IPER
Instituto de Previdência
do Estado de Roraima

MANUAL DE OPERAÇÃO

da Gestão da Tecnologia e Segurança da Informação do IPER

IPER

Instituto de Previdência
do Estado de Roraima

CORPO DIRETIVO

RAFAEL DAVID AIRES ALENCAR
Presidente

ADRIANA SIQUEIRA MELLO PADILHA
Vice-Presidente

CARLOS ALEXANDRE PRAIA RODRIGUES DE CARVALHO
Diretor de Investimento e Arrecadação

HERICK FEIJÓ MENDES
Diretor de Previdência

NATHALYA CYNTYA LOURETO DOS SANTOS
Diretora de Previdência Militar

FRANCISCO EDGLEI ALEXANDRE CESÁRIO
Diretor de Administração e Finanças

EZIO DE JESUS GOMES DE LUCAS
Corregedor

BRUNO CONTI SIQUEIRA LEITE E SILVA 200.509
Chefe do Controle Interno

RONNIE BRITO BEZERRA
Chefe da Consultoria Jurídica

DENYSE DE ASSIS TAJUJÁ
Presidente da C.P.L

FLAVIA ALESSANDRA DA SILVA XAVIER
Ouvidora

WEMERSON BATISTA SILVA
Chefe de Planejamento

JOSINEIA MENDES GEREMIAS DIAS
Chefe de Auditoria

RICARDO GOMES DOS SANTOS
Assessor de Comunicação

1. OBJETIVO DO MANUAL DE OPERAÇÃO DA GESTÃO DA TECNOLOGIA E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IPER.

Estabelecer estratégias e definir responsabilidades e competências e a formalização de apoio para a implementação da gestão de Política de Segurança da Informação do Instituto de Previdência do Estado de Roraima - IPER.

2. ABRANGÊNCIA

Esta Política de Segurança da Informação (PSI) aplica-se a todos os indivíduos e entidades que, de forma direta ou indireta, possuam acesso aos ativos de informação, sistemas, infraestrutura tecnológica ou instalações físicas do IPER.

A abrangência inclui, mas não se limita a:

- Servidores públicos (efetivos e comissionados).
- Estagiários e colaboradores internos.
- Prestadores de serviço, fornecedores, consultores e empresas contratadas (terceiros).

A adesão à PSI é obrigatória para todos os usuários. O cumprimento desta Política será formalizado mediante a assinatura dos seguintes termos, que devem ser arquivados em sistema próprio (SEI/SISPREV):

Categoria do Usuário	Formalização e Termos Requeridos
Servidores, Comissionados e Estagiários	* **Termo de Responsabilidade – Uso de Equipamento, ciência de uso e ciência da Política de Segurança da Informação (Anexo C):** Formaliza a responsabilidade pelo uso adequado dos recursos de TI e equipamentos institucionais. * **Termo de Confidencialidade e Sigilo (Anexo E):** De adesão obrigatória para todos os usuários que têm acesso às informações do IPER. ***Termo de Responsabilidade** – Termo de uso e responsabilidade de acesso a sistemas (SEI, Sisprev, e-mail corporativo, rede e outros) (Anexo G): Formaliza a responsabilidade pelo uso adequado dos sistemas de TI institucionais.

Categoria do Usuário	Formalização e Termos Requeridos
Prestadores de Serviço, Fornecedores e Empresas Contratadas	* **Termo de Confidencialidade e Sigilo (Anexo E):** Obrigatório para qualquer terceiro que tenha acesso a Informações ou infraestrutura. * **Termo de Consentimento para Tratamento de Dados Pessoais - Fornecedores e Prestadores De serviços (Anexo D)**: Obrigatório quando houver coleta, armazenamento, ou processamento de informações e dados pessoais (dados sensíveis, segurados, beneficiários) imprescindíveis para a relação contratual, em conformidade com a LGPD.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação é um documento formal que define como uma organização pretende proteger seus ativos de informação e sistemas contra ameaças internas e externas. Essas políticas são essenciais para garantir a confidencialidade, integridade e disponibilidade das informações críticas do Instituto.

2.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IPER

A política de segurança das informação tem por objetivo possibilitar o gerenciamento da segurança de informação do IPER, estabelecendo regras e padrões para proteção da informação.

2.2. CLASSIFICAÇÃO DA INFORMAÇÃO

2.2.1 O processo eletrônico é aberto com a opção iniciar o processo) pelo Sistema Eletrônico de Informação - SEI e/ou pelo Sistema de Gestão de Regime Próprio de Previdência Social - SISPREV, com um documento produzido eletronicamente ou digitalizado (onde será elaborado um documento eletrônico ou anexado um digitalizado) por usuários interno do IPER dos sistemas.

2.2.2 Os atos gerados no SEI e/ou SISPREV serão registrados automaticamente com a identificação do usuário, data e hora de sua realização, conforme horário oficial do Estado de Roraima.

2.2.3 O processo eletrônico no SEI e/ou SISPREV deve ser iniciado e mantido pelos usuários de forma a permitir sua eficiente localização e controle, mediante o preenchimento dos campos próprios do sistema, observados os seguintes requisitos:

2.2.3.1 No Sistema SEI (https://sei.rr.gov.br/portalsei/), conforme Manual do Usuário (https://softwarepublico.gov.br/social/articles/0004/9746/sei-doc-usuario.pdf):

I – observar a publicidade das informações como preceito geral e o sigilo como Exceção;
II – Informar o nível de acesso de seus documentos individualmente atribuído, quanto à informação nele contida, como público, restrito ou sigiloso, ou alterado sempre que necessário, ampliando ou limitando o acesso, conforme o item Restrição de Acesso do Manual do usuário do SEI e a tabela do item 2.2.5.
III – observar o cadastro das informações ao "Iniciar Processo" no SEI , preenchendo obrigatoriamente os campos "Tipo do Processo","Especificação", "Classificação por Assuntos", "Interessados" (quando houver);
IV – quando necessário, alterar o tipo de cada processo instaurado que tramitar por sua unidade; e
V – criar e gerir as bases de conhecimento correspondentes no SEI RR.

2.2.4 Ademais o Manual do Usuário do SEI, orienta o usuário que abrir o processo eletrônico sigiloso ou restrito deverá observar as disposições legais para a atribuição desta classificação, e será o responsável pela concessão da credencial de acesso aos demais usuários que necessitarem acompanhar e instruir o processo.

2.2.4.1 A credencial de acesso poderá ser cassada pelo usuário que a concedeu ou renunciada pelo próprio usuário

2.2.4.2 A pessoa que tomar conhecimento de documento ou assunto sigiloso fica responsável pela manutenção do sigilo.2.2.5 Quanto as classificações da informação, sua descrição e documentos no Sistema SEI do IPER:

Classificação	Descrição	Documentos
Público	Nível de acesso utilizado para informações sobre as quais não recaia qualquer hipótese de limitação de acesso, ou que seja de amplo conhecimento público em razão de ato do seu titular ou de terceiros.	Formulários, Despachos, Ofícios, Requerimentos, Relatórios, Documento de Formalização de Processos- DFD, Minuta, Contrato, Estudo Técnico Preliminar, Termo de Referência, Anexo, Esclarecimentos, Justificativa, Requerimento e todos os outros
Restrito	Nível de acesso do Processo e/ou documento que cujo teor não deve ser do conhecimento do público em geral, sendo acessados apenas pelos interessados e por agentes públicos das unidades nas quais são tramitados;	Perícia Médica e documentos que envolvem dados sensíveis. Tipo de Processo: Ação de cobrança, Motivo de Limitação: Proteção do envolvido, Possibilidade de Contestação. Tipo de Processo: Multa ao Gestor, Motivo de Limitação: Exposição do envolvido, Direto a ampla defesa e ao contraditório. E os demais relacionados no tem 2.2.5.1.
Sigiloso	Nível de acesso: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada. São visualizados apenas pelos usuários com credencial de acesso ao processo.	Os demais relacionados no item2.2.5.2.

2.2.5.1. Restrito:

Tipo de Processo	Motivo de Limitação
Apuração de dano ou extravio de bem público	Proteção a honra e imagem do envolvido; possibilidade dos dados serem encaminhadas para apuração de responsabilidade (PAD)
Reserva Remunerada (revisão)	Proteção dos dados dos envolvidos, Possibilidade de Contestação.

Tipo de Processo	Motivo de Limitação
Reforma (revisão)	Proteção a honra e imagem do envolvido; possibilidade dos dados serem encaminhadas para apuração de responsabilidade (PAD)
Reserva Remunerada (revisão)	Exposição da causa da Reforma, Direito a ampla defesa e ao contraditório a depender do tipo de Reforma.
Pensão Militar por Morte (revisão)	Proteção dos dados dos envolvidos, Possibilidade de Contestação.
Pensão Militar por perda de cargo (revisão)	Exposição da causa da Pensão, e dos beneficiários/envolvidos.
Averbação de Tempo de Contribuição e Serviço Militar (revisão)	Proteção dos dados dos requerentes
Aposentadoria	Proteção dos dados dos envolvidos.
Pensão por Morte	Proteção dos dados dos envolvidos.
Isenção de Imposto de Renda	Proteção dos dados dos envolvidos.
Perícia Médica (avaliação de grau de deficiência, dependência vitalícia)	Proteção dos dados dos envolvidos.
Alteração de Dados Bancários	Proteção dos dados dos envolvidos.
Emissão de CTC	Proteção dos dados dos envolvidos.
Solicitação de Acesso de Sistema	Informação individual de login e senha de cadastros de sistemas.

2.2.5.2. Sigiloso:

Tipo de Processo	Motivo de Limitação
Denúncias e investigações em Geral	Proteção dos dados dos envolvidos e necessidade de sigilo para proceder com a devida apuração.
Solicitação de Declaração Negativa de não cometimento ou punição por ilícitos administrativos (Sindicância, Processo Administrativo Disciplinar).	Proteção dos dados Pessoais

Tipo de Processo	Motivo de Limitação
Apuração de dano ao erário previdenciário	Proteção dos dados dos envolvidos e necessidade de sigilo para proceder com a devida apuração
Apuração de irregularidades na concessão e manutenção de benefício previdenciário	Proteção dos dados dos envolvidos e necessidade de sigilo para proceder com a devida apuração.
Que versão sobre pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose, nos casos que estabelece; e altera a Lei nº 6.259, de 30 de outubro de 1975.	Lei n.º 14.289, de 03 de janeiro de 2022;

2.2.5 Dos autos de processos eletrônicos que necessitem ser remetidos a outros órgãos ou entidades, serão extraídas cópias em formato PDF e enviados pelo SEI na opção correio eletrônico.

2.2.5.1 No Sistema SEI poderá ser liberado acesso à usuário externo credenciado para vista e consulta dos autos, por período determinado.

2.2.5.2 Nos casos em que haja garantia legal do sigilo ou que mereçam restrição à consulta pública, o acesso será limitado aos usuários previamente autorizados.

2.2.6 A autoria, a autenticidade e a integridade dos documentos e da assinatura, nos processos administrativos eletrônicos, poderão ser obtidas por meio de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, observados os padrões definidos por aquela Infraestrutura.

2.2.6.1 O disposto no caput não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizam identificação por meio de nome de usuário e senha (assinatura eletrônica).

2.2.6.2 O item 2.2.6 neste artigo não se aplica a situações que permitam identificação simplificada do interessado ou nas hipóteses legais de anonimato.

O envio de requerimentos, de recursos e a prática de atos processuais por meio eletrônico, serão admitidos para usuários externos, mediante uso de assinatura eletrônica ou digital.

2.2.7 A utilização de assinatura eletrônica importa aceitação das normas sobre o assunto pelo usuário, inclusive no que se refere à responsabilidade por eventual uso indevido.

2.2.8 A tramitação de processos no SEI e/ou SISPREV não oferecem a emissão de comprovante de recebimento do processo, sendo o envio e o recebimento registrados automaticamente pelo sistema.

2.2.8.1 A unidade é responsável pelo processo desde o momento em que este lhe foi encaminhado, não havendo no âmbito do SEI e/ou SISPREV a situação de processo em trânsito.

2.2.8.2 Caso o processo seja encaminhado para a unidade incorreta, esta deverá devolvê-lo ao remetente.

2.2.8.3 O processo poderá ser encaminhado para quantas unidades for necessário para instruí-lo.

2.2.8.4 O processo no Sistema SEI poderá ser mantido aberto na unidade enquanto for necessária a continuidade simultânea de sua análise.

2.2.9 No Sistema SISPREV
(https://nuvem.agendadatacenter.com.br/roraima/sisprevweb/Login/Login.aspx):

I- Observar o cadastro das informações ao “Incluir Documentos” no SISPREV , marcando os campos “Confidencial” ou “Não Confidencial”;

Classificação	Descrição	Documentos
Confidencial	São visualizados apenas pelos usuários com credencial de acesso ao processo. Nível de acesso: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada. São visualizados apenas pelos usuários com credencial de acesso ao processo.	Somente no Perfil Master (Administrador), Certidão de Tempo de Contribuição
Não Confidencial	Nível de acesso utilizado para informações sobre as quais não recaia qualquer hipótese de limitação de acesso, ou que seja de amplo conhecimento público em razão de ato de seu titular ou de terceiros.	Todos os Documentos

2.2.9 Gestão documental que vai ditar as regras de temporalidade:
Tanto no Sistema SEI e No Sistema SISPREV, o Manual de Gestão de Documentos e Arquivos do Instituto de Previdência de Roraima 2022 e o Código de Classificação e Tabela de Temporalidade e destinação de documentos relativos as atividades-fim do Instituto de Previdência de Roraima-IPER, conforme o Anexo I- Classificação, Temporalidade e destinação de documentos de arquivo das atividades-fim Civil e Militar do IPER.

2.2.10 – Abrangência e Responsabilidade de Terceiros:
Esta Política aplica-se a todos os servidores efetivos, comissionados, estagiários, fornecedores, consultores, empresas contratadas e qualquer terceiro que tenha acesso a informações, sistemas ou infraestrutura tecnológica do IPER, sendo obrigatória quando for o caso, a assinatura dos Termos de Confidencialidade e Consentimento LGPD.

2.3 USO DA INTERNET, CORREIO ELETRÔNICO E COMPUTADORES

2.3.1 Normas de Uso de Recursos Tecnológicos:

2.3.1.1 O uso dos Recursos de Internet e e-mail:

I. É vedado o acesso às páginas com conteúdo que envolva pornografia, racismo ou preconceitos de quaisquer naturezas, jogos ou outros conteúdos notadamente fora do contexto do trabalho;
II. É vedado obter na Internet arquivos (download) que não estejam relacionados com suas atividades, incluindo vídeos, jogos programas de qualquer tipo; e
III. Os e-mails encaminhados pelo correio eletrônico institucional deverão adotar assinatura conforme sugerido abaixo com as seguintes informações para facilitar a rastreabilidade, caso seja necessário:

1) Nome completo do servidor;
2) Cargo e Setor;
3) Nome da Autarquia, por extenso;
4) Telefones da Instituto de Previdência de Roraima (IPER);
5) Endereço do site e correio eletrônico do IPER

IV. Os e-mails não institucionais podem ser utilizados:

1) Indisponibilidade do serviço de WebMail do IPER;
2) Aguardar liberação da Caixa Postal do WebMail;
3) O arquivo anexado exceder o tamanho permitido;
4) Esquecimento da senha do WebMail;
5) Estagiários em processo de transição em virtude da rotatividade.

V. A utilização indevida das caixas postais acarretará, na primeira ocorrência, a edição de advertência formal ao titular da caixa de origem. Em caso de reincidência, haverá a suspensão de uso, somente liberado após solicitação do superior imediato do titular da caixa de origem. Em caso de nova utilização indevida, ficará sujeito à aplicação de penalidades administrativas, nos termos da Lei Complementar Estadual n.º 53/2001;
VI. É desaconselhável a abertura de mensagens de procedência desconhecida contendo anexos executáveis devido ao risco de contaminação da rede por vírus e outros arquivos prejudiciais, sendo de inteira responsabilidade do usuário as eventuais consequências da inobservância desta recomendação;

2.3.1.1 O uso dos Recursos de Internet e e-mail:

VII. Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de Tecnologia da Informação deve ser imediatamente comunicada ao GTI;
VIII. O acesso à Internet deve restringir-se às páginas com conteúdo relacionado às atividades desempenhadas pelo usuário para a autarquia em consultas ou obtenção de informações e dados necessários ao serviço;
IX. Na modalidade de teletrabalho (home office) ficam aplicados todos os dispositivos deste artigo e será implementada conforme orientação da Gerência de Tecnologia da Informação.
X. É vedada as downloads ou instalação de softwares não autorizados;
XI. É proibido o uso da rede e e-mail institucional para fins pessoais;
XII. É de Responsabilidade do usuário pelo sigilo de suas credenciais.
XIII. Bloqueio automático de sites não institucionais e o Monitoramento de logs de acesso são realizados pela GTI;
XIV. É vedada a divulgação ou uso de informações contidas nos documentos físicos, digitais e híbridos para qualquer fim que não esteja ligado às atividades do IPER.

2.3.1.2. Os administradores dos sistemas computacionais do IPER são responsáveis pelo uso adequado dos recursos sob sua responsabilidade, devendo zelar pela integridade e confidencialidade dos sistemas e dos dados sob seus cuidados, bem como os arquivistas e servidores lotados no DIVAP são responsáveis por manter a integridade, fidedignidade dos documentos físicos e acesso controlado aos documentos que estão sob a responsabilidade do setor.

2.4 PROCEDIMENTOS DE CONTINGÊNCIA E AUDITORIA DE ACESSOS

2.4.1 Auditoria Semestral de Acessos aos Sistemas

2.4.1.1 A Auditoria Semestral de Acessos aos Sistemas do IPER tem como objetivo assegurar que os perfis, credenciais e permissões concedidas aos usuários dos sistemas institucionais estejam compatíveis com suas atribuições funcionais, obedecendo aos princípios de necessidade,

proporcionalidade, privacidade, segregação de funções e menor privilégio.

2.4.1.2 Essa auditoria atende aos requisitos das boas práticas previstas nas normas ISO/IEC 27001 e 27002, e às disposições da Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

2.4.2 Objetivos da Auditoria

2.4.2.1 Verificar se os acessos aos sistemas (SISPREV Web, SEI, Banco de Dados, E-mail Institucional e demais aplicações) estão alinhados às funções desempenhadas pelos usuários;

2.4.2.2 Identificar acessos indevidos, excessivos, duplicados ou inconsistentes;

2.4.2.3 Verificar se usuários desligados tiveram suas credenciais revogadas;

2.4.2.4 Avaliar se há riscos relacionados a privilégios inadequados;

2.4.2.5 Validar os controles de segurança e de segregação de funções;

2.4.2.1 Emitir recomendações e ações corretivas para mitigação de riscos;

2.4.2.6 Registrar evidências para auditorias internas, externas e para o Pró-Gestão RPPS.

2.4.3 Escopo da Auditoria

2.4.3.1 A auditoria abrangerá, no mínimo:

a) Sistema SISPREV Web;
b) Sistema Eletrônico de Informações – SEI;
d) Active Directory (AD) ou mecanismos de autenticação equivalentes;
e) E-mail institucional;
f) Servidores de arquivos e pastas compartilhadas;
g) Acessos administrativos (root, administrador, superusuário);
h) Acessos a bancos de dados.

2.4.4 Periodicidade

2.5.4.1 A Auditoria de Acessos será realizada obrigatoriamente a cada 6 (seis) meses, preferencialmente nos meses de junho e dezembro.

2.4.4.2 Situações extraordinárias que exijam revisão imediata poderão ser acionadas, tais como:

a) Incidentes de segurança;
b) Vazamento de dados;
c) Ataques cibernéticos;
d) Alterações estruturais nos sistemas;
e) Trocas de gerência ou reorganização administrativa.

2.4.5 Procedimentos da Auditoria

2.4.5.1 A auditoria seguirá o fluxo abaixo:

I – Extração das Listas de Usuários

A GTI deverá extrair relatórios contendo:

a) Nome completo
b) CPF
c) Setor de lotação
d) Função / cargo
e) Tipo de acesso e permissões
f) Data da criação da conta
g) Último acesso
h) Situação (ativo / inativo)

II – Validação com as Gerências

Cada relatório será enviado aos responsáveis das Gerências, Diretorias e Presidência para validação funcional dos acessos.

III – Confronto com o Cadastro de RH

Será realizada conferência com o cadastro de pessoal para verificar:

a) Usuários desligados
b) Usuários em afastamento
c) Alteração de funções
d) Movimentações internas

IV – Análise Técnica pela GTI

A GTI avaliará:

a) Privilégios excessivos
b) Contas sem uso (90 dias)
c) Acessos administrativos inconsistentes
d) Perfis duplicados
e) Senhas provisórias não alteradas
f) Acessos externos e remotos
g) Riscos de segregação de funções (ex.: concessão e homologação)

V – Aplicação de Correções

A GTI executará as correções necessárias:

a) Revogação de acessos indevidos
b) Readequação de permissões
c) Exclusão de contas inativas
d) Ajuste de perfis conforme matriz

VI – Evidências e Registro em SEI/SISPREV
Todas as evidências obrigatórias deverão ser arquivadas:

a) Relatórios extraídos
b) Planilhas analisadas
c) Pareceres das gerências
d) Comprovantes de correção

2.4.5.2 O processo será criado no SEI com o assunto: **Auditoria Semestral de Acessos aos Sistemas – Segurança da Informação**, Nível de acesso: **restrito**, conforme LGPD e PSI.

2.4.6 Responsabilidades

I – Gerência de Tecnologia da Informação (GTI)

a) Executar a auditoria semestral;
b) Emitir relatórios técnicos;
c) Propor ações corretivas;
d) Validar acessos privilegiados;
e) Garantir evidências para auditorias externas.

II – Gerências e Diretorias

a) Validar perfis e permissões de seus servidores;
b) Comunicar inconsistências;
c) Autorizar readequações necessárias.

III – Presidência do IPER

a) Aprovar ações estratégicas e medidas de alto impacto;
b) Garantir recursos para execução das melhorias recomendadas

2.4.7 Relatório Final da Auditoria

O relatório final deverá conter:

a) Sumário executivo;
b) Quantitativo de usuários por sistema;
c) Não conformidades encontradas;
d) Acessos suspensos ou corrigidos;
e) Riscos identificados;
f) Ações corretivas adotadas;
g) Riscos residuais;
h) Evidências anexas;

i) Recomendações para o próximo ciclo.

2.4.7.1 O relatório deverá ser assinado digitalmente e mantido em SEI pelo prazo mínimo previsto na Tabela de Temporalidade.

2.4.8 Indicadores de Desempenho (KPIs)

2.4.8.1 Os seguintes indicadores deverão ser monitorados:

Indicador	Meta	Periocidade
% de contas inativas identificadas	0%	Semestral
% de acessos corrigidos no prazo	≥ 95%	Semestral
% de usuários validados pelas gerências	100%	Semestral
Incidentes relacionados a acessos	0	semestral

2.4.9 Conformidade e Sanções

2.4.9.1 O não cumprimento das diretrizes desta auditoria poderá resultar:

a) Em responsabilização administrativa (LC 53/2001);
b) Em responsabilização civil ou penal;
c) Em medidas disciplinares previstas nas normas internas;
d) Em reporte à Presidência.

3.4 DIVULGAÇÃO, CONSCIENTIZAÇÃO E TREINAMENTO DA POLÍTICA DE SEGURANÇA

3.4.1 A Política de Segurança da Informação do IPER dependerá da ampla disseminação de seus conteúdos e da contínua conscientização dos servidores, estagiários, prestadores de serviços e fornecedores. Para isso, estabelece-se o seguinte conjunto de diretrizes para divulgação, capacitação, atualização e desenvolvimento da cultura de segurança da informação.

3.4.2 Realização de treinamento semestral obrigatório sobre segurança e privacidade;

3.4.3 Divulgação da PSI e cartilhas digitais no portal interno e site institucional;

3.4.4 Assinatura de termo eletrônico de ciência pelos usuários.

3.4.5 Divulgação da Política de Segurança da Informação

3.4.5.1 A Política de Segurança da Informação (PSI) deverá ser divulgada por meio de canais institucionais, incluindo:

a) Portal interno do IPER (Intranet);
b) Página institucional do IPER na Internet;
c) Comunicados oficiais via e-mail institucional;
e) Eventos presenciais e/ou virtuais promovidos pela GTI (Gerência de Tecnologia da Informação).

3.4.5.2 A PSI deverá estar acessível a todos os usuários, garantindo fácil consulta e compreensão.

3.4.5.3 Toda contratação que envolva acesso a dados, sistemas ou infraestrutura do IPER deverá incluir cláusula de adesão e vinculação às diretrizes da PSI.

3.4.5.4 Prestadores de serviços, fornecedores e parceiros externos deverão receber a versão vigente da PSI, devendo atestar formalmente que tiveram ciência das diretrizes estabelecidas

3.4.6 Conscientização em Segurança da Informação

3.4.6.1. A conscientização dos usuários é parte essencial do processo de governança de segurança da informação e deverá ocorrer de forma contínua e periódica.

3.4.6.2. O IPER promoverá campanhas permanentes sobre boas práticas de segurança, com foco em:

a) Prevenção contra ataques cibernéticos (phishing, engenharia social, malware, ransomware);
b) Proteção de dados pessoais e sigilosos (conforme LGPD);
c) Uso adequado da internet, e-mail e equipamentos institucionais;
d) Recomendações de segurança para senhas, dispositivos móveis e acesso remoto;
e) Regras de tratamento, classificação e guarda de documentos;
f) Boas práticas de prevenção contra vazamento de dados e incidentes de privacidade.

3.4.6.3. A Gerência de Tecnologia da Informação (GTI), em conjunto com o CSI, deverá elaborar materiais educativos, como:

a) Vídeos curtos;
b) Cartazes internos;
c) Cartilhas ilustradas;
d) Orientações periódicas por e-mail;
e) Informativos de riscos e alertas de segurança.

3.4.6.4. Os materiais de conscientização deverão ser atualizados com base em ameaças emergentes, recomendações da ANPD e melhores práticas de mercado.

3.4.7 Treinamento Obrigatório

3.4.7.1 Todos os servidores, estagiários e prestadores de serviços deverão participar, anualmentedo Treinamento Obrigatório de Segurança da Informação, que abordará:

a) Conceitos fundamentais de segurança;
b) Princípios da PSI do IPER;
c) Política de classificação da informação;
d) Procedimentos de contingência e resposta a incidentes;

e) Procedimentos operacionais de uso dos sistemas (SEI, SISPREV, e-mail, rede etc.);
f) Boas práticas de proteção de dados pessoais;
g) Responsabilidades legais e administrativas em caso de violação.

3.4.7.3. Ao final de cada treinamento, deverá ser realizado registro de participação, com certificação individual, que será arquivado no SEI para fins de comprovação junto às auditorias do Pró-Gestão.

3.4.7.4. Novos servidores, estagiários e prestadores de serviços recém-admitidos deverão obrigatoriamente receber treinamento introdutório de segurança da informação nos primeiros 30 dias.

3.4.8 Obrigações dos Usuários

3.4.8.1 Os usuários deverão:

a) Ler e compreender a PSI e seus anexos;
b) Assinar os Termos de Ciência e Responsabilidade;
c) Cumprir todas as diretrizes da PSI;
d) Comunicar imediatamente incidentes, suspeitas de incidente ou uso indevido de informações;
e) Zelar pelo sigilo das credenciais de acesso;
f) Participar dos treinamentos obrigatórios anuais;
g) Aplicar as práticas aprendidas no ambiente de trabalho.

3.4.8.2 O não cumprimento das obrigações poderá resultar em responsabilização administrativa, civil e penal, conforme normas internas e legislação vigente.

3.4.9 Monitoramento e Avaliação da Eficácia

3.4.9.1 A Gerência de Tecnologia da Informação avaliará, anualmente, a eficácia das ações de divulgação e treinamento, por meio de:
a) Indicadores de participação;

3.5 Política de Classificação e Temporalidade

3.5.1 A classificação e a temporalidade das informações do Instituto de Previdência do Estado de Roraima – IPER seguem critérios formais destinados a assegurar a adequada proteção, o acesso, a guarda e a destinação dos documentos e dados produzidos ou recebidos no âmbito institucional. Tais procedimentos integram a gestão documental e estão diretamente vinculados à proteção de dados pessoais e à segurança da informação.

3.5.2 A Política de Classificação e Temporalidade da Informação do IPER observa, obrigatoriamente, os seguintes instrumentos normativos: Portaria nº 188/2024 – IPER: Aprova o Plano de Classificação de Documentos; Portaria nº 189/2024 – IPER: Aprova a Tabela de Temporalidade de Documentos Administrativos; Portaria nº 190/2024 – IPER: Aprova a Tabela de Temporalidade de Documentos Previdenciários;

3.6. Utilização das Normas do Plano de Contingência do IPER (anexo F)

3.6.1 As normas do Plano de Contingenciamento (anexo F), constitui o instrumento normativo e operacional que detalha os procedimentos necessários para garantir a continuidade dos serviços essenciais de Tecnologia da Informação e a preservação dos ativos informacionais em situações de incidentes, falhas críticas, desastres, interrupções de conectividade, ataques cibernéticos ou qualquer evento que comprometa a disponibilidade, integridade ou confidencialidade das informações sob responsabilidade do Instituto.

4.DOCUMENTOS COMPLEMENTARES

- Constituição Federal.
- Constituição Estadual.
- Portaria Nº 1.467/2022.
- EC 103/2019.
- Norma ISO/IEC 27002/2022.
- Lei Geral de Proteção de Dados, LEI Nº 13.853, DE 8 DE JULHO DE 2019.
- Lei de Acesso à Informação, Lei nº 12.527/2011 e suas atualizações.
- Decreto 27.971-E/2020

- Decreto Nº 20.477-E DE 16 DE FEVEREIRO DE 2016.
- PORTARIA MTP Nº 1.467, DE 02 DE JUNHO DE 2022.
- INSTRUÇÃO NORMATIVA 004/2018-TCE/RR.
- Decreto Nº 32.307-E/2022.
- Lei nº 14.289/2022
- INSTRUÇÃO NORMATIVA 94/2022.
- Manual do Pró-Gestão
- Manual do usuário SEI- Roraima.
- PORTARIA Nº 188/IPER/PRESI/GPRES, DE 28 DE FEVEREIRO DE 2024.
- ANEXO-CÓDIGO DE CLASSIFICAÇÃO E TABELA DETEMPORALIDADE E DESTINAÇÃO DE DOCUMENTOSRELATIVOS ÀS ATIVIDADES-MEIO.
- PORTARIA Nº 189/IPER/PRESI/GPRES, DE 28 DE FEVEREIRO DE 2024.
- PORTARIA Nº 190/IPER/PRESI/GPRES, DE 28 DE FEVEREIRO DE 2024. ANEXO - MANUAL DE GESTÃO DE DOCUMENTOS.

5. MATRIZ DE RESPONSABILIDADES

O Instituto de Previdência do Estado de Roraima (IPER)tem definida na sua matriz de responsabilidade e atribuições o Principal Responsável (P) e o Co-responsável (C) das atividades do processo:

Matriz de Responsabilidades									
		RESPONSABILIDADES							
Nº	Atribuição	Presidente	Vice Presidente	Conselho de Previdência	Diretor de Administração e Finanças	Gerente de TI	Técnicos de Informática	Servidores	Prestadores de Serviço
1	Aprovar a Política de Segurança da Informação	P	C	C	----	----	----	----	----
2	Revisão da Política de Segurança da Informação	----	----	----	----	C	C	----	----
3	Implantação das ações da Política de Segurança da Informação	----	----	----	P	P	P	----	----
4	Treinamento e capacitação de pessoas	----	----	----	----	P	P	----	----
5	Cumprir a Política de Segurança da Informação	P	P	P	P	P	P	P	P
6	Comunicação da Política de Segurança da Informação	P	---	----	P	P	P	----	----
7	Monitoramento das ações	----	----	----	P	P	----	----	----

6. DESCRIÇÃO DO PROCESSO

Deve-se apresentar quais os processos e subprocessos estarão descritos no manual de operação.

a) .TERMOS, ABREVIATURAS, SIGLAS E DEFINIÇÕES

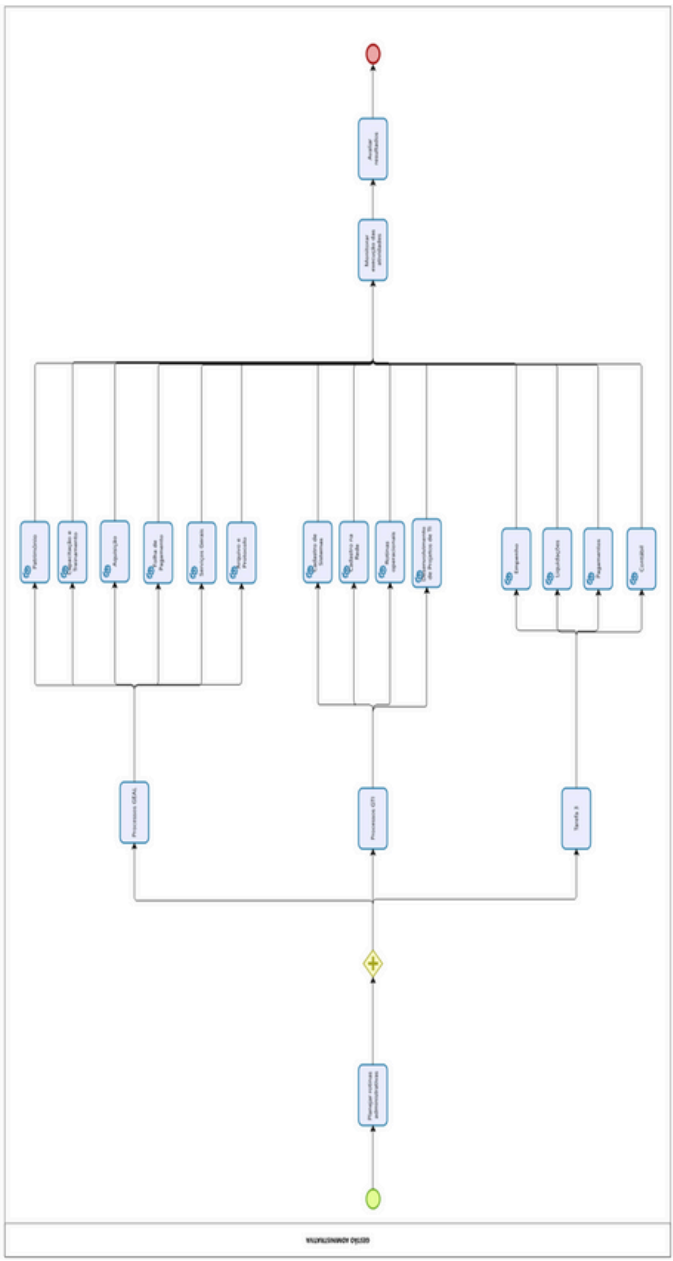
Afim de fazer com que o servidor tenha alinhamento com o processo é importante conceituar todos os termos e definições que serão aplicados durante a execução das suas atividades de forma contextualizada.

Item	Termo	Descrição
1	Endereço IP:	código atribuído a recurso de TI (do IPER ou externo) com objetivo de identificá-lo unicamente na Internet ou em uma rede interna. Exemplo: "143.54.1.20", "8.8.4.4", "2804:1f20:0:1::20". Gestor de Recurso de TI: pessoa responsável por algum recurso de TI.
2	Firewall institucional:	conjunto de equipamentos e tecnologias que visam implementar e monitorar a política de comunicação da rede de dados do IPER com a Internet.
3	Gestor de Recurso de TI:	pessoa responsável por algum recurso de TI.
4	Incidente de Segurança:	violação de requisito de segurança estabelecido por gestor de recurso de TI ou violação de legislação ou norma vigente
5	Recurso de TI:	equipamento de computação ou telecomunicação de dados que utilize a rede de dados ou que custodie informações da Universidade ou relacionados a processos de negócio da mesma. Também são recursos de TI quaisquer serviços e aplicações, de armazenamento ou comunicação, fornecidos por equipamentos de qualquer natureza. Exemplos de recursos de TI são computadores desktops, terminais de acesso, servidores, equipamentos de rede como comutadores (switches) e roteadores, equipamentos de suporte com acesso a rede como nobreaks e geradores, equipamentos de comunicação como telefones VoIP, e todos os softwares, aplicações e informações que estejam armazenados em quaisquer destes dispositivos, entre outros.
6	TI:	Tecnologia da Informação
7	URL:	Universal Resource Locator ou Localizador Universal de Recurso, texto que indica o endereço de localização na Internet de um sítio ou aplicação Web. Exemplos: "www.iper.rr.gov.br";

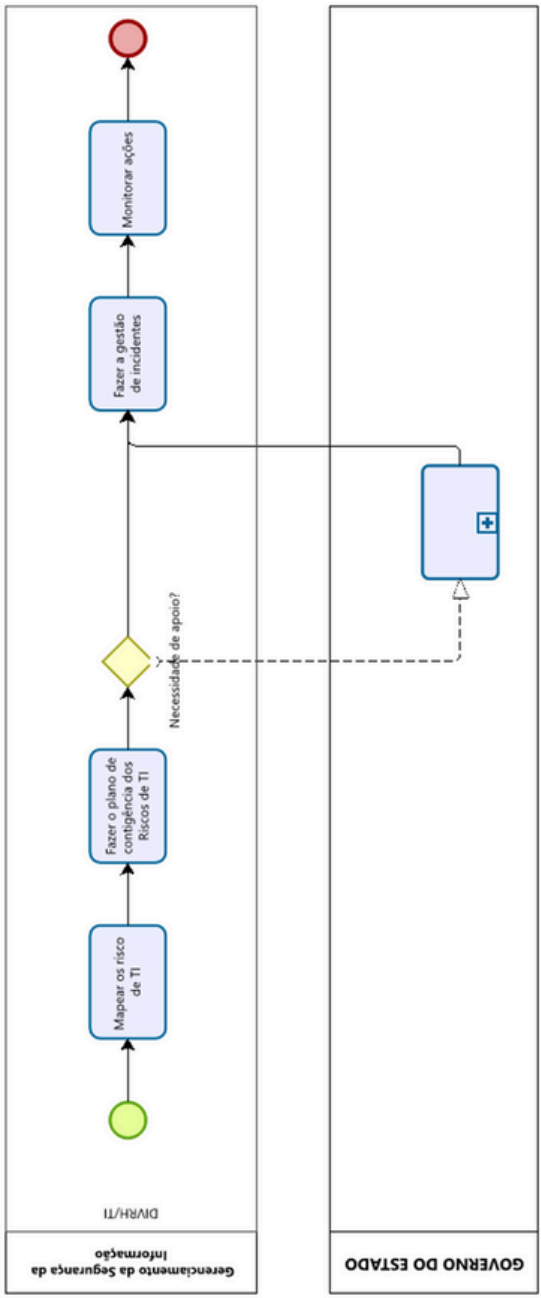
Item	Termo	Descrição
9	Agente de Criptografia:	Indivíduo que utiliza de técnicas que transformam/esconde/codifica informação inteligível em algo que um agente externo seja incapaz de compreender.
10	DEK (Chave de Criptografia de Dados) Criptografada:	É um tipo de chave projetada para criptografar e descriptografar dados pelo menos uma vez, ou possivelmente várias vezes. As DEKs são criadas por um mecanismo de criptografia. Os dados são criptografados e descriptografados com a ajuda da mesma DEK; portanto, uma DEK deve ser armazenada por pelo menos uma duração especificada para descriptografar o texto cifrado gerado.
11	KMS (Sistema de Gerenciamento de Chaves):	Fornece uma visão geral do material de chave utilizado na empresa. Ele possibilita o acesso controlado a dados criptografados de acordo com a estratégia de segurança da TI.
12	AES (Padrão Avançado de Criptografia):	É um tipo de cifra (um método de transformar uma mensagem para ocultar seu significado) que protege a transferência de dados pela internet. Atualmente um dos protocolos de criptografia mais comuns e confiáveis.
13	CRM:	Base de dados da Zoho Services que impede que os dados sejam roubados ou perdidos, convertendo o texto claro (ou legível) em texto cifrado (ou não legível) acessível apenas a partes autorizadas. Mesmo que um potencial invasor tenha acesso aos dados, as informações armazenadas no texto cifrado são não legíveis.

6.2 FLUXOGRAMA DO PROCESSO

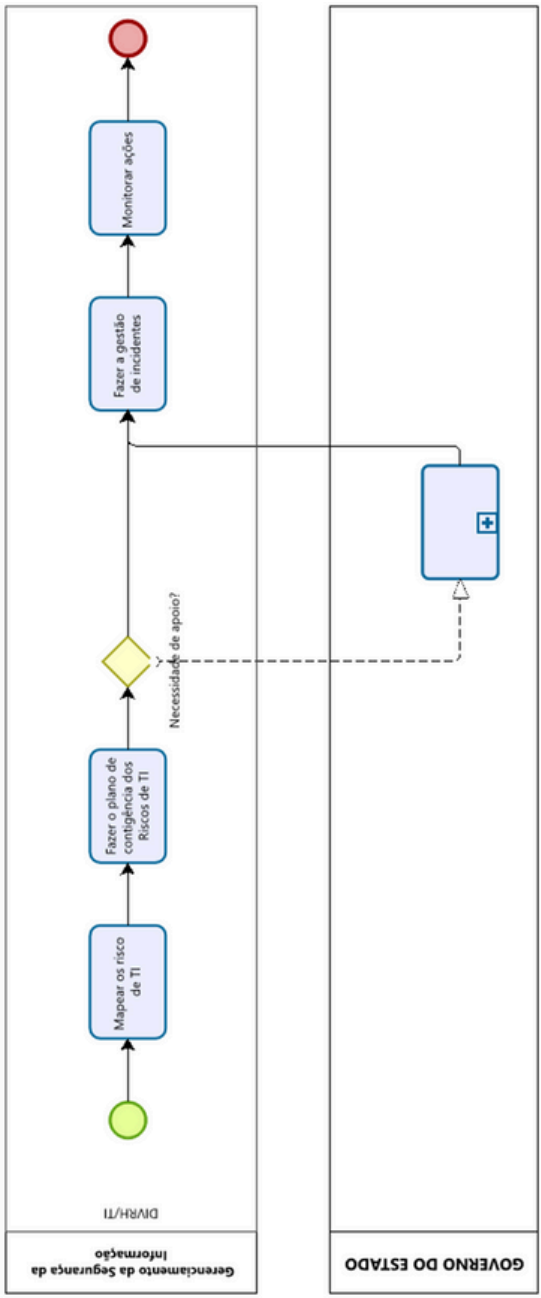
6.2.1FLUXOGRAMA GESTÃO ADMINISTRATIVA: GTI



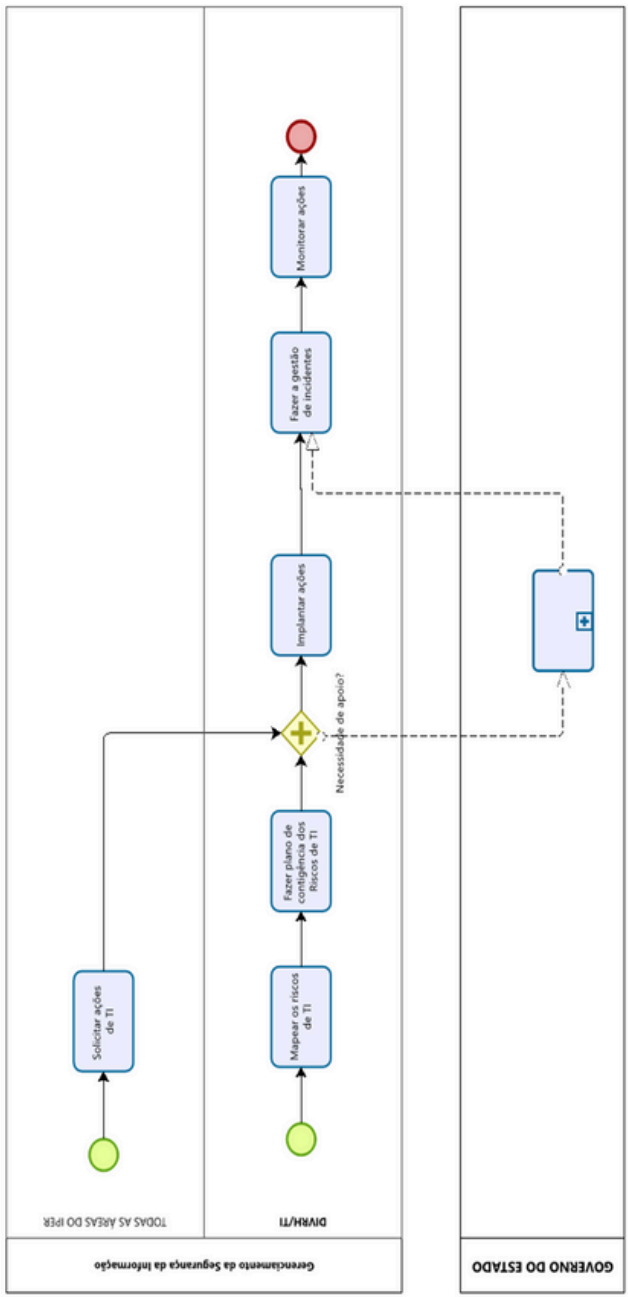
6.2.1FLUXOGRAMA PLANO DE CONTINGÊNCIAS



6.2.2 FLUXOGRAMA PLANO DE CONTINGÊNCIAS



6.2.3 FLUXOGRAMA GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO



6.3 DETALHAMENTO DO PROCESSO

Descrever detalhadamente as atividades mapeadas nos seus respectivos fluxos

Etapa	Atividade	Responsável	Detalhamento da tarefa	Controle da Atividade
1	Identificação dos principais sistemas	Gerente de T.I	1. Receber as demandas de necessidades dos setores 2. Identificar os Sistema de acordo com as necessidades; 3. Incluir no plano de aquisições anualmente	Gerência de TI -GTI
2	Identificação dos Riscos	Gerente de T.I	1. identificar dos riscos; 2. analisar riscos; 3. avaliar os riscos; 4. tratar os riscos e monitoramento 5. analisar a crítica dos riscos	Gerência de TI -GTI
3	Regras de uso internet	Gerente de T.I	1. Receber ato de nomeação de servidores, estagiários com devidos setores/cargos 2. Solicitar e receber o acesso aos sistemas aos responsáveis 3. Encaminhar a efetivação do acesso a Divisão Recursos Humanos	Gerência de TI -GTI
4	Uso de e-mail	Gerente de T.I	Toda a comunidade da IPER tem direito a um endereço eletrônico no domínio "iper.rr.gov.br". Visando a garantia da autenticidade das comunicações oficiais da Universidade, todos os servidores efetivos, cargos comissionados e estagiários devem utilizar o endereço com domínio “iper.rr.gov.br” para comunicações relacionadas às suas funções no Instituto. 1. Receber ato de nomeação de servidores, estagiários com devidos setores/cargos 2. Realizar o cadastro do e-mail 3. Encaminhar a efetivação do acesso ao Divisão de Recursos Humano	Gerência de TI -GTI
5	Utilização de unidades de armazenamento portátil	Equipe Técnica de T.I	1. Receber solicitação do Pedido de Acesso Responsável do Setor 2. Encaminhar a efetivação do acesso ao Responsável do Setor	Gerência de TI -GTI
6	Antivírus	Equipe Técnica de T.I	1. Identificação de Atualização de Ferramenta Antivírus 2. Realização da Atualização de Ferramenta Antivírus	Gerência de TI -GTI

7	Regras de acesso aos sistemas	Gerente de T.I	1. Receber ato de nomeação de servidores, estagiários com devidos setores/cargos 2. Solicitar e receber o acesso aos sistemas aos responsáveis 3. Encaminhar a efetivação do acesso ao Recursos humanos	Gerência de TI -GTI
8	Regras de acesso aos ambientes	Gerente de Administração e Logística	1. Realizar o atendimento inicial na portaria 2. Conferir o documento de identificação e anotar em lista própria 3. Encaminhar para a sala/setor competente	Setor de Serviços Gerais
9	Regras de exposição dos sistemas (uso de celular)	Gerente de T.I	1. Receber ato de nomeação de servidores, estagiários com devidos setores/cargos 2. Solicitar e receber o acesso aos sistemas aos responsáveis 3. Encaminhar a efetivação do acesso ao Recursos humanos	Gerência de TI -GTI
10	Regras de criptografia	Gerente de T.I	1- O agente de criptografia deve determinar, com base nos metadados, se há necessidade de criptografar o campo antes de armazená-lo no banco de dados. 2- O agente da criptografia deve verificar a memória cache quanto a DEKs correspondentes. Se nenhuma DEK correspondente for encontrada, o agente de criptografia solicitará uma DEK do KMS. 3-O KMS verifica seu banco de dados quanto a uma DEK criptografada correspondente. 3.1 Se uma DEK criptografado correspondente for encontrada, o KMS descriptografará a DEK criptografada e a retornará ao agente de criptografia. 3.2 Se nenhuma DEK correspondente for encontrada, o KMS gerará uma DEK. Essa nova DEK é criptografada com KEKs e armazenada nos servidores do KMS. 4. O agente deve receber a DEK e, em seguida, criptografa/descriptografa os dados usando criptografia AES de 256 bits. 5. O texto cifrado (os dados criptografados) é, então, armazenado no CRM (no banco de dados/sistema de arquivos do Zoho Services).	Gerência de TI -GTI

11	Regras de uso, compartilhamento e disponibilização de senhas de uso de terceiros	Gerente de T.I	1. Receber solicitação do Pedido de Acesso Responsável do Setor 2. Encaminhar o TERMO de efetivação ou a negação do acesso ao Responsável do Setor	
12	Regras de uso de wifi	Gerente de T.I	1. GTI: Receber solicitação do Pedido de Acesso Responsável do Setor 2. GTI: Encaminhar a efetivação do acesso ao Responsável do Setor	
13	Regras de atualização de sistemas	Gerente de T.I	1. Verificar as atualizações de sistemas 2. Executar as atualizações existentes	
14	Regras de compra de equipamentos	Gerente de T.I	1. Verificar as necessidades; 2. Descrever as configurações de acordo com os padrões normativos; 3. Solicitar Autorização de Aquisição 4. Elaborar ETP 5. Encaminhar para a GEAL continuar a Aquisição	
15	Regras de uso de ferramentas de comunicação	Gerente de T.I	1. Definir as Ferramentas; 2. Configurar perfil de usuários das Ferramentas; 3. Instalar as Ferramentas;	
16	Regras de backup físico e em nuvem	Gerente de T.I	**4. Regras para Backup Físico: Identificação de Dados Críticos: Listar e identificar os dados críticos que precisam ser copiados regularmente. Frequência de Backup: Estabelecer a frequência de backup com base na taxa de alteração dos dados e na importância deles.** 1. **Mídia de Armazenamento:** Escolher mídias de armazenamento confiáveis, como discos rígidos externos, fitas magnéticas ou unidades USB. 2. **Local de Armazenamento:** Manter cópias dos backups em locais físicos separados para proteção contra desastres, como incêndios ou inundações. 3. **Segurança Física:** Proteger fisicamente os dispositivos de backup para evitar acesso não autorizado ou danos. 4. **Criptografia:** Utilizar criptografia para proteger os dados armazenados em dispositivos físicos contra acessos não autorizados. **Regras para Backup em Nuvem:** **1. Seleção do Provedor de Nuvem:** Escolher um provedor de nuvem confiável e compatível com os requisitos de segurança da sua organização.	

			2. Política de Retenção: Definir uma política de retenção para determinar por quanto tempo os backups serão mantidos na nuvem. **3. Autenticação Multifator (MFA):** Ativar a autenticação multifator para reforçar a segurança do acesso à nuvem. **4. Encriptação de Dados:** Certificar se os dados em trânsito e em repouso na nuvem estejam criptografados. **5. Testes de Restauração:** Realizar testes regulares de restauração para garantir que os backups na nuvem possam ser recuperados conforme necessário. **6. Monitoramento e Alertas:** Implementar sistemas de monitoramento para detectar atividades suspeitas e configure alertas para notificar sobre possíveis problemas. **7. Compliance:** Certificar se o armazenamento em nuvem esteja em conformidade com regulamentações de privacidade e segurança aplicáveis.	
17	Política de Segurança de redes	Gerente de T.I	1- Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal. 2- Utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha. 3- Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma. 4- Não armazenar senhas nos navegadores (Mozila, Chrome, Internet Explore etc.), pois são facilmente visualizadas e comprometem a segurança das informações. 5- A distribuição de senhas aos usuários de Tecnologia da Informação (inicial ou não) deve ser feita de forma segura.	Receber ato de nomeação de servidores, estagiários com devidos setores/cargos 2- Solicitar e receber o acesso aos sistemas aos responsáveis 3- Encaminhar a efetivação do acesso ao Recursos humanos

			A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso. 6- A troca de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário.	
18	Política de treinamento de servidores em TI e Segurança da Informação	Gerente de T.I	1- Definir a Política de treinamento de servidores em TI e Segurança da Informação; 2- Atualizar a Política de treinamento de servidores em TI e Segurança da Informação	
19	Regras de proteção de informações em meio físico	Gerente de T.I	1- Estabelecer regras de proteção de informações em meio físico; 2- Seguir as regras de proteção de informações em meio físico;	
20	Regras de descarte de mídias e informações	Gerente de T.I	1- Descritas na Política de Proteção de Dados.	
21	Regras para uso de impressora e scanners	Gerente de T.I	1- Documento enviado para a impressora deverá ser retirado com uso de senha de rede. 2- A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. 3- Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não autorizado. Isto é, documentos esquecidos nas impressoras, ou com demora em retirada, ou até mesmo em cima da mesa, podem ser lidos, copiados ou levados por outro funcionário ou por alguém de fora da rede do IPER.	
22	Regras de utilização de rede, software, internet, acesso físico e lógico, documentos e sistemas por fornecedores e prestadores de serviços.	Gerente de T.I	Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal. 2- Utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar	

			informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha. 3- Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma. 4- Não armazenar senhas nos navegadores (Mozila, Chrome, Internet Explore etc.), pois são facilmente visualizadas e comprometem a segurança das informações. 5- A distribuição de senhas aos usuários de Tecnologia da Informação (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso. 6- A troca de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário.	
23	Regras de privacidade de dados	Gerente de T.I	1. Avaliar a Inicial de Privacidade 2. Desenvolver de Políticas de Privacidade 3. Implementar de Medidas de Segurança 4. Conscientizar e manter os funcionários informados sobre as melhores práticas e responsabilidades relacionadas à privacidade de dados. 5. Gerenciar o Consentimento e os Incidentes de Privacidade 6. Monitorar, Auditar e Implementar sistemas para monitorar continuamente o cumprimento das políticas de privacidade e a segurança dos dados. 7. Revisar e Atualizar as Políticas	

24			Plano de Contingência para o Setor de Tecnologia da Informação: 1. Identificação de Riscos: - Realizar uma análise detalhada dos possíveis riscos que podem afetar o setor de TI, como falhas de hardware, ataques cibernéticos, desastres naturais, entre outros. 2. Estratégias de Backup: - Implementar rotinas regulares de backup dos dados críticos, armazenando essas cópias em locais seguros e fora das dependências do órgão. 3. Segurança Cibernética: - Reforçar as medidas de segurança cibernética, como firewalls, antivírus atualizados, autenticação em dois fatores e políticas de acesso restrito aos sistemas. 4. Plano de Recuperação de Desastres: - Elaborar um plano detalhado de recuperação de desastres, com procedimentos claros sobre como restaurar os sistemas e os dados em caso de incidentes graves. 5. Testes e Treinamentos: - Realizar testes periódicos do plano de contingência para garantir sua eficácia e promover treinamentos regulares com a equipe para que todos saibam como agir em situações emergenciais. 6. Comunicação e Coordenação: - Estabelecer canais claros de comunicação interna e externa para informar rapidamente sobre incidentes e coordenar as ações necessárias para a mitigação dos impactos. 7. Monitoramento Contínuo: - Implementar sistemas de monitoramento contínuo da infraestrutura de TI para identificar precocemente possíveis problemas e agir proativamente na sua resolução. 8. Revisão Periódica: - Revisar a cada dois anos o plano de contingência, atualizando-o conforme novas ameaças e tecnologias surgirem, garantindo a sua relevância e eficácia contínuas.	

25	Monitoramento da Segurança de Informação	Gerente de T.I	1. Implementar sistemas de monitoramento para detectar atividades suspeitas 2. Configurar alertas para notificar sobre possíveis problemas.	
26	Política de Consequências (Código de ética e Regime Jurídico de Servidores – LC nº 053/2001).	Comissão de Ética	1- Identificar das regras de acordo com a política de ética do IPER; 2- Aplicar o Código de Código de ética do IPER.	
27	Plano de Atualização da PSI (revisão a cada 2 anos).	Gerente de T.I	1- Revisar e Analisar a versão atual da PSI para identificar áreas que precisam de atualização ou melhoria. 2- Identificar as Mudanças Necessárias: Listar as mudanças na legislação, regulamentação, tecnologia e operações que impactam a PSI. 3.Definir os objetivos específicos da atualização da PSI . 4- Revisar e Submeter a nova versão da PSI para revisão interna por todas as partes interessadas relevantes. 5- Aprovar pela Alta Administração: Obter a aprovação formal da nova PSI pela alta administração ou pelo comitê de governança de TI. 6- Divulgar a Nova PSI: Comunicar a nova PSI a todos os funcionários e partes interessadas. 7- Atualizar os Documentos e Recursos: Atualizar todos os documentos e recursos relacionados à PSI (por exemplo, manuais de políticas, intranet da empresa). 8- Monitorar continuamente e Estabelecer processos para monitorar a conformidade com a nova PSI e identificar quaisquer problemas ou áreas de melhoria. 9- Realizar avaliações periódicas para garantir que a PSI continua relevante e eficaz, e para planejar futuras atualizações.	

7. REVISÃO E ATUALIZAÇÃO

6.1 Esta Política será revisada a cada dois anos, ou sempre que houver:

a) Alterações legais ou regulamentares relevantes;
b) Mudanças significativas na infraestrutura tecnológica;

8. ANEXOS

- MATRIZ DE IDENTIFICAÇÃO DE RISCOS
- QUADRO DO SISTEMAS DE INFORMAÇÕES IPER
- TERMO DE RESPONSABILIDADE DE USO DE EQUIPAMENTOS, CIÊNCIA DE USO E CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IPER
- TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS FORNECEDORES E PRESTADORES DE SERVIÇOS
- TERMO DE CONFIDENCIALIDADE E SIGILO
- PLANO DE CONTINGÊNCIA E CONTINUIDADE DE TECNOLOGIA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA DO ESTADO DE RORAIMA – IPER
- TERMO DE USO E RESPONSABILIDADE DE ACESSO A SISTEMAS

ANEXO A - MATRIZ DE RISCOS DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO

RISCO	FATOR DE RISCO	TIPO	PROBABILIDADE	CONSEQUÊNCIA	CLASSIFICAÇÃO DO RISCO INERENTE	TRATAR?	TIPO DE TRATAMENTO	CONTROLES	PRAZO INICIAL	PRAZO FINAL
Ataques Cibernéticos	Falta de controle de acesso.	Operacional	4. Muito provável	4. Alta		Sim	Redução da probabilidade	Criar as diretrizes para controle de acesso físico e aos sistemas da empresa	16/08/2023	30/08/2023
Ataques Cibernéticos	Não ter antivírus.	TI	2. Improvável	2. Baixa		Não	Não realizar	Verificar a atualização contínua dos antivírus instalados	16/08/2025	16/08/2026
Ataques Cibernéticos	Falta de treinamento para configuração de firewall.	Operacional	4. Muito provável	4. Alta		Sim	Redução da consequência	Elaborar Plano de Treinamento	16/08/2024	31/12/2026
Desvios de conduta	Servidor fornecer senhas não autorizadas	Operacional	4. Muito provável	5. Extrema		Sim	Redução da probabilidade e consequência	Criar as diretrizes e regras para utilização de senhas	16/08/2023	16/12/2024
Risco de Disponibilidade	Rompimento de fibra ótica para transmissão de internet.	TI	5. Quase certo	4. Alta		Sim	Redução da consequência	Adquirir redundância de link	16/08/2024	30/03/2026
Privacidade de dados	Acesso indevido a dados pessoais.	Operacional	3. Provável	4. Alta		Sim	Redução da probabilidade	Criar política de controle de acesso	16/08/2024	31/12/2026
Fraudes Tecnológicas	Utilização de senhas fracas.	Operacional	4. Muito provável	4. Alta		Sim	Redução da probabilidade	Implementar medidas de segurança robustas	16/08/2023	Implementado
Atualização Tecnológica	Falta de Planejamento Orçamentário.	Estratégico	3. Provável	4. Alta		Sim	Redução da probabilidade	Realização de planejamento anual	16/08/2023	31/12/2024
Ambiente de Segurança	Falta de Controle de Acesso físico a CPD.	Operacional	2. Improvável	2. Baixa		Não	Não realizar		16/08/2023	31/12/2026
Não cumprimento de requisitos legais	Falta de Atualização de Requisitos Legais nos Sistemas.	Compliance	4. Muito provável	4. Alta		Sim	Redução da probabilidade e consequência	Criar diretrizes de prazos de implementações importantes	16/08/2024	31/12/2026
Conflito de interesses	Falta de Critérios Definidos para Tomada de decisão.	Estratégico	3. Provável	4. Alta		Sim	Redução da probabilidade e consequência	Elaborar justificativas técnicas e objetivas	16/08/2024	31/10/2026
Ambiente de Segurança	Falta de controle de acesso físico.	Operacional	3. Provável	3. Moderada		Sim	Redução da probabilidade	Criar um controle de registo de acesso ao ambiente	16/08/2024	31/10/2026
Privacidade de dados	Vazamento de informações.	Operacional	3. Provável	4. Alta		Sim	Redução da probabilidade	Assinatura de termo de responsabilidade e implantação de ferramentas de identificação do usuário.	25/08/2023	31/10/2026
Risco de Confidencialidade	Não ter a classificicação das informações.	Estratégico	4. Muito provável	4. Alta		Sim	Compartilhamento	Definir os critérios de classificação das informações do IPER	25/08/2023	31/10/2026
Risco de Integridade	Manipulação indevidos de dados.	Operacional	2. Pouco Provável	4. Alta		Sim	Redução da probabilidade	Assinatura de termo de responsabilidade e implantação de ferramentas de identificação do usuário.	25/08/2023	31/01/2026
Risco de Disponibilidade	Indisponibilidade de sistemas, serviços e informações.	TI	3. Provável	4. Alta		Sim	Redução da probabilidade e consequência	Criar redundância nos sistemas, Redundância de internet	25/08/2023	31/12/2026
Fraudes Tecnológicas	Adulteração de sistemas e redes	Operacional	2. Pouco Provável	4. Alta		Não	Não realizar	Firewall físico e locais, sistemas proprietários, antivírus, infraestrutura tecnológica e sala cofre.	XXX	XXX
Ambiente de Segurança	Utilização de softwares não licenciados.	Operacional	2. Pouco Provável	2. Baixa		Não	Não realizar	Restrição de acesso à administrador de usuário.	XXX	XXX
Conflito de interesses	Desconhecimento da Política de Segurança de Informação e das suas boas práticas.	Compliance	4. Muito provável	4. Alta		Sim	Redução da probabilidade e consequência	Implantar a Política de Segurança da Informação	25/08/2023	31/12/2024
Ambiente de Segurança	Falta de backup.	Estratégico	1. Improvável	4. Alta		Não	Não realizar	Sistema automatizado de backup	XXX	XXX
Ambiente de Segurança	Não ter planos de contingências	Estratégico	3. Provável	4. Alta		Sim	Redução da consequência	Elaborar plano de contingências	25/08/2023	31/10/2023
Ambiente de Segurança	Acesso externo à rede interna sem autorização	Operacional	2. Pouco Provável	4. Alta		Sim	Redução da consequência	Estabelecer ferramentas para bloqueio de acesso, atualização de antivírus e firewall, atualização dos sistemas operacional dos servidores de redes.	25/08/2023	31/10/2023
Ambiente de Segurança	Uso sem autorização de equipamento pessoais para trabalho.	Operacional	1. Improvável	4. Alta		Não	Não realizar	Acesso permitido apenas pelo administrador de redes.	01/10/2023	31/10/2023

ANEXO B - QUADRO DO SISTEMAS DE INFORMAÇÕES IPER

SISTEMAS	APLICAÇÃO	FORNECEDOR
SISPREV (Sistema de Gestão Previdenciária)	Concessão de Benefícios, Almoxarifado, Folha de Pagamento, Financeiro, Investimentos, Arrecadação, Censo e Recadastramento, Portal do Segurado.	Agenda Assessoria
Portal da Transparência	Disponibilização de informações LAI e Prestação de Contas.	Agenda Assessoria
SEI	Sistema de tramitação documentação e processos.	Governo do Estado
FIPLAN	Planejamento, Finanças e Contabilidade	Governo do Estado
iPonto	Sistema de ponto eletrônico de servidores	INSPELL Software
CADPREV	Informações gerais de RPPS	Ministério da Previdência
COMPREV	Compensação Previdenciária	DATAPREV
BG COMPREV	Compensação Previdenciária	DATAPREV
CONTRATOSGOV	Sistema de Gestão e Fiscalização de Contratos	CONTRATOSGOV SISTEMA LTDA
SISTEMA DE INFORMAÇÕES DE REGISTRO CIVIL – SIRC	Plataforma digital que conecta os cartórios aos ambientes de governo eletrônico do Estado Brasileiro	DATAPREV

ANEXOC- TERMO DE RESPONSABILIDADE DE USO DE EQUIPAMENTOS, CIÊNCIA DE USO E CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IPER

1. Identificação do Usuário

Nome: _____
Matrícula: _____
Cargo/Função: _____
Setor/Unidade: _____
Telefone/Contato: _____
E-mail Institucional: _____

2. Equipamentos e Acessos Recebidos

Declaro que recebi do IPER, para uso estritamente institucional, os seguintes recursos tecnológicos:

( ) Computador Desktop – Patrimônio nº _____
( ) Notebook – Patrimônio nº _____
( ) Tablet – Patrimônio nº _____
( ) Smartphone Institucional – Patrimônio nº _____
( ) Acesso ao SEI/RR
( ) Acesso ao SISPREV Web
( ) Acesso à Rede Interna/Wi-Fi IPER
( ) E-mail institucional: _____
( ) Outros: _____

3. Finalidade do Termo

Este termo tem por objetivo: Formalizar a responsabilidade do servidor/colaborador pelo uso adequado e seguro dos equipamentos cedidos; registrar a ciência expressa das diretrizes estabelecidas Manual Operacional de Gestão da Segurança da Informação; vincular o usuário às normas previstas nos itens 2.1 a 3.6, incluindo classificação da informação, uso de internet/e-mail, credenciais, backup, contingência e auditoria.

4. Declaração de Responsabilidade e Obrigações do Usuário
Declaro que estou ciente e de acordo com as seguintes regras:

4.1 Uso dos Equipamentos (Anexo C – Manual – Regras Gerais)
Utilizarei os equipamentos e sistemas exclusivamente para atividades vinculadas ao IPER;
Manterei a integridade física e lógica dos equipamentos sob minha guarda;
Não instalarei softwares, aplicativos ou extensões sem autorização prévia da GTI;
Não utilizarei equipamentos pessoais para executar rotinas institucionais, salvo autorização formal da GTI; realizarei o uso seguro de unidades de armazenamento portátil, conforme diretrizes da GTI.

4.2 Sigilo e Credenciais (Itens 2.3, 17 e 22 do Manual)
Estou ciente de que: Toda credencial é pessoal e intransferível; É proibido compartilhar senhas, acessos ou perfis com terceiros; É obrigatório o uso de senha forte, contendo letras maiúsculas, minúsculas, números e caracteres especiais; É vedado anotar senhas em papel, local visível ou dentro do equipamento; Senhas iniciais devem ser alteradas no primeiro acesso;
Senhas bloqueadas só podem ser desbloqueadas mediante solicitação formal do usuário;
É proibido armazenar senhas em navegadores.

4.3 Classificação e Tratamento da Informação (Item 2.2 do Manual)
Declaro ciência de que devo:
Classificar corretamente documentos no SEI (público, restrito, sigiloso) e no SISPREV (confidencial / não confidencial); respeitar o sigilo legal de dados sensíveis, restritos e sigilosos;
Manter confidencialidade absoluta sobre dados pessoais, previdenciários, médicos e administrativos;
Garantir que documentos impressos ou digitais sejam protegidos contra acesso indevido.

4.4 Uso da Internet, E-mail e Sistemas (Item 2.3 do Manual)
Comprometo-me a:
Utilizar internet e e-mail institucional apenas para fins laborais;
Não acessar conteúdos ilícitos, pornográficos, ofensivos, jogos ou páginas sem relação com o trabalho;

Não realizar download de arquivos sem pertinência laboral;
Usar assinatura de e-mail conforme padrão institucional;
Comunicar imediatamente à GTI qualquer anomalia, suspeita ou incidente;
Evitar abertura de anexos desconhecidos;
Utilizar VPN, acesso remoto ou home office conforme normas da GTI.

4.5 Equipamentos e Impressões (Itens 21 e 2.3)
Documentos impressos devem ser retirados imediatamente; Impressões sigilosas serão realizadas apenas com supervisão; é proibido deixar documentos em mesas, impressoras ou locais públicos.

4.6 Backup, Armazenamento e Restrição (Itens 16, 19, 20)
Não realizarei backups em mídias externas sem autorização da GTI; manterei documentos físicos sob guarda e proteção adequada; seguirei as regras institucionais para descarte de documentos e mídias.

4.7 Monitoramento e Auditoria (Itens 2.4 e 3.4.9)
Estou ciente de que: A GTI pode monitorar logs, acessos, tráfego, tentativas de login e uso operacional; Auditorias semestrais validarão meus acessos e permissões; Inconsistências poderão resultar em bloqueio ou suspensão de acessos.

4.8 Contingência e Incidentes (Itens 24, 3.6 e Fluxos)
Comprometo-me a: Seguir orientações do Plano de Contingência; comunicar imediatamente incidentes de segurança, vazamento, perda de equipamento ou suspeita de violação; adotar medidas preventivas conforme treinamentos e diretrizes da GTI.

5. Ciência da Política de Segurança da Informação (PSI/IPER)
Declaro que: Li e compreendi a PSI/IPER, o Manual Operacional de Gestão da Segurança da Informação e seus anexos; estou ciente das obrigações, proibições e controles neles previstos;
Estou de acordo com a realização de treinamentos periódicos obrigatórios;
Reconheço que qualquer violação poderá gerar responsabilização administrativa, civil e penal, conforme LC 053/2001, LGPD e normas internas do IPER.

6. Devolução dos Equipamentos

Comprometo-me a: Devolver integralmente todos os equipamentos e acessórios quando solicitado ou quando ocorrer mudança de função, setor ou desligamento; garantir que não haverá cópias não autorizadas de dados institucionais; permitir a verificação técnica do equipamento na devolução.

7. Vigência

Este termo permanecerá válido enquanto houver posse, guarda ou acesso a qualquer equipamento, sistema ou informação do IPER.

8. Assinaturas

Usuário
Assinatura:
_____
Data:

Assinatura:
_____
Data:

Conferência/Inventário – GTI
( ) Equipamento entregue
( ) Acessos liberados
( ) Treinamento realizado
( ) Registro de inventário atualizado

Responsável pela Entrega

ANEXO E
TERMO DE CONFIDENCIALIDADE E SIGILO
INSTITUTO DE PREVIDÊNCIA DO ESTADO DE RORAIMA – IPER

ANEXO D- TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOSFORNECEDORES E PRESTADORES DE SERVIÇOS

1. Identificação do declarante

Nome: _____
CPF: _____
Cargo/Função: _____
Setor/Lotação: _____
E-mail Institucional: _____
Telefone/Ramal: _____

2. OBJETO DO TERMO

Este Termo tem por objeto o compromisso de confidencialidade, sigilo e proteção de dados e informações acessadas pelo DECLARANTE no exercício de suas atividades no Instituto de Previdência do Estado de Roraima – IPER, incluindo:

- Dados pessoais e dados pessoais sensíveis (LGPD, art. 5º)
- Documentos internos do IPER
- Informações de segurados, dependentes, aposentados e pensionistas
- Dados previdenciários e financeiros
- Informações estratégicas, administrativas ou sigilosas
- Registros de sistemas (SEI, SISPREV, e-mail institucional, AD etc.)

3. COMPROMISSOS DO DECLARANTE

Ao assinar este termo, o DECLARANTE assume o compromisso de:

I – Manter sigilo absoluto sobre toda informação a que tiver acesso, verbal, escrita ou eletrônica.
II – Utilizar as informações exclusivamente para fins de trabalho no IPER.
III – Não copiar, transmitir, alterar ou divulgar informações sem autorização da autoridade competente.
IV – Não permitir que terceiros, internos ou externos, acessem informações sigilosas.

V – Proteger documentos, credenciais e sistemas sob sua guarda.
VI – Respeitar a LGPD, a LAI e a Política de Segurança da Informação.
VII – Reportar imediatamente vazamentos, acessos indevidos ou incidentes.
VIII – Não compartilhar senhas ou credenciais de acesso.

4. PROTEÇÃO DE DADOS (LGPD)
O DECLARANTE reconhece que:

- Dados pessoais de segurados e servidores são protegidos por lei;
- O tratamento de dados deve seguir a LGPD e normas internas;
- O uso inadequado pode resultar em responsabilização civil, administrativa e penal;
- Qualquer incidente deverá ser comunicado à GTI e ao Encarregado de Dados do IPER.

5. RESTRIÇÕES ESPECÍFICAS
É expressamente proibido:

1. Utilizar informações do IPER para fins particulares;
2. Armazenar dados institucionais em dispositivos pessoais (celular, notebook etc.);
3. Remover documentos sigilosos das dependências do IPER sem autorização;
4. Tirar fotografias de sistemas, documentos ou ambientes restritos;
5. Transferir arquivos institucionais por aplicativos não autorizados;
6. Compartilhar documentos ou informações com terceiros sem justificativa funcional.

6. VIGÊNCIA DO SIGILO

O dever de confidencialidade:
- Permanece vigente durante todo o período de atuação no IPER
- E continua mesmo após o desligamento, por tempo indeterminado

7. PENALIDADES
O descumprimento deste termo poderá resultar em:
- Processo administrativo disciplinar (LC nº 53/2001)
- Responsabilidade civil por danos

- Responsabilidade penal (arts. 153, 154 e 325 do Código Penal)
- Rescisão contratual (no caso de terceirizados)
- Comunicação à ANPD (se envolver dados pessoais)

8. DECLARAÇÃO FINAL
Declaro que:

- Li e compreendi todas as cláusulas deste termo;
- Recebi orientação sobre a Política de Segurança da Informação e a LGPD;
- Estou ciente de minhas responsabilidades e deveres legais;
- Comprometo-me a cumpri-las integralmente.

9. ASSINATURAS
Declarante:

Assinatura
Data:
Responsável pelo IPER:

Assinatura
Data:

ANEXO G-TERMO DE USO E RESPONSABILIDADE DE ACESSO A SISTEMAS (SEI, SISPREV, E-MAIL CORPORATIVO, REDE E OUTROS) INSTITUTO DE PREVIDÊNCIA DO ESTADO DE RORAIMA – IPER

1. IDENTIFICAÇÃO DO USÁRIO

Nome completo: _____
CPF: _____
Cargo/Função: _____
Setor/Lotação: _____
E-mail Institucional: _____
Telefone/Ramal: _____
Tipo de vínculo:

( ) Servidor Efetivo
( ) Comissionado
( ) Estagiário
( ) Terceirizado
( ) Consultor/Prestador

2. SISTEMAS AOS QUAIS O USUÁRIO TERÁ ACESSO

(Assinale conforme autorização da chefia e GTI)
✓ ( ) SEI – Sistema Eletrônico de Informações
✓ ( ) SISPREV – Sistema Previdenciário
✓ ( ) E-mail Corporativo
✓ ( ) Rede e Unidades Compartilhadas
✓ ( ) Ambiente de Servidores
✓ ( ) Sistema de Ponto
✓ ( ) Outros: _____

3. RESPONSABILIDADES DO USUÁRIO

Ao assinar este Termo, o usuário declara estar ciente e concordar com as seguintes responsabilidades:
I – Utilizar o acesso somente para atividades institucionais.
II – Proteger suas credenciais de acesso (login e senha).
III – Não compartilhar senha com terceiros, sob qualquer circunstância.
IV – Não permitir que terceiros realizem operações utilizando seu login.

V – Respeitar as diretrizes da Política de Segurança da Informação (PSI).
VI – Respeitar as normas da LGPD ao tratar dados pessoais.
VII – Zelar pela integridade e confidencialidade dos dados acessados.
VIII – Utilizar níveis corretos de classificação no SEI e SISPREV.
IX – Reportar imediatamente incidentes, acessos indevidos ou suspeitas.
X – Não copiar, excluir, alterar ou divulgar informações sem autorização.

4. USO DO SEI
O usuário se compromete a:

- Realizar a classificação correta dos documentos (Público, Restrito, Sigiloso);
- Não inserir informações pessoais ou sensíveis sem necessidade funcional;
- Não duplicar processos ou documentos indevidamente;
- Seguir as orientações do Arquivo e da GTI;
- Não realizar movimentações indevidas ou fora de sua competência.

5. USO DO SISPREV
O usuário reconhece que:

- O sistema contém dados pessoais e sensíveis de segurados e dependentes;
- A consulta e manipulação de dados devem ser justificadas por atividade previdenciária;
- Logs de acesso são monitorados;
- Qualquer acesso indevido poderá gerar responsabilização disciplinar e penal.

6. USO DO E-MAIL CORPORATIVO
O usuário se compromete a:

- Utilizar o e-mail apenas para fins institucionais;
- Manter postura profissional e urbanidade;
- Não utilizar e-mail pessoal para envio de documentos do IPER;
- Não enviar arquivos sigilosos sem criptografia ou autorização

- Evitar clicar em links suspeitos ou anexos duvidosos.

7. USO DA REDE E UNIDADES COMPARTILHADAS
O usuário reconhece que:

- A rede é monitorada pela GTI;
- Pastas compartilhadas devem ser utilizadas conforme perfil autorizado;
- É proibido armazenar arquivos pessoais ou não relacionados ao trabalho;
- É proibido excluir arquivos institucionais sem autorização.

8. POLÍTICA DE SENHAS
O usuário concorda com as regras:

- Senha pessoal e intransferível;
- Mínimo de 8 caracteres, com complexidade;
- Troca imediata em caso de suspeita;
- Não reutilizar senhas de outros sistemas;
- Perfis privilegiados devem usar autenticação multifator (MFA).

9. PROTEÇÃO DE DADOS (LGPD)
O usuário reconhece que:

- Dados pessoais e sensíveis acessados são protegidos pela LGPD;
- Qualquer vazamento ou incidente deve ser comunicado imediatamente;
- É proibida a cópia ou exportação de dados para dispositivos pessoais;
- O mau uso pode gerar responsabilização administrativa, civil e penal.

10. VIOLAÇÕES E PENALIDADES
O descumprimento das regras deste Termo poderá resultar em:

- Advertência ou suspensão de acesso;
- Processo administrativo disciplinar;
- Responsabilidade civil por danos causados;
- Responsabilidade penal (arts. 153, 154, 325 do Código Penal);
- Rescisão de contrato (para terceirizados).

11. VIGÊNCIA E REVOGAÇÃO
Este termo:

- Entra em vigor na data da assinatura;
- Permanece válido enquanto o usuário mantiver vínculo com o IPER;
- O acesso poderá ser revogado a qualquer momento por decisão da GTI ou Diretoria.

12. DECLARAÇÃO FINAL
Declaro que li, compreendi e concordo integralmente com as regras estabelecidas neste Termo, responsabilizando-me pelo uso adequado dos acessos institucionais sob minha guarda.

13. ASSINATURAS

Usuário:

Nome e Assinatura
Data:

IPER

Instituto de Previdência
do Estado de Roraima