RESOLUÇÃO Nº 002/2024

APROVA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE DIVINÓPOLIS - DIVIPREV.

A Superintendência e o Conselho Administrativo do INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE DIVINÓPOLIS, usando das atribuições que lhe são conferidas por lei, e

CONSIDERANDO as definições do Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social, instituído pela Portaria MPS nº 185/2015.

CONSIDERANDO que a informação é um ativo essencial da organização e precisa ser adequadamente protegida;

CONSIDERANDO o compromisso do RPPS com a proteção das informações sob sua guarda e a formalização das normas para segurança;

CONSIDERANDO a deliberação do Conselho Administrativo pela aprovação da **Política de Segurança da Informação**, ocorrida na reunião ordinária realizada em 13 de março de 2024.

R E S O L V E:

Instituir a **Política de Segurança da Informação** no âmbito do INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE DIVINÓPOLIS, transcrita a seguir:

1. INTRODUÇÃO

Segurança da Informação (SI) é a disciplina dedicada à proteção da informação de forma a garantir a continuidade dos serviços, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de atuação de uma instituição.

A Política de Segurança da Informação (PSI), por sua vez, é o documento formal que orienta e estabelece as diretrizes corporativas para a proteção dos ativos de informação e a gestão da segurança da informação.

"Política de Segurança da Informação e Comunicações: documento aprovado pela Superintendência e o Conselho Administrativo do DIVIPREV, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações".

Os objetivos genéricos da Política de Segurança da Informação para o DIVIPREV são:

A. Certificar e garantir segurança com contato externo em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

B. Promover a conscientização de todos servidores pertinentes para compreensão e manuseio de situações relacionadas à segurança da informação;

C. Promover as ações necessárias à implementação e manutenção da segurança da informação.

2. CAMPO DE APLICAÇÃO

Os objetivos e diretrizes estabelecidos nesta Política de Segurança da Informação serão aplicados em toda a organização; deverão ser observados por todos servidores, órgãos colegiados, colaboradores e também a fornecedores e prestadores de serviço quando pertinente ou aplicável a área da informação, em qualquer meio ou suporte. Este documento, dentre outras diretrizes, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do órgão poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

3. SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICIPIO DE DIVINOPOLIS – DIVIPREV.

3.1 PRINCÍPIOS E OBJETIVOS

Além de buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade; são objetivos da Política de Segurança da Informação do DIVIPREV:

A. Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional.

B. Designar e definir ações e responsabilidades a serem tomadas por parte dos servidores pertinentes.

C. Apoiar a implantação das iniciativas relativas à Segurança da Informação.

D. Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

São princípios da Política de Segurança da Informação do DIVIPREV:

A. Toda informação produzida ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence ao DIVIPREV. As exceções devem ser explícitas e formalizadas entre as partes.

B. Todos os recursos de informação do DIVIPREV devem ser projetados para que seu uso seja consciente e responsável. Os recursos comunicacionais e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalísticos.

C. Deverão ser criados e instituídos controles apropriados, registros de atividades e afins, em todos os pontos e sistemas em que a instituição julgar necessário, com vistas à redução dos riscos dos seus ativos de informação.

D. Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade. Todo o acesso a redes e sistemas do órgão deverá ser feito, preferencialmente, por meio de login de acesso único, pessoal e intransferível.

E. O DIVIPREV pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada em sua infraestrutura.

F. Cada usuário é responsável pela segurança das informações dentro do DIVIPREV, principalmente daquelas que estão sob sua responsabilidade.

G. A gestão da segurança da informação no DIVIPREV será realizada pela Superintendência, bem como pelo setor de Processamento de dados.

H. Deverá constar em todos os contratos do DIVIPREV, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades no DIVIPREV.

I. Esta Política de Segurança da Informação será implementada no DIVIPREV por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

4. PAPÉIS E RESPONSABILIDADES

4.1 Descrição de papéis em Segurança da Informação:

PAPEL	PERFIL ASSOCIADO	DESCRIÇÃO
Usuário Interno	Servidores públicos e demais funcionários e colaboradores internos	Todos os servidores, gestores, técnicos, estagiários, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais do DIVIPREV.
Usuário Externo	Prestadores de Serviços, órgãos colegidos e demais colaboradores externos	Prestadores de serviços contratados direta ou indiretamente pelo DIVIPREV e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.

Área de TI	Superintendência e setor técnico especialista.	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e custodiante da informação.

4.2 Responsabilidades Gerais

São responsabilidades gerais de todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais do DIVIPREV:

A. Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso.

B. Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do DIVIPREV.

C. Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do DIVIPREV.

Os modelos de declaração de compromisso e de ciência das normas de Segurança da Informação vigentes no DIVIPREV estão presentes no ANEXO I e II.

4.3 Responsabilidades específicas

4.3.1 Usuários internos e externos.

Será de inteira responsabilidade de cada usuário (interno ou externo) todo prejuízo ou dano que vier a sofrer ou causar ao DIVIPREV em decorrência da não obediência às diretrizes e normas referidas na Política de Segurança da Informação e nas normas e procedimentos específicos dela decorrentes. Os usuários externos devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes. O DIVIPREV poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da política de SI ou das normas e procedimentos específicos dela decorrentes.

4.3.2 Gestores de pessoas e processos.

Os gerentes e o Superintendente do DIVIPREV devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação do DIVIPREV, tomando as ações necessárias para cumprir tal responsabilidade.

4.3.3 Área de Tecnologia da Informação.

Quanto à gestão de segurança da informação, serão responsabilidades específicas da área de Tecnologia da Informação:

A. Zelar pela eficácia dos controles de SI utilizados e informar aos gestores e demais interessados os riscos residuais.

B. Negociar e acordar com os gestores níveis de serviço relacionados a SI, incluindo os procedimentos de resposta a incidentes.

C. Configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação.

D. Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

E. Administrar e proteger cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para o DIVIPREV.

F. Informar previamente sobre o fim do prazo de retenção de informações, para que se tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custodiante.

G. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta (a responsabilidade pela gestão dos “logins” de usuários externos é do gestor do contrato de prestação de serviços ou do gestor do setor em que o usuário externo desempenha suas atividades).

5. DIRETRIZES GERAIS.

5.1 Tratamento da informação.

São diretrizes específicas e procedimentos próprios de tratamento da informação corporativa do DIVIPREV:

A. Documentos imprescindíveis para as atividades dos usuários da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

B. Arquivos pessoais e/ou não pertinentes às atividades institucionais do DIVIPREV (fotos, músicas, vídeos, etc..) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário.

5.2 Controles de Acesso.

O controle de acesso observará as seguintes diretrizes específicas e procedimentos próprios:

A. Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o DIVIPREV e/ou terceiros.

B. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

C. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

D. Todos os dispositivos de identificação utilizados no DIVIPREV, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

E. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

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

G. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o DIVIPREV e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

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

I. O setor de Processamento de Dados responde pela criação da identidade lógica dos colaboradores na instituição.

J. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

K. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

L. 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.

M. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a Superintendência deverá imediatamente comunicar tal fato à Gerência de Pessoal, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

N. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

5.3 Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade do DIVIPREV, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nesta PSI.

A. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento técnico do responsável do DIVIPREV.

B. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o responsável técnico mediante registro de chamado.

C. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

D. Arquivos pessoais e/ou não pertinentes ao negócio do DIVIPREV (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente.

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

F. Os colaboradores do DIVIPREV e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Superintendência.

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

- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por técnico responsável do DIVIPREV ou por terceiros devidamente contratados para o serviço.

- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a

possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

• O colaborador deverá manter a configuração do equipamento disponibilizado pelo DIVIPREV, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

• Deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

• Todos os recursos tecnológicos adquiridos pelo DIVIPREV devem ter imediatamente suas senhas padrões (default) alteradas.

• Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

H. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do DIVIPREV:

• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

• Burlar quaisquer sistemas de segurança.

• Acessar informações confidenciais sem explícita autorização do proprietário.

• Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

• Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual ou perturbação;

• Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

5.4 Correio Eletrônico.

O objetivo desta norma é informar aos colaboradores do DIVIPREV quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

A. O uso do correio eletrônico do DIVIPREV é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o DIVIPREV e também não cause impacto no tráfego da rede.

B. Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do DIVIPREV:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o DIVIPREV ou suas unidades vulneráveis a ações civis ou criminais;

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

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

- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do DIVIPREV estiver sujeita a algum tipo de investigação.

- produzir, transmitir ou divulgar mensagem que:

  - □ contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do DIVIPREV;

  - □ contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;

  - □ contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

□ vise obter acesso não autorizado a outro computador, servidor ou rede;

□ vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

□ vise burlar qualquer sistema de segurança;

□ vise vigiar secretamente ou assediar outro usuário;

□ vise acessar informações confidenciais sem explícita autorização do proprietário;

□ vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

□ inclua imagens criptografadas ou de qualquer forma mascaradas;

□ contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)

□ tenha conteúdo considerado impróprio, obsceno ou ilegal;

□ seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

□ contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

□ tenha fins políticos locais ou do país (propaganda política);

□ inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

C. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Gerência ou departamento
- Nome da empresa

• Telefone(s)

5.5 Serviço de Backup.

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

A. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

B. Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios do DIVIPREV, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

C. Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

D. Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

5.6 Data Center.

A. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de PSI - Política de Segurança da Informação liberação de acesso.

B. O Datacenter deverá ser mantido limpo. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

C. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

D. A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com a autorização desse instrumento pelo responsável do Datacenter.

5.7 Monitoramento do Ambiente.

Para garantir a aplicação das diretrizes mencionadas nesta PSI, além de fixar normas e procedimentos complementares sobre o tema, o DIVIPREV poderá:

A. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

B. Tornar públicas as informações obtidas pelos sistemas de monitoramento e registros de atividade, no caso de exigência judicial;

C. Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

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

E. Desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

5.8 Uso e acesso à internet.

Todas as regras atuais do DIVIPREV visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

A. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o DIVIPREV, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela quando necessário.

B. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, 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.

C. O DIVIPREV, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

D. A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

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

E. Somente os colaboradores que estão devidamente autorizados a falar em nome do DIVIPREV para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

F. Apenas os colaboradores autorizados pela instituição 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.

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

H. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no DIVIPREV e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Superintendência.

I. 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. Qualquer software não autorizado baixado poderá ser excluído.

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

K. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

L. Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao DIVIPREV ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

M. Os colaboradores não poderão utilizar os recursos do DIVIPREV para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

5.9 Gestão de Riscos.

A "Gestão de Riscos de Segurança da Informação e Comunicações é o conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos". As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações do DIVIPREV deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão, direta e indireta, além de estarem alinhadas a esta Política de Segurança da Informação.

6. PENALIDADES.

O DIVIPREV, ao gerir e monitorar seus ativos de informação, pretende garantir a integridade destes, juntamente com suas informações e recursos. O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, às quais o DIVIPREV responderá com a aplicação de todas as medidas administrativas, cíveis e criminais cabíveis. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor. O uso de qualquer recurso em inobservância das normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos

administrativo, civil e criminal, em que a instituição cooperará ativamente com as autoridades competentes.

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o DIVIPREV e/ou terceiros.

7. ESTRUTURA NORMATIVA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

O documento que comporá a estrutura normativa de gestão de segurança da informação se dará pela Política de Segurança da Informação que: constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o DIVIPREV decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados.

7.1 Divulgação e acesso à estrutura normativa.

Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados a todos os servidores, órgãos colegiados, colaboradores, estagiários, aprendizes e prestadores de serviços do DIVIPREV quando de sua admissão, e também publicadas na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

7.2 Aprovação e revisão.

Os documentos integrantes da estrutura normativa de gestão de segurança da informação do DIVIPREV poderão ser revisados e alterados conforme deliberação do Conselho Administrativo.

8. REFERÊNCIAS LEGAIS E NORMATIVAS.

Referências legais e normativas:

- Lei Federal 8.159/1991, de 08/01/1991 - Dispõe sobre a política nacional de arquivos públicos e privados.

- Lei Federal 9.610/1998, de 19/02/1998 - Dispõe sobre o direito autoral.

- Lei Federal 9.279/1996, de 14/05/1996 - Dispõe sobre marcas e patentes.
- Lei Federal 10.406/2002, de 10/01/2002 - Institui o Código Civil brasileiro.
- Decreto-Lei 2.848/1940, de 07/12/1940 - Institui o Código Penal brasileiro.

9. DISPOSIÇÕES FINAIS.

Para a uniformização da informação organizacional, esta Política de Segurança da Informação deverá ser comunicada a todos os gestores, servidores, colaboradores e prestadores de serviço do DIVIPREV – a fim de que seja cumprida dentro e fora da autarquia.

O não cumprimento dos requisitos previstos nesta política acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

Revogam-se em todos os seus termos a Resolução nº 06/2020.

Esta Resolução entra em vigor na data de sua publicação.

Divinópolis/MG, 13 de março de 2024.

INSTITUTO DE PREVIDENCIA DOS SERVIDORES DO MUNICI:04286331000190
Assinado de forma digital por INSTITUTO DE PREVIDENCIA DOS SERVIDORES DO MUNICI:04286331000190
Dados: 2024.03.13 11:13:34 -03'00'

Aguinaldo Henrique Ferreira Lage

Superintendência

gov.br Documento assinado digitalmente
BRUNO ALVES CAMARGOS
Data: 12/03/2024 19:35:50-0300
Verifique em https://validar.iti.gov.br

Bruno Alves Camargos

Conselho de Administração

ANEXO I

TERMO DE COMPROMISSO **CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO**	
IDENTIFICAÇÃO DO CONTRATO:	
Nº DO CONTRATO	
NOME DA EMPRESA CONTRATADA	
CNPJ DA CONTRATADA	
OBJETO RESUMIDO	
VIGÊNCIA CONTRATUAL	

TERMO:

O <Contratante>, sediado em <Endereço Contratante>, CNPJ n.º <CNPJ Contratante>, doravante denominado **CONTRATANTE**, e, de outro lado, a <Contratada>, sediada em <Endereço Contratada>, CNPJ n.º <CNPJ Contratada>, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do CONTRATO N.º <n° contrato / ano> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na **Política de Segurança da Informação** da CONTRATANTE;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E CONFIDENCIALIDADE DAS INFORMAÇÕES**, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO
Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE - por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes - segundo Portaria nº 053/2018, de 09 de abril de 2018, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES
Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

I. Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

II. Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

III. Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

IV. Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

V. Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO DE COMPROMISSO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O termo INFORMAÇÃO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, publicações, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, projetos, cópias, modelos, amostras de ideias, aspectos financeiros e

econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que, diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

§1° – Comprometem-se as partes a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

§2° – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO DE COMPROMISSO não serão aplicadas àquelas informações que:
I. Sejam comprovadamente de domínio público no momento da revelação;
II. Tenham sido comprovada e legitimamente recebidas de terceiros, estranhos ao presente TERMO DE COMPROMISSO;
III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO DE COMPROMISSO.

§1° – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

§2° – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO DE COMPROMISSO bem como da natureza sigilosa das informações.

I. A CONTRATADA deverá firmar acordos por escrito com seus empregados visando a garantir o cumprimento de todas as disposições do presente TERMO DE COMPORMISSO e dará ciência à CONTRATANTE dos documentos comprobatórios.

§3° – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

§4° – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste

TERMO DE COMPROMISSO.

I. Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes

§5° – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, prepostos, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

§6° – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III. Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV. Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações

sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO DE COMPROMISSO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislação em vigor que trata desse assunto, podendo culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO DE COMPROMISSO é parte integrante e inseparável do CONTRATO PRINCIPAL.
§1° – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.
§2° – O disposto no presente TERMO DE COMPROMISSO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tais como aqui definidas.
Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I. A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II. A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III. A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV. Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V. O presente TERMO DE COMPROMISSO somente poderá ser alterado mediante TERMO ADITIVO firmado pelas partes;

VI. Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO DE COMPROMISSO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO ADITIVO ao CONTRATO PRINCIPAL;

VIII. Este TERMO DE COMPROMISSO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da cidade de CIDADE (UF), onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

DE ACORDO

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

CONTRATANTE	**CONTRATADA**

Local, dia/mês/ano. Nome do Responsável pelo Contratante Cargo	Local, dia/mês/ano. Nome do Responsável pelo Contratada Cargo/ CPF

ANEXO II

TERMO DE CIÊNCIA INDIVIDUAL **CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO**	
IDENTIFICAÇÃO DO CONTRATO:	
Nº DO CONTRATO	
NOME DA EMPRESA CONTRATADA	
CNPJ DA CONTRATADA	
OBJETO RESUMIDO	
VIGÊNCIA CONTRATUAL	
TERMOS: O(s) funcionário(s) abaixo qualificado(s) declara(m) ter pleno conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas, bem como sobre todas as informações que eventualmente ou por força de sua(s) função(ões) venha(m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com o TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO firmado entre as partes.	
OBSERVAÇÕES:	
DE ACORDO E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE	

CIÊNCIA é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.	
LOCAL, dia/mês/ano	
IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S):	
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:

NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:

CONSELHO ADMINISTRATIVO

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE DIVINÓPOLIS – DIVIPREV
Rua Rio de Janeiro, nº 426 – Loja 2 – Térreo – Centro- Divinópolis-MG CEP: 35500-009

ATA DA REUNIÃO ORDINÁRIA DO CONSELHO ADMINISTRATIVO DO MÊS DE MARÇO/2024

Aos 13 dias do mês de março de 2024, às 18:30 hs (dezoito e trinta horas), na sede do Instituto de Previdência dos Servidores do Município de Divinópolis- DIVIPREV, localizada à Rua Rio de Janeiro, nº 426 – Loja 2 - Térreo, centro, em Divinópolis, Minas Gerais, foi realizada a Reunião Ordinária do Conselho Administrativo, com a presença dos seguintes conselheiros: Anderson Cesar de Oliveira, Bruno Alves Camargos, Júnia Custódio Ferreira, Jussara Dias Avelar, Marco Antonio Pinto Silva, Marco Aurélio Gomes, e Paulo Sérgio Machado. Aberta a reunião, foi apresentada pauta para julgamento. Em seguida foi apresentada documentação referente ao balancete e demais documentos referente ao mês de JANEIRO/2024, sendo verificado o total geral da receita o valor de R$ 7.522.048,89, o total geral da despesa o valor de R$ 11.947.845,65 e o valor do numerário em 31/01/2024 *o valor de* ***R$ 548.871.588,56.*** Em seguida foi apresentado Relatório Mensal de Investimentos, Balancete e demais documentos alusivo ao mês de Janeiro/2024. Após análise e discussão o mesmo foi aprovado por unanimidade, sem ressalvas. Em seguida foi apresentada **Portaria nº 056/2024** que estabelece o **Plano Anual de Capacitações do Instituto de Previdência dos Servidores do Município de Divinópolis – Diviprev para o exercício de 2024**. Após a devida análise e discussão o mesmo foi **APROVADO** por unanimidade sem ressalvas. Dando continuidade à reunião foi apresentada Resolução nº 001/2024 que **aprova o Plano de Ação para o ano de 2024 do Instituto de Previdência dos Servidores do Município de Divinópolis – Diviprev**. Após a devida análise e discussão o mesmo foi **APROVADO** por unanimidade sem ressalvas. Em continuidade foi apresentada Resolução 002/2024 que **aprova a Política de Segurança da Informação do Instituto de Previdência dos Servidores do Município de Divinópolis – Diviprev**. Após a devida análise e discussão o mesmo foi **APROVADO** por unanimidade sem ressalvas. Em seguida foi apreciado Ofício 147/2024, em atendimento à LC 146/2009 solicitando crédito suplementar nas seguintes rubricas e fichas: R$ 180.000,00 (Saindo da Ficha 29 e alocando na Ficha 25). R$ 30.000,00 (Saindo das fontes de recursos 18 e 21 e alocando na Ficha 16), sendo um total geral de suplementação de R$ 210.000,00 (duzentos e dez mil reais) para atendimento de necessidades do Instituto, os quais foram **APROVADOS** sem ressalvas. Em seguida foi repassado para conhecimento, em atendimento à solicitação deste Conselho, resposta do Instituto com análise de contribuições referente à **Cleide de Fátima Ribeiro,** esclarecendo que a mesma contribui no salário de 125 horas-aulas ininterruptamente desde 2014. Colocado assunto em discussão e tendo em vista dúvidas dos conselheiros sobre a questão, ficou decidido solicitar da recorrente a reformulação do pedido, uma vez que no que está sendo julgado contém questões que não compete ao conselho decidir. Em seguida foi repassado para conhecimento, em atendimento à solicitação deste Conselho, resposta do Instituto com análise de contribuições de 2019 até a presente data referente à **Simone Moreira dos Santos Lauar,** sendo que de Janeiro/2019 até Agosto/2020 contribuiu sobre 81 horas-aulas e de Setembro/2021 até Janeiro/2024

contribuiu sobre 125 horas-aulas. Com relação à servidora foi apresentado também a documentação faltosa quando da apresentação do recurso, verificado na reunião anterior, para juntada e complementação. Estando agora, portanto, apto ao julgamento. Colocado assunto em discussão e tendo em vista dúvidas dos conselheiros sobre a questão, ficou decidido também solicitar da recorrente a reformulação do pedido, uma vez que no que está sendo julgado contém questões que não compete ao conselho decidir. Em seguida foi repassado para conhecimento, em atendimento à solicitação deste Conselho, resposta do Instituto com análise de contribuições referente à **Minervina Maria da Silva Costa,** esclarecendo que a mesma passou a contribuir com 125 horas-aulas a partir de outubro/2020 e tendo aposentado a partir de 01/12/2020. Ao final acrescentou que a servidora contribuiu somente com 2 meses em 125 horas. Colocado assunto em discussão foi apresentado que a servidora impetrou ação judicial que recebeu o nº 5001105-31.2022.8.13.0223 e desta forma os conselheiros acharam por bem aguardar o trânsito em julgado do mesmo para dar andamento no recurso. Em seguida não havendo nada mais a ser tratado foi encerrada a reunião com elaboração da presente ata que após lida se aprovada será por todos assinada.

Bruno Alves Camargos _____

Marco Antonio Pinto Silva _____

Anderson Cesar de Oliveira _____

Júnia Custódio Ferreira _____

Jussara Dias Avelar _____

Marco Aurélio Gomes _____

Paulo Sérgio Machado _____

PREFEITURA MUNICIPAL DE DIVINÓPOLIS
RESOLUÇÃO Nº 002/2024

APROVA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE DIVINÓPOLIS - DIVIPREV.

A Superintendência e o Conselho Administrativo do INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE DIVINÓPOLIS, usando das atribuições que lhe são conferidas por lei, e
CONSIDERANDO as definições do Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social, instituído pela Portaria MPS nº 185/2015.
CONSIDERANDO que a informação é um ativo essencial da organização e precisa ser adequadamente protegida;
CONSIDERANDO o compromisso do RPPS com a proteção das informações sob sua guarda e a formalização das normas para segurança;
CONSIDERANDO a deliberação do Conselho Administrativo pela aprovação da **Política de Segurança da Informação**, ocorrida na reunião ordinária realizada em 13 de março de 2024.

R E S O L V E:

Instituir a **Política de Segurança da Informação** no âmbito do INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE DIVINÓPOLIS, transcrita a seguir:

1. INTRODUÇÃO

Segurança da Informação (SI) é a disciplina dedicada à proteção da informação de forma a garantir a continuidade dos serviços, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de atuação de uma instituição.
A Política de Segurança da Informação (PSI), por sua vez, é o documento formal que orienta e estabelece as diretrizes corporativas para a proteção dos ativos de informação e a gestão da segurança da informação.
"Política de Segurança da Informação e Comunicações: documento aprovado pela Superintendência e o Conselho Administrativo do DIVIPREV, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações".
Os objetivos genéricos da Política de Segurança da Informação para o DIVIPREV são:
A. Certificar e garantir segurança com contato externo em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;
B. Promover a conscientização de todos servidores pertinentes para compreensão e manuseio de situações relacionadas à segurança da informação;
C. Promover as ações necessárias à implementação e manutenção da segurança da informação.

2. CAMPO DE APLICAÇÃO

Os objetivos e diretrizes estabelecidos nesta Política de Segurança da Informação serão aplicados em toda a organização; deverão ser observados por todos servidores, órgãos colegiados, colaboradores e também a fornecedores e prestadores de serviço quando pertinente ou aplicável a área da informação, em qualquer meio ou suporte. Este documento, dentre outras diretrizes, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do órgão poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

3. SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICIPIO DE DIVINOPOLIS – DIVIPREV.

3.1 PRINCÍPIOS E OBJETIVOS

Além de buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade; são objetivos da Política de Segurança da Informação do DIVIPREV:
A. Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional.
B. Designar e definir ações e responsabilidades a serem tomadas por parte dos servidores pertinentes.
C. Apoiar a implantação das iniciativas relativas à Segurança da Informação.
D. Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.
São princípios da Política de Segurança da Informação do DIVIPREV:
A. Toda informação produzida ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence ao DIVIPREV. As exceções devem ser explícitas e formalizadas entre as partes.
B. Todos os recursos de informação do DIVIPREV devem ser projetados para que seu uso seja consciente e responsável. Os recursos comunicacionais e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalísticos.
C. Deverão ser criados e instituídos controles apropriados, registros de atividades e afins, em todos os pontos e sistemas em que a instituição julgar necessário, com vistas à redução dos riscos dos seus ativos de informação.
D. Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade. Todo o acesso a redes e sistemas do órgão deverá ser feito, preferencialmente, por meio de login de acesso único, pessoal e intransferível.
E. O DIVIPREV pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada em sua infraestrutura.
F. Cada usuário é responsável pela segurança das informações dentro do DIVIPREV, principalmente daquelas que estão sob sua responsabilidade.
G. A gestão da segurança da informação no DIVIPREV será realizada pela Superintendência, bem como pelo setor de Processamento de dados.
H. Deverá constar em todos os contratos do DIVIPREV, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades no DIVIPREV.

I. Esta Política de Segurança da Informação será implementada no DIVIPREV por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

4. PAPÉIS E RESPONSABILIDADES

4.1 Descrição de papéis em Segurança da Informação:

PAPEL	PERFIL ASSOCIADO	DESCRIÇÃO
Usuário Interno	Servidores públicos e demais funcionários e colaboradores internos	Todos os servidores, gestores, técnicos, estagiários, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais do DIVIPREV.
Usuário Externo	Prestadores de Serviços, órgãos colegidos e demais colaboradores externos	Prestadores de serviços contratados direta ou indiretamente pelo DIVIPREV e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.
Área de TI	Superintendência e setor técnico especialista.	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e custodiante da informação.

4.2 Responsabilidades Gerais

São responsabilidades gerais de todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais do DIVIPREV:

A. Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso.

B. Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do DIVIPREV.

C. Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do DIVIPREV.

Os modelos de declaração de compromisso e de ciência das normas de Segurança da Informação vigentes no DIVIPREV estão presentes no ANEXO I e II.

4.3 Responsabilidades específicas

4.3.1 Usuários internos e externos.

Será de inteira responsabilidade de cada usuário (interno ou externo) todo prejuízo ou dano que vier a sofrer ou causar ao DIVIPREV em decorrência da não obediência às diretrizes e normas referidas na Política de Segurança da Informação e nas normas e procedimentos específicos dela decorrentes. Os usuários externos devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes. O DIVIPREV poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da política de SI ou das normas e procedimentos específicos dela decorrentes.

4.3.2 Gestores de pessoas e processos.

Os gerentes e o Superintendente do DIVIPREV devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação do DIVIPREV, tomando as ações necessárias para cumprir tal responsabilidade.

4.3.3 Área de Tecnologia da Informação.

Quanto à gestão de segurança da informação, serão responsabilidades específicas da área de Tecnologia da Informação:

A. Zelar pela eficácia dos controles de SI utilizados e informar aos gestores e demais interessados os riscos residuais.

B. Negociar e acordar com os gestores níveis de serviço relacionados a SI, incluindo os procedimentos de resposta a incidentes.

C. Configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação.

D. Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

E. Administrar e proteger cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para o DIVIPREV.

F. Informar previamente sobre o fim do prazo de retenção de informações, para que se tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custodiante.

G. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta (a responsabilidade pela gestão dos "logins" de usuários externos é do gestor do contrato de prestação de serviços ou do gestor do setor em que o usuário externo desempenha suas atividades).

5. DIRETRIZES GERAIS.

5.1 Tratamento da informação.

São diretrizes específicas e procedimentos próprios de tratamento da informação corporativa do DIVIPREV:

A. Documentos imprescindíveis para as atividades dos usuários da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

B. Arquivos pessoais e/ou não pertinentes às atividades institucionais do DIVIPREV (fotos, músicas, vídeos, etc..) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário.

5.2 Controles de Acesso.

O controle de acesso observará as seguintes diretrizes específicas e procedimentos próprios:

A. Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o DIVIPREV e/ou terceiros.

B. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

C. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

D. Todos os dispositivos de identificação utilizados no DIVIPREV, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

E. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

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

G. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o DIVIPREV e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

H. É proibido o compartilhamento de login para funções de administração de sistemas.
I. O setor de Processamento de Dados responde pela criação da identidade lógica dos colaboradores na instituição.
J. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
K. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.
L. 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.
M. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a Superintendência deverá imediatamente comunicar tal fato à Gerência de Pessoal, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.
N. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

5.3 Computadores e Recursos Tecnológicos
Os equipamentos disponíveis aos colaboradores são de propriedade do DIVIPREV, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nesta PSI.
A. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento técnico do responsável do DIVIPREV.
B. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o responsável técnico mediante registro de chamado.
C. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.
D. Arquivos pessoais e/ou não pertinentes ao negócio do DIVIPREV (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente.
E. Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.
F. Os colaboradores do DIVIPREV e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Superintendência.
G. No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:
• Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
• É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por técnico responsável do DIVIPREV ou por terceiros devidamente contratados para o serviço.
• Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.
• O colaborador deverá manter a configuração do equipamento disponibilizado pelo DIVIPREV, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.
• Deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
• Todos os recursos tecnológicos adquiridos pelo DIVIPREV devem ter imediatamente suas senhas padrões (default) alteradas.
• Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.
H. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do DIVIPREV:
• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
• Burlar quaisquer sistemas de segurança.
• Acessar informações confidenciais sem explícita autorização do proprietário.
• Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
• Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual ou perturbação;
• Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

5.4 Correio Eletrônico.
O objetivo desta norma é informar aos colaboradores do DIVIPREV quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.
A. O uso do correio eletrônico do DIVIPREV é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o DIVIPREV e também não cause impacto no tráfego da rede.
B. Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do DIVIPREV:
• enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
• enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
• enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o DIVIPREV ou suas unidades vulneráveis a ações civis ou criminais;
• divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
• falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
• apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do DIVIPREV estiver sujeita a algum tipo de investigação.
• produzir, transmitir ou divulgar mensagem que:

- contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do DIVIPREV;
- contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- vise obter acesso não autorizado a outro computador, servidor ou rede;
- vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- vise burlar qualquer sistema de segurança;
- vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- inclua imagens criptografadas ou de qualquer forma mascaradas;
- contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

C. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:
• Nome do colaborador
• Gerência ou departamento
• Nome da empresa
• Telefone(s)

5.5 Serviço de Backup.

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

A. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

B. Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios do DIVIPREV, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

C. Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

D. Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

5.6 Data Center.

A. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de PSI - Política de Segurança da Informação liberação de acesso.

B. O Datacenter deverá ser mantido limpo. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

C. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

D. A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com a autorização desse instrumento pelo responsável do Datacenter.

5.7 Monitoramento do Ambiente.

Para garantir a aplicação das diretrizes mencionadas nesta PSI, além de fixar normas e procedimentos complementares sobre o tema, o DIVIPREV poderá:

A. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

B. Tornar públicas as informações obtidas pelos sistemas de monitoramento e registros de atividade, no caso de exigência judicial;

C. Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

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

E. Desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

5.8 Uso e acesso à internet.

Todas as regras atuais do DIVIPREV visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

A. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o DIVIPREV, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela quando necessário.

B. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, 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.

C. O DIVIPREV, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

D. A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

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

E. Somente os colaboradores que estão devidamente autorizados a falar em nome do DIVIPREV para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

F. Apenas os colaboradores autorizados pela instituição 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.
G. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.
H. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no DIVIPREV e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Superintendência.
I. 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. Qualquer software não autorizado baixado poderá ser excluído.
J. Os colaboradores não poderão em hipótese alguma utilizar os recursos do DIVIPREV para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.
K. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.
L. Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao DIVIPREV ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.
M. Os colaboradores não poderão utilizar os recursos do DIVIPREV para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

5.9 Gestão de Riscos.

A "Gestão de Riscos de Segurança da Informação e Comunicações é o conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos". As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações do DIVIPREV deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão, direta e indireta, além de estarem alinhadas a esta Política de Segurança da Informação.

6. PENALIDADES.

O DIVIPREV, ao gerir e monitorar seus ativos de informação, pretende garantir a integridade destes, juntamente com suas informações e recursos. O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, às quais o DIVIPREV responderá com a aplicação de todas as medidas administrativas, cíveis e criminais cabíveis. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor. O uso de qualquer recurso em inobservância das normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos administrativo, civil e criminal, em que a instituição cooperará ativamente com as autoridades competentes.
Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o DIVIPREV e/ou terceiros.

7. ESTRUTURA NORMATIVA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

O documento que comporá a estrutura normativa de gestão de segurança da informação se dará pela Política de Segurança da Informação que: constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o DIVIPREV decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados.

7.1 Divulgação e acesso à estrutura normativa.

Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados a todos os servidores, órgãos colegiados, colaboradores, estagiários, aprendizes e prestadores de serviços do DIVIPREV quando de sua admissão, e também publicadas na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

7.2 Aprovação e revisão.

Os documentos integrantes da estrutura normativa de gestão de segurança da informação do DIVIPREV poderão ser revisados e alterados conforme deliberação do Conselho Administrativo.

8. REFERÊNCIAS LEGAIS E NORMATIVAS.

Referências legais e normativas:
Lei Federal 8.159/1991, de 08/01/1991 - Dispõe sobre a política nacional de arquivos públicos e privados.
Lei Federal 9.610/1998, de 19/02/1998 - Dispõe sobre o direito autoral.
Lei Federal 9.279/1996, de 14/05/1996 - Dispõe sobre marcas e patentes.
Lei Federal 10.406/2002, de 10/01/2002 - Institui o Código Civil brasileiro.
Decreto-Lei 2.848/1940, de 07/12/1940 - Institui o Código Penal brasileiro.

9. DISPOSIÇÕES FINAIS.

Para a uniformização da informação organizacional, esta Política de Segurança da Informação deverá ser comunicada a todos os gestores, servidores, colaboradores e prestadores de serviço do DIVIPREV – a fim de que seja cumprida dentro e fora da autarquia.
O não cumprimento dos requisitos previstos nesta política acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.
Revogam-se em todos os seus termos a Resolução nº 06/2020.
Esta Resolução entra em vigor na data de sua publicação.

Divinópolis/MG, 13 de março de 2024.

AGUINALDO HENRIQUE FERREIRA LAGE
Superintendência

BRUNO ALVES CAMARGOS
Conselho de Administração

ANEXO I

TERMO DE COMPROMISSO **CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO**

IDENTIFICAÇÃO DO CONTRATO:	
Nº DO CONTRATO	
NOME DA EMPRESA CONTRATADA	
CNPJ DA CONTRATADA	
OBJETO RESUMIDO	
VIGÊNCIA CONTRATUAL	

TERMO:

O <Contratante>, sediado em <Endereço Contratante>, CNPJ n.º <CNPJ Contratante>, doravante denominado **CONTRATANTE**, e, de outro lado, a <Contratada>, sediada em <Endereço Contratada>, CNPJ n.º <CNPJ Contratada>, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do CONTRATO N.º <n° contrato / ano> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na **Política de Segurança da Informação** da CONTRATANTE;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E CONFIDENCIALIDADE DAS INFORMAÇÕES**, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE - por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes - segundo Portaria nº 053/2018, de 09 de abril de 2018, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

I. Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

II. Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

III. Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

IV. Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

V. Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO DE COMPROMISSO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O termo INFORMAÇÃO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, publicações, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, projetos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que, diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

§1° – Comprometem-se as partes a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

§2° – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO DE COMPROMISSO não serão aplicadas àquelas informações que:

I. Sejam comprovadamente de domínio público no momento da revelação;

II. Tenham sido comprovada e legitimamente recebidas de terceiros, estranhos ao presente TERMO DE COMPROMISSO;

III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO DE COMPROMISSO.

§1° – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

§2° – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO DE COMPROMISSO bem como da natureza sigilosa das informações.

I. A CONTRATADA deverá firmar acordos por escrito com seus empregados visando a garantir o cumprimento de todas as disposições do presente TERMO DE COMPORMISSO e dará ciência à CONTRATANTE dos documentos comprobatórios.

§3° – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

§4° – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste

TERMO DE COMPROMISSO.

I. Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes

§5° – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, prepostos, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

§6° – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III. Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV. Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO DE COMPROMISSO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislação em vigor que trata desse assunto, podendo culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO DE COMPROMISSO é parte integrante e inseparável do CONTRATO PRINCIPAL.

§1° – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

§2° – O disposto no presente TERMO DE COMPROMISSO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tais como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I. A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II. A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III. A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV. Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V. O presente TERMO DE COMPROMISSO somente poderá ser alterado mediante TERMO ADITIVO firmado pelas partes;

VI. Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO DE COMPROMISSO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO ADITIVO ao CONTRATO PRINCIPAL;

VIII. Este TERMO DE COMPROMISSO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da cidade de CIDADE (UF), onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

DE ACORDO

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

CONTRATANTE	**CONTRATADA**
Local, dia/mês/ano. Nome do Responsável pelo Contratante Cargo	Local, dia/mês/ano. Nome do Responsável pelo Contratada Cargo/ CPF

ANEXO II

TERMO DE CIÊNCIA INDIVIDUAL
CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

IDENTIFICAÇÃO DO CONTRATO:

Nº DO CONTRATO	
NOME DA EMPRESA CONTRATADA	
CNPJ DA CONTRATADA	
OBJETO RESUMIDO	
VIGÊNCIA CONTRATUAL	

TERMOS:

O(s) funcionário(s) abaixo qualificado(s) declara(m) ter pleno conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas, bem como sobre todas as informações que eventualmente ou por força de sua(s) função(ões) venha(m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com o TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO firmado entre as partes.

OBSERVAÇÕES:

DE ACORDO

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIÊNCIA é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

LOCAL, dia/mês/ano

IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S):

NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:
NOME: IDENTIDADE: CPF:	ASSINATURA:

CARGO/FUNÇÃO:	
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:

Publicado por:
Felipe Henrique de Assis Miguel
Código Identificador:CC534DD7

Matéria publicada no Diário Oficial dos Municípios Mineiros no dia 15/03/2024. Edição 3726
A verificação de autenticidade da matéria pode ser feita informando o código identificador no site:
https://www.diariomunicipal.com.br/amm-mg/