RESOLUÇÃO Nº 000/CMP/IPMS/2024

SERINGUEIRAS/RO, - de - de 2024.

CONSELHO MUNICIPAL DE PREVIDENCIA – CMP

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

"DISPÕE SOBRE A APROVAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SERINGUEIRAS-RO".

CONSIDERANDO os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade e eficiência, aplicáveis à administração pública, conforme disposto no art. 37, caput, da Constituição Federal de 1988.

CONSIDERANDO o Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social dos Sevidres Publicos do municipio de Seringueiras, irá formalizar adesão;

CONSIDERANDO a exigência, na atualidade, de instituições que prezem pela transparência, sem prejuízo da preservação dos sigilos legais;

CONSIDERANDO o grande fluxo de informações públicas e privadas que transitam entre os diversos agentes internos e externos que se relacionam com autarquia;

CONSIDERANDO a importância dessas informações e a indispensabilidade de uma melhor gestão sobre o fluxo de dados, registros, documentos e demais temas correlatos;

CONSIDERANDO a necessidade de estabelecer diretrizes que norteiem o aspecto da segurança da informação nessas relações.

RESOLVE:

Art. 1º APROVAR e INSTITUIR sua primeira versão da Política de Segurança da Informação do IPMS, nos termos do Anexo I desta Resolução.

Art. 2º Caberá ao DIRETOR EXECUTIVO do IPMS disponibilizar, de maneira formal, no prazo de até cinco dias úteis após a data de publicação desta Resolução, a versão da Política de Segurança da Informação aos agentes públicos do IPMS, a fim de que se ateste sua ciência, compreensão e aceitação, aderindo às práticas nele disciplinadas.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

Seringueras/RO, - de - de 2024.

Adriana Correia da Silva
Presidente do Conselho Deliberativo

Kenia de Jesus Moraes
Membro do Conselho Deliberativo

Fabio Junior Romão de Barros
Membro do Conselho Deliberativo

Dieimis Ribeiro
Membro do Conselho deliberativo

Wolney Blosfeld
Membro do Conselho Deliberativo

ANEXO I
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO I - DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
CAPÍTULO I - DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituído, no âmbito do Instituto de Previdência Municipal de SERINGUEIRAS/RO IPMS, a "Política de Segurança da Informação", destinado aos agentes públicos do IPMS, com a finalidade de estabelecer orientações e procedimentos a serem adotados para o manuseio, controle e proteção das informações sob a guarda da entidade fundacional, em qualquer meio ou suporte, contra destruição, modificação e/ou divulgação indevidas e acessos não autorizados

Art. 2º Toda informação produzida ou recebida, derivada da atividade profissional pelos usuários, pertence ao IPMS, salvo as exceções explícitas e formalizadas previamente em documento entre as partes envolvidas.

CAPÍTULO II - DOS AGENTES PÚBLICOS

Art. 3º Para os fins desta Política de Segurança da Informação, considera-se agente público todo aquele que exerce, ainda que transitoriamente, com ou sem remuneração, por eleição, nomeação, designação, contratação, cedência ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no IPMS, incluindo servidores efetivos, cedidos, comissionados, temporários, estagiários, conselheiros, segurados, beneficiários, dependentes e pessoas jurídicas ou físicas contratadas.

CAPÍTULO III - DOS PRINCÍPIOS

Art. 4º São princípios basilares da Política de Segurança da Informação, no âmbito do IPMS:

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

II. Integridade: Garantia da exatidão das informações e dos métodos de processamento;

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

CAPÍTULO IV - DOS OBJETIVOS

Art. 5º São objetivos norteadores da Política de Segurança da Informação, no âmbito do IPMS:

I. Proteger a informação sob a guarda do Instituto de Previdência Social do Municipio de Seringueiras, em qualquer meio ou suporte, de vários tipos de

ameaças, para garantir a continuidade das atividades no âmbito do IPMS, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição;

II. Adotar condutas que observem os preceitos legais, de acordo com aspectos de legitimidade, legalidade e justiça;

III. Garantir a segurança dos ativos computacionais, instalações prediais e documentos em meio físico abrangendo, também, o controle de acesso de pessoas às instalações do IPMS PREVIDENCIARIA;

IV. Garantir a segurança de toda e qualquer informação contida em meio digital, seja em equipamentos, tráfego de informações pela rede, por correio eletrônico ou armazenada em estações de trabalho dos usuários;

V. Promover a educação e conscientização de cada usuário sobre a responsabilidade para com a segurança da informação, por meio de sugestões e ações educativas;

VI. Promover ampla divulgação da Política de Segurança da Informação a todos os servidores efetivos, cedidos, comissionados, temporários, estagiários, conselheiros, segurados, beneficiários, dependentes e pessoas jurídicas ou físicas contratadas pelo IPMS.

CAPÍTULO V - DA AUTENTICAÇÃO DE ACESSO AOS SISTEMAS DE GESTÃO DE SERINGUEIRAS

Art. 6º A autenticação de acesso dos usuários aos sistemas informatizados de gestão do IPMS ocorrerá por meio de login e senha individuais e intransferíveis, sendo esta composta por, no mínimo 06 (seis) caracteres alfanuméricos (letras e números).

§1º As senhas deverão ser alteradas sempre que necessário.

§2º Todas as ações executadas por meio do login individual serão de inteira responsabilidade do usuário correspondente.

CAPÍTULO VI - DO USO DO CORREIO ELETRÔNICO E DO ACESSO À INTERNET

Art. 7º A ferramenta de correio eletrônico corporativo constitui meio de comunicação corporativa do IPMS, a ser utilizado com nome do “setor” seguido do domínio <@institutodeprevidenciaipms@gmail.com>,devendo ser utilizado de acordo com os princípios estabelecimentos na Política de Segurança da Informação.

§1º É vedado o uso de contas particulares de correio eletrônico para fins institucionais.

§2º Os e-mails encaminhados pelo correio eletrônico corporativo deverão adotar assinatura padrão com as seguintes informações:

I. Nome completo do servidor;
II. Cargo, acompanhado do registro no órgão fiscalizador da profissão, se for o caso;
III. Logomarca ou nome do IPMS;
IV. Telefone de contato;
V. Endereço do site do IPMS.

§3º A autenticação de acesso do usuário ao seu respectivo correio eletrônico corporativo do IPMS ocorrerá por meio de login e senha individual e intransferível, sendo esta composta por, no mínimo 06 (seis) caracteres.

Art. 8º Os recursos de internet, correio eletrônico corporativo ou qualquer outro existente ou que venha a ser adotado, deverão ser utilizados em consonância com os interesses do IPMS.

Art. 9º É vedada a moderação no uso do correio eletrônico corporativo, considerando-se abuso a utilização que comprometa o desempenho do servidor em horário de trabalho, a boa imagem e a segurança dos dados do IPMS, bem como qualquer outra forma de utilização que fuja à legalidade, à moralidade ou a qualquer outro princípio administrativo.

Art. 10 É permitida a comunicação instantânea via aplicativos de celular, a exemplo de 'Whatsapp', etc., e de redes sociais, no aparelho celular da Chefia imediata, desde que utilizado para fins corporativos, sendo vedado seu uso para fins particulares.

Art. 11 O acesso recreativo à internet deverá observar, além dos princípios constitucionais da legalidade, moralidade, razoabilidade e demais aplicáveis, as seguintes restrições:
I. Proibição do acesso a sites não confiáveis, impróprios, incluindo aqueles com conteúdo sexual ou preconceituoso, jogos, salas de bate-papo, apostas e assemelhados;
II. Proibição do uso de ferramentas Peer-to-Peer (P2P), para o compartilhamento de serviços e dados;
III. Proibição do uso e instalação de jogos ou do download de arquivos que comprometam o tráfego da rede (vídeos, imagens, músicas, etc.), para fins particulares;
IV. Proibição de uso excessivo ou abusivo.

CAPÍTULO VII - DO USO DA INTERNET PELA REDE WI-FI

Art. 12 O uso da Internet pela rede Wi-fi, no âmbito do IPMS, é permitido aos servidores efetivos, cedidos, comissionados, temporários, estagiários e conselheiros,

desde que para o uso profissional, condizente com as tarefas do cargo ou função.
§1º Os usuários deverão conhecer as regras de acesso à referida rede, contidas na Política de Uso e estar cientes das penalidades que poderão ocorrer caso haja violação das mesmas.

Art. 13 A Política de Uso da rede Wi-fi (Wireless Fidelity), no âmbito do IPMS, é constituída pela seguintes regras:
I. Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;
II. Responsabilizar-se pela sua identidade eletrônica, senha ou outro dispositivo de segurança, negando revelá-la a terceiros;
III. Manter seus dispositivos pessoais (notebooks, smartphones, etc.) com softwares e antivírus atualizados;
IV. Não usar a rede para trafegar informações confidenciais e/ou sigilosas, salvo quando utilizado algum meio seguro de transmissão (vpn, conexões cifradas, etc.);
V. Responder pelo mau uso dos recursos computacionais em qualquer circunstância;

Art. 14 Considerar-se-á violação das regras de Política de Uso da rede Wi-fi (Wireless Fidelity), no âmbito do IPMS:
I. Acessar, mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;
II. Utilizar os recursos computacionais do IPMS para constranger, assediar, ameaçar ou perseguir qualquer pessoa;
III. Efetuar ou tentar efetuar qualquer tipo de acesso não autorizado aos recursos computacionais do IPMS;
IV. Utilizar os recursos computacionais do IPMS para invadir, alterar ou destruir recursos computacionais de outras instituições;
V. Violar ou tentar violar os sistemas de segurança, quebrando ou tentando adivinhar a identidade eletrônica de outro usuário, senhas ou outros dispositivos de segurança;
VI. Interceptar ou tentar interceptar a transmissão de dados através de monitoração;
VII. Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando o congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais do IPMS;
VIII. Utilizar os recursos computacionais do IPMS para fins comerciais ou políticos, tais como mala direta, spams ou propaganda política;
IX. Não fazer uso ou divulgar conteúdos impróprios como: pornografia, erotismo, racista, sexista, difamatório, falsos perfis em sites pessoais ou quaisquer outros tipos de ataques dessa categoria;

CAPÍTULO VIII - DAS ESTAÇÕES DE TRABALHO

Art. 15 Cada servidor do IPMS deverá utilizar uma estação de trabalho determinada, que deverá ser protegida por senha individual e intransferível, sendo esta composta por, no mínimo 08 (oito) caracteres alfanuméricos (letras e números), com letras maiúsculas e minúsculas.

Art. 16 O uso das estações de trabalho do IPMS deverá observar, além dos princípios constitucionais da legalidade, moralidade, razoabilidade e demais aplicáveis, as seguintes restrições:

I. Proibição do armazenamento, edição ou distribuição de qualquer material de cunho sexual, preconceituoso, ou ilegal, incluindo piratarias;

II. Proibição da retirada de equipamentos eletrônicos da sede do IPMS, salvo autorização do Diretor executivo;

III. Proibição da retirada de arquivos físicos ou digitais da sede do IPMS, salvo autorização do Diretor executivo;

IV. Proibição de instalação de softwares ou hardwares não licenciados sem autorização do Diretor executivo, ou qualquer outro tipo de pirataria.

Art. 17 O antivírus deverá estar sempre atualizado, cabendo ao usuário da estação de trabalho informar ao Diretor executivo do IPMS quaisquer atitudes suspeitas em sua estação de trabalho ou notificações que venha a receber, incluindo notificações relacionadas ao funcionamento do programa.

CAPÍTULO IX - DOS PROCEDIMENTOS BÁSICOS DE SEGURANÇA

Art. 18 O IPMS adotará providências no sentido de garantir:

I. Que os equipamentos estejam em bom estado de conservação para atender as demandas do IPMS e não comprometam a segurança das informações produzidas;

II. Caso não seja utilizado sistema de “webmail” ou qualquer outro sistema de armazenamento virtual das informações do correio eletrônico corporativo, cada usuário deverá realizar o backup semanal das mesmas, que não deverá ser disponibilizado a terceiros, salvo em caso de reestabelecimento do backup na estação de trabalho que tenha apresentado falhas que comprometam a integridade das informações, à pessoa ou empresa previamente autorizada pela Gerência Administrativa.

Art. 19 Os usuários de sistemas e serviços de informação do IPMS deverão registrar e relatar ao Diretor executivo qualquer observação ou suspeita de fragilidade de segurança das informações armazenadas.

Art. 20 As evidências dos incidentes de segurança deverão ser coletadas e armazenadas pelo Diretor executivo, a fim de que sejam tomadas as providências

devidas.

Art. 21 A acesso aos documentos armazenados nos arquivos físicos do IPMS só poderão ocorrer por servidor público efetivo ou cedido ao IPMS ou pelo Diretor executivo, autorizado e designado previamente por esta, mediante o preenchimento dos controles de retirada e devolução dos documentos, nos quais deverão constar o arquivo retirado/devolvido, nome do servidor que acessou o documento, data e horário.

§1º O armazenamento de documentos em arquivos físicos do IPRESF e o acesso aos mesmos deverão observar regras e princípios básicos de arquivologia e biblioteconomia, e da legislação aplicável, a citar-se, especialmente, a Lei de Acesso à Informação (Lei Federal n.º 12.527, de 18 de novembro de 2011), Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709, de 14 de agosto de 2018), ISO 27002, observadas as garantias legais e constitucionais de sigilo de determinadas informações de cunho pessoal.

Art. 22 Além dos procedimentos básicos descritos no Capítulo VIII, desta Política de Segurança da Informação, os agentes públicos deverão observar integralmente das disposições do Plano de Contingência, descritas no Anexo II, deste instrumento.

CAPÍTULO X - DO ACESSO REMOTO

Art. 23 O acesso remoto de terceiros à rede do IPMS será permitido somente para atender aos interesses do Instituto de Previdência Municipal, mediante autorização prévia e expressa do Diretor executivo, através de abertura de requisição de serviço.

§1º A ferramenta de conexão remota utilizada poderá ser “TeamViewer”, “LoMeIn”, “AnyDesk” ou outra ferramenta de uso gratuito, ou da qual o terceiro possua licença de uso.

§2º Os terceiros que tenham acesso remoto à rede do IPMS deverão observar os seguintes requisitos, sob pena de aplicação das penalidades cabíveis:

I. Manter sigilo das informações às quais tiverem acesso, sendo de sua total e exclusiva responsabilidade qualquer operação realizada sob suas credenciais de uso;

II. Comunicar imediatamente ao Diretor executivo qualquer situação que coloque em risco o acesso ao ambiente de rede do IPMS.

CAPÍTULO XI - DAS PENALIDADES

Art. 24 O não cumprimento dos preceitos da Política de Segurança da Informação implicará na adoção das providências necessárias, mediante provocação ou de ofício, com vistas à aplicação das sanções administrativas cabíveis, observados o

contraditório e a ampla defesa, sob pena de nulidade, sem prejuízo das demais sanções cíveis e penais previstas na legislação em vigor.

CAPÍTULO XII - DAS DISPOSIÇÕES FINAIS

Art. 25 Todos os usuários ficam cientes de que os ambientes, sistemas, computadores e redes do IPMS poderão ser monitorados e gravados pelo Diretor executivo.

Art. 26 É vedado aos usuários de sistemas e serviços de informação do IPMS aceitar ajuda técnica de pessoas estranhas e não autorizadas, salvo do quadro de funcionários do IPMS ou da equipe técnica especializada contratada mediante procedimento licitatório adequado.

7 Os usuários deverão ser cientificados da existência da Política de Segurança da Informação e sobre o uso correto dos ativos disponibilizados ao estabelecerem vínculo com o IPMS, de forma a minimizar os possíveis riscos de segurança, bem como garantir o conhecimento de suas responsabilidades.

Art. 28 O IPMS exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos, serviços e informações, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.
Parágrafo Único. O usuário que tomar conhecimento de qualquer irregularidade sobre essa Política de Segurança da Informação deverá comunicar, imediatamente, a autoridade competente do IPMS

Art. 29 O IPMS realizará, sempre que julgar necessário, ações preventivas e educativas visando garantir a aplicação da Política de Segurança da Informação.

Art. 30 O IPMS terá o prazo de 60 (sessenta) dias para a adequação dos procedimentos, de acordo com o estabelecido neste instrumento, a partir da sua entrada em vigor.

Art. 31 Este instrumento entra em vigor na mesma data da publicação da Resolução do Conselho Administrativo que o aprovar.

Seringueiras-RO, 24 de julho de 2024.

Adriana Correia da Silva
Presidente do Conselho Deliberativo

Kenia de Jesus Moraes
Membro do Conselho Deliberativo

Fabio Junior Romão de Barros
Membro do Conselho Deliberativo

Dieimis Ribeiro
Membro do Conselho Deliberativo

Wolney Blosfeld
Membro do Conselho Deliberativo

ANEXO II
PROCEDIMENTOS DE CONTINGÊNCIA

SUMÁRIO

1. CONCEITO DE PROCEDIMENTOS DE CONTINGÊNCIA

Os procedimentos de contingência em Tecnologia da Informação, no âmbito do Instituto de Previdência de SERINGUEIRAS, correspondem às ações previamente planejadas deverão ser adotadas para reduzir as consequências negativas que podem ser causadas por uma situação inesperada, a fim de reduzir o tempo de indisponibilidade dos serviços e, consequentemente, evitar que mais danos e prejuízos sejam causados por razão do incidente.

2. OBJETIVOS

Determinar as ações previamente planejadas para o enfrentamento de ações inesperadas que possam causar prejuízos ou vulnerabilidade das informações, a fim de reestabelecer os serviços prestados pelo IPMS. O presente instrumento estabelece um conjunto de procedimentos pré-estabelecidos para que os serviços de informática permaneçam em funcionamento total ou parcial, quando houver algum impedimento externo.

3. APLICAÇÃO E ÁREA RESPONSÁVEL

Este instrumento tem abrangência no âmbito do Instituto de Previdência Social dos Servidores Públicos de Seringueiras, a ser executado pelo Diretor Executivo.

4. PONTOS FRÁGEIS

A relação dos pontos frágeis aponta os possíveis focos de crise das tecnologias utilizadas pelo IPMS, destacando-se:

a. Servidor de arquivos;
b. Servidor de hospedagem;
c. Serviço de acesso à Internet;
d. Serviço de telefonia.

5. SETORES PREJUDICADOS

Os setores potencialmente prejudicados abrangem:
a. Atendimento aos aposentados e pensionistas;
b. Compras, contratos e licitações;
c. Concessão de benefícios;
d. Contabilidade;
e. Financeiro;
f. Tesouraria;
g. Recursos humanos;
h. Atendimento às demais entidades do poder executivo e legislativo.

6. PROCEDIMENTOS PARA RESTAURAÇÃO DOS SERVIDORES

Os servidores são equipamentos de alta performance capazes de executar aplicações para vários usuários conectados a uma rede de computadores. Eles apresentam diversas funcionalidades para atender às demandas desses usuários e são indispensáveis. À execução das atividades de entidades públicas ou privadas, a exemplo do Instituto de Previdência Municipal de SERINGUEIRAS – IPMS. Essas funcionalidades podem ser o armazenamento de arquivos e bancos de dados, contas de e-mail, compartilhamento de recursos como impressoras, etc. Algumas de suas vantagens são a facilidade para gerenciar os dados de forma centralizada e permitir o acesso remoto aos usuários das aplicações da empresa.

Diversos fatores podem fazer computadores, impressoras, Internet e a própria rede, ficar fora do ar. Os principais motivos normalmente são: defeitos nos equipamentos, ataques cibernéticos, erros provocados por colaboradores, problemas na rede de computadores, rede elétrica e configurações erradas.

Para identificá-los, é preciso verificar os alertas emitidos pelo sistema operacional, softwares aplicativos, utilitários e de gestão, avisos sonoros emitidos pelos nobreaks entre outros, além de realizar testes nos dispositivos.

6.1. Servidor de arquivos

Um servidor de arquivos é um computador conectado a uma rede que tem como objetivo principal proporcionar um local para o armazenamento compartilhado de arquivos de computadores (como documentos, arquivos de som, fotografias, filmes, imagens, bases de dados, etc) que podem ser acessados pelos dispositivos que estão ligados à rede de computadores.

O Servidor seria a ‘máquina principal’ enquanto os dispositivos ligados ao servidor são chamados de ‘clientes’. É projetado principalmente para permitir o

armazenamento, compartilhamento e recuperação rápida de dados onde a computação pesada é fornecida pelas estações de trabalho.

Em caso de problemas no servidor de arquivos deve-se adotar o seguinte procedimento:

a. Avisar aos setores os serviços afetados e o prazo para restabelecimento;
b. A mantenedora providenciara um novo equipamento para instalação, caso o problema não consiga ser resolvido dentro do prazo estabelecido;
c. Instalar os drivers e serviços necessários;
d. Restaurar o backup dos arquivos;
e. Configurar o acesso dos usuários e os serviços;
f. Testar a autenticação via rede e integridade dos arquivos.

6.2. Servidor de hospedagem

Um servidor de hospedagem possui o armazenamento de um site e disponibiliza o mesmo na internet, ou seja, o serviço de hospedagem possibilita que o site seja visualizado 24h por dia em todo o mundo. Em caso de problemas no servidor de hospedagem deve-se adotar o seguinte procedimento:

a. Avisar aos setores os serviços afetados e o prazo para restabelecimento;
b. Abrir um chamado no sistema de atendimento da empresa contratada para prestação
deste serviço;
c. Acompanhar através de e-mail ou telefonema, o andamento do chamado;
d. Alterar as senhas dos administradores do painel do cliente;

7. SERVIÇO DE ACESSO Á INTERNET

O serviço de acesso à internet disponibiliza os meios pelos quais os usuários podem conectar-se à rede mundial de computadores. Em caso de problemas no acesso à internet deve-se adotar o seguinte procedimento:

a. Avisar aos setores os serviços afetados;
b. Checar o cabeamento de rede;
c. Checar a alimentação de energia elétrica dos equipamentos de rede (modem, roteadores e switches);
d. Analisar se o problema é local ou no provedor de acesso;
e. Contatar o provedor deste serviço para solicitação de reparo;
f. Avisar aos setores o prazo para restabelecimento.

8. NOTIFICAÇÕES

As notificações devem ocorrer a todos os usuários afetados quando acontecer qualquer um dos problemas acima citados. Deverá ser notificado o problema ocorrido, causa (quando houver) e informado o prazo estimado para a

resolução do mesmo e ações que os usuários devem adotar (quando for o caso).

A notificação deverá ocorrer da seguinte forma:

a. Notificação Interna:
i. E-mail;
ii. Whatsapp;
iii. Telefone.

b. Notificação Externa:
i. E-mail;
ii. Whatsapp;
iii. Telefone;
iv. Website;
v. Instagram.

9. BACKUP

Backup é uma cópia de segurança. O objetivo da ação é o usuário se resguardar de uma ocasional perda de arquivos originais, seja por ações despropositadas do usuário, ou ainda mal funcionamento dos sistemas. Ter uma cópia de segurança permite restaurar os dados perdidos. As formas de backup atualmente disponíveis são:

a. Meios físicos: HD externo e pen-drive;
b. Meios virtuais: armazenamento nas nuvens e e-mails.

Seringueiras/RO-RO, - de - de 2024.

Adriana Correia da Silva
Presidente do Conselho Deliberativo

Kenia de Jesus Moraes
Membro do Conselho Deliberativo

Fabio Junior Romão de Barros
Membro do Conselho Deliberativo

Dieimis Ribeiro
Membro do Conselho deliberativo

Wolney Blosfeld
Membro do Conselho Deliberativo