, nunca com finalidades conflitantes com os interesses do GOIANIAPREV, bem como nunca infringindo nenhuma lei, norma, regulamentação e políticas internas da PREFEITURA DE GOIÂNIA/GOIANIAPREV.

2. Proibições:

É vedado o uso da Internet e Correio Eletrônico para:

✓ Acessar a sites pornográficos, obscenos, racistas, de conteúdo claramente ofensivo ou contra a legislação;

✓ Obter *softwares*, arquivos ou informações de qualquer natureza, amparados por lei de proteção à privacidade ou à propriedade intelectual, excetuando-se os casos em que, explicitamente, o material detiver as respectivas licenças ou autorizações para uso livre;

✓ Transmitir, arquivos contendo “vírus” de computador ou códigos que, de qualquer forma, possam prejudicar os programas, arquivos ou equipamentos;

✓ Obter informações a respeito de terceiros sem anuência do titular;

✓ Tentar violar ou violar sistemas de segurança da informação;

✓ Obter ou tentar obter acesso não autorizado a qualquer equipamento, *software* ou sistema;

✓ Violar ou tentar violar as regras estabelecidas no firewall, ou na política de acesso à Internet, incluindo, mas não limitado a:

✓ Uso de Webproxies, Proxy Virtual, Proxy Anônimo, VPN ou similar;

✓ Uso de protocolo HTTPS para evitar a lista de sites bloqueados;

✓ Uso de tunelamento;

✓ Uso de re-encapsulamento;

✓ Veicular mensagens ou informações consideradas ofensivas aos princípios éticos, morais ou religiosos;

✓ Enviar propagandas, avisos ou informações não autorizadas, caracterizadas como SPAM;

✓ Transmitir ou obter informações e materiais, mesmo que públicos, em desacordo com a legislação brasileira;

✓ Falar ou escrever em nome da Prefeitura de Goiânia/GOIANIAPREV para os meios de comunicação, sites de bate-papo (chat, rooms e outros), programas de mensagens (WhatsApp, Telegram, Skype e outros), grupos (fóruns, newsgroups e outros) ou mídias sociais (Facebook. Twitter, Instagram, Snapchat e outros), exceto se seu cargo ou função possui esta permissão;

✓ Divulgar informações consideradas confidenciais ou estratégicas.

3. Responsabilidade:

✓ É de inteira responsabilidade do usuário (O termo de responsabilidade refere-se às responsabilidades previstas nas Leis n.º 9.609 de 19/02/1998, 12527 de 18/11/2011 e a 13.709 de 14/08/2018);

✓ A responsabilidade do usuário se estende pelas consequências e/ou por quaisquer danos causados por estes arquivos;

✓ Download da Internet de qualquer tipo de arquivo (softwares, arquivos, imagens, documentos, multimídia, etc.);

✓ A responsabilidade do usuário se estende pelas consequências e/ou por quaisquer danos causados por estes arquivos;

✓ Determinar o tipo de licenciamento do software (freeware, livre, shareware, etc.);

✓ Adquirir sua licença (se necessário)

✓ Saber se a sua utilização não está violando algum item ou artigo do seu licenciamento;

✓ Saber se o seu download / utilização não está violando algum direito autoral;

✓ Determinar se o software possui funções, não descritas, que causam prejuízos;

✓ Determinar se o arquivo viola algum tipo de lei.

✓ Qualquer problema, dano ou prejuízo, direto ou indireto, causado pela utilização de quaisquer serviços oferecidos pela internet que não atende aos interesses da Prefeitura de Goiânia.

4. Bloqueio

✓ O controle de acesso à Internet será feito de um equipamento denominado de Firewall. Apesar de estar configurado para a aplicação das regras desta política, devido à grande diversidade da Internet, não é possível garantir o bloqueio ou liberação de todos os sites corretamente; por isso, fica determinado que:

a) O usuário poderá entrar em contato com o Depto. Suporte Técnico da SICTEC toda vez que um site for bloqueado ou liberado indevidamente. O método de contato está descrito na página que é retornada ao navegador avisando do bloqueio.

b) O uso da Internet está baseado nas políticas de acesso e não no bloqueio ou liberação do Firewall, ou seja, mesmo que o site for liberado pelo Firewall não significa que ele poderá ser acessado. A permissão ou negação de acesso deverá ser baseada nas políticas.

✓ **O controle de acesso à Internet fará (Firewall):**

1. Bloqueio a sites pornográficos, racistas e outros de conteúdo claramente ofensivo, contra a legislação;

2. Bloqueio a sites que dissemina vírus e afins, ou que contenham instruções para burlar regras de segurança;

3. Bloqueio de todas as portas TCP/IP de Entrada e Saída que não seja a porta 80, utilizada para navegação web, com isso alguns serviços disponíveis na Internet não funcionarão ou terão seu funcionamento prejudicado;

4. Para locais cujo link de acesso é inferior a 16mbps:

5. Bloqueio a sites de transmissão tipo streaming (rádios, vídeos, TV's online);

6. Bloqueio a sites de download tipo: Megaupload, Fileserv, Rapidshare, etc.

5. Logs

Todo acesso à Internet é registrado e fica disponível para consulta pela chefia, gerencia e pelo próprio usuário.

Para garantir a transparência deste controle, o usuário será informado todas as vezes que seu registro (log) foi verificado.

O log só estará disponível após a implantação da autenticação de usuários para acesso à Internet.

6. Flexibilização

✓ Qualquer necessidade de bloqueio ou liberação diferente desta política básica poderá ser solicitada à SICTEC que por meio de reunião conjunta com o órgão irá definir as personalizações do acesso.

✓ Liberações para programas já amplamente utilizados na prefeitura que utilize porta TCP/IP diferente da porta 80, tipicamente programas de FGTS, CEF, CAT, Secretaria da Previdência, etc, serão liberados através do envio de ofício para a SICTEC indicando o programa, informando qual endereço IP e porta TCP a ser liberada.

SISTEMAS COMPLETE, INTRANET E OUTROS SISTEMAS

1. O acesso ao Sistema Complete, Sistema Intranet e outros são feitos mediante um controle de acesso de usuários e senhas.

2. **A senha** é o meio de validação de acessos a recursos e serviços, funcionando como a assinatura digital do Colaborador, portanto, devem ser verificados os seguintes cuidados básicos para sua proteção:

a) Manter sua confidencialidade;
b) Criar senhas fortes, respeitando, ao menos, os critérios abaixo:

✓ As senhas não podem ser óbvias, como senhas sequenciais (ex.: sequências numéricas ou alfabéticas) ou derivadas de dados pessoais (ex.: nome ou data de nascimento do usuário);
✓ Devem ter pelo menos 8 caracteres, com ao menos um caractere especial e um número. Os acessos, validados por meio da utilização de senha, serão limitados aos recursos e serviços necessários para o desempenho das atividades exercidas por cada Colaborador, e poderão ser revogados rapidamente quando necessário.

3. **Gerente de Senhas** é uma atribuição dentro da Política de Segurança da Informação designada a uma ou mais pessoas cuja função é gerenciar o controle de acesso dentro do órgão.

O Gerente de Senhas é nomeado através de ofício enviado pelo responsável (secretário ou presidente) da pasta (secretaria, companhia ou órgão). Cada órgão deverá nomear no mínimo 1 (um) gerente de senhas, sendo que a recomendação é que sejam entre 03 (três) e 04 (quatro) gerentes por órgão, dependendo do seu tamanho.

O Gerente de Senhas possui as seguintes competências COMPLETE:

1. Criar usuário no COMPLETE;
2. Criar usuário de Rede;
3. Regerar senha de usuário COMPLETE;
4. Regerar senha de usuários de Rede;
5. Bloquear usuários do COMPLETE;
6. Bloquear usuários de Rede;
7. Excluir usuários do COMPLETE;
8. Excluir usuários de Rede;
9. Desbloquear usuários do COMPLETE;
10. Desbloquear usuários de Rede;
11. Criar e-mail corporativo;
12. Excluir e-mail corporativo;
13. Conceder acessos a pastas do Servidor de Rede;
14. Remover acessos a pastas do Servidor de Rede;
15. Criar usuário GED (específico GOIANIAPREV);
16. Regerar senha de usuário GED (específico GOIANIAPREV);
17. Bloquear usuário GED (específico GOIANIAPREV);
18. Excluir usuário GED (específico GOIANIAPREV);

O Gerente de Senhas possui as seguintes competências INTRANET:
1. Criar usuário na INTRANET;
2. Conceder acessos aos sistemas do COMPLETE;
3. Conceder acessos aos sistemas da INTRANET;
4. Remover acessos aos sistemas do COMPLETE;
5. Remover acessos aos sistemas da INTRANET.

O Gerente de Sistemas (Gabinete do Prefeito) possui as seguintes competências SEI:

1. Concede os acessos através de solicitação via SEI autorizada pelo Presidente do GOIANIAPREV.

O Gerente de Sistemas possui as seguintes competências SIGEP:
1. Solicitar via SEI com Termo de Compromisso Individual e Compromissos de acessos assinados.

Tanto o Gerente de Senhas quanto o Gerente de Sistemas fazem as solicitações através de um Sistema de Controle de Acesso (informalmente chamado de Sistemas de Senhas), onde além das solicitações é

possível consultar os históricos dos pedidos (solicitações passadas), visualizar os pedidos por gerente e também saber qual funcionário atendeu à solicitação, dentre outras consultas.

OUTROS ITENS DE SEGURANÇA

- A senha do Sistema Complete expira a cada 45 (quarenta e cindo) dias, ou seja, é necessário à sua troca a cada 45 dias, o usuário é bloqueado em 3 (três) tentativas erradas e a senha deve possuir de 5 a 8 caracteres.
- Todos os equipamentos do GOIANIAPREV conectados no domínio da Prefeitura exigem senhas para "logon", ou seja, sem a identificação de um usuário ou senha válida no domínio não é possível utilizar o Windows;
- Todas as vezes que um usuário muda de lotação, departamento ou órgão no Recursos Humanos da Prefeitura ele perde todos os acessos e o usuário é bloqueado;
- Nenhum usuário de rede é administrador do seu computador, evitando assim proliferação de vírus ou trojans.
- Todos os computadores do GOIANIAPREV possuem software antivírus corporativo com gerenciamento centralizado. A SICTEC possui corpo técnico especializado que monitora a ocorrência de vírus na rede do GOIANIAPREV. O usuário não consegue desativar ou remover o software antivírus.
- É terminantemente proibida a instalação ou uso de softwares ilegais descritos na Lei n.º 9.609 de 19/02/1998 – Lei de Software, que dispõe sobre a proteção da propriedade intelectual de software, sua comercialização no País, e dá outras providências. Qualquer necessidade de novos programas ou sistemas deverá ser discutida com a SICTEC para providências.

2. INFRAESTRUTURA SISTEMAS (BACKUP, BANCO DE DADOS, CONTIGÊNCIA, CONTROLE DE ACESSO)

BACKUP

Servidores

Todos os dados pertinentes ao GOIANIAPREV deverão ser armazenados no Servidor de Rede, de responsabilidade de cada servidor do GOIANIAPREV este armazenamento.

A integridade e não perda dos dados armazenados no Servidor de Rede é de responsabilidade da **SICTEC**.

BANCO DE DADOS

Atualmente existem 03 (três) Banco de Dados, o ADABAS, o DB2, e o SQL Server, nestes bancos estão armazenados todos os dados dos sistemas corporativos da prefeitura de Goiânia/GOIANIAPREV.

Estes bancos possuem cópias de segurança diária de segunda a sexta-feira, com a seguinte retenção: 12 (doze) dias, dia-a-dia e uma cópia mensal com retenção de 05 (cinco) anos.

CONTINGÊNCIA

Os Sistemas da Intranet são executados em equipamentos virtualizados tolerante a falhas, ou seja, mesmo que o servidor ou disco que está executando os Sistemas da Intranet venham a falhar ele será executado em um novo servidor acessando outro disco.

O mesmo acontece para o controle de acesso à rede que possui diversos servidores de "login" (Controladores de Domínio) em paralelo.

O Data Center onde estão os computadores servidores possui energia estabilizada e tolerante a falhas através de Nobreak de 15 minutos e gerador de energia através de motor a diesel.

A temperatura do Data Center é controlada por um sistema de refrigeração com alerta para falhas.

Para falhas catastróficas semanalmente uma cópia dos principais dados de backup são retirados do Data Center e enviados a uma outra localidade.

CONTROLE DE ACESSO

O Data Center da **SICTEC** possui um controle de acesso através de verificação digital e câmeras de videomonitoramento, de tal forma que somente pessoas autorizadas conseguem adentrar ao Data Center e é possível recuperar a imagem de todas as pessoas que adentraram ao local.

Art.9º *USO DAS IMPRESSORAS*:

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização deste equipamento:

a) Quaisquer impressões, são retiradas na impressora mediante o uso da matrícula funcional e senha pessoal;

b) Esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;

c) As impressoras são ferramentas para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas pelo GOIANIAPREV. Impressões para finalidade pessoal devem ser limitadas e com bom-senso, nunca com finalidades conflitantes com os interesses do GOIANIAPREV, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e políticas internas do GOIANIAPREV;

d) Impressões coloridas apenas devem ser feitas apenas em caráter excepcional, quando a utilização da cor interferir na compreensão do documento ou quando a situação assim exigir.

***Art. 10º* GESTAO/RESPONSABILIDADE**

I – ***Gestão de incidentes*:** que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências;

II – ***Gestão de Riscos***: será estabelecido um processo de Gestão de Riscos, contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação, de modo a produzir subsídios para a Gestão de Continuidade dos Negócios. Os riscos devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e em fatores de risco como ameaça, vulnerabilidade, probabilidade e impacto;

III – ***Auditoria de Conformidade***: deverão ser realizadas periodicamente Auditorias de Conformidade nas quais as atividades do GOIANIAPREV estão submetidas, de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão;

IV –***Segurança Física***: Toda entrega de materiais, inclusive equipamentos e suprimentos, deve ser comunicada antecipadamente à área administrativa responsável pelo patrimônio/almoxarifado, com indicação do tipo de material e da unidade a que se destina e nome do servidor responsável pelo recebimento.

O acesso ao GOIANIAPREV será somente permitido para pessoas autorizadas, pelo monitoramento da recepção, acompanhado pelo guarda municipal ou vigilante terceirizado, de modo a controlar entrada e saída de visitantes, pessoal interno e estabelecer perímetros de segurança;

V – ***Acesso à Internet Uso de e-mail***: o serviço de correio eletrônico disponibilizado pela SICTEC/GOIANIAPREV constitui recurso institucional/Prefeitura disponibilizado na rede de comunicação de dados para aumentar a agilidade, segurança e comunicação oficial e informal;

VI ***– Capacitação e Aperfeiçoamento***: os servidores deverão ser continuamente, capacitados para o desenvolvimento de competências previdenciárias em conjunto com a Segurança da Informação;

VII – ***Acesso à Internet***: todos os servidores têm o direito de acesso à internet, com utilização exclusiva para fins diretos e complementares às atividades do setor, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que contribuam para o desenvolvimento de seus trabalhos;

VIII – ***Patrimônio Intelectual***: as informações, os sistemas e os métodos criados pelos servidores do GOIANIAPREV, no exercício de suas funções, são patrimônios intelectuais do Instituto, não cabendo a seus criadores

qualquer forma de direito autoral;

IX – ***Termo de Responsabilidade e Sigilo***: é o documento oficial que compromete colaboradores, terceirizados e prestadores de serviço com a PSI do GOIANIAPREV.

Art. **11º** A sensibilização e cultura da segurança, bem como da importância das informações processadas, dos seus riscos e suas vulnerabilidades, bem como dos impactos do não cumprimento ou de falhas de segurança, devem ser desenvolvidas e mantidas por meio treinamentos, palestras, seminários, e outros canais de comunicação disponíveis no âmbito do GOIANIAPREV.

Art. **12º** Controles Operacionais serão tratados em Procedimentos, Instruções de Trabalhos, Ordens de Serviços, Fluxos e Manuais, e estarão sujeitos a alterações constantes.

Art. **13º** Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pelo Comitê de Segurança da Informação do GOIANIAPREV, em parceria com outras entidades, quando necessário.

Art. **14º** A implementação da PSI-GOIANIAPREV será feita de forma gradual, de acordo com a disponibilidade técnica, recursos humanos, tecnológicos e financeiros, cujas ações serão priorizadas em virtude de seu grau de relevância, criticidade, impacto e investimentos envolvidos.

Art. **15º** Esta Portaria entrará em vigor na data de sua publicação.

Cientifique-se. Publique-se. Cumpra-se.

Goiânia, 25 de março de 2024.

CAROLINA ALVES LUIZ PEREIRA
Presidente

Documento assinado eletronicamente por **Carolina Alves Luiz Pereira**, **Presidente do Instituto de Previdência dos Servidores do Município de Goiânia**, em 25/03/2024, às 11:45, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://www.goiania.go.gov.br/sei informando o código verificador **3803512** e o código CRC **C75C0E7A**.

Avenida B, nº 155 -
- Bairro Setor Oeste
CEP Goiânia-GO

Referência: Processo Nº 23.20.000000856-5 SEI Nº 3803512v1