POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PSI

Outubro de 2025

RIOPREVIDÊNCIA
FUNDO ÚNICO DE PREVIDÊNCIA SOCIAL DO ESTADO DO RIO DE JANEIRO

GOVERNO DO ESTADO
RIO DE JANEIRO

Fundo Único de Previdência do Estado do Rio de Janeiro

Rioprevidência

Presidente

DEIVIS MARCON ANTUNES

Chefe de Gabinete

CAMILLA DOS SANTOS COSTA MORAES

Gerente da Tecnologia da Informação e Comunicação

EDSON DELCIR MARAN

CONTROLE DE VERSÃO

#	Versão	Autor	Data	Alteração	Responsável
1	1.0	RIOPREVIDÊNCIA	05/04/2021	Criação do documento	Joaquim Leal da Silva, Robs Araújo Cipriano, Maykl Kamaroff e Inácio do Nascimento Moura
2	1.1	Every Cybersecurity and GRC Solutions	08/04/2024	Revisão do documento	Ismael Junior, Gabriel Dias, Kevin Martins, Marcos Gontijo e Pedro Baldez
3	1.2	Every Cybersecurity and GRC Solutions	25/04/2024	Ajuste no documento	Ismael Junior, Gabriel Dias, Kevin Martins, Marcos Gontijo e Pedro Baldez
4	1.3	Every Cybersecurity and GRC Solutions	29/04/2024	Revisão ortográfica do documento	Amanda Valadares e Tereza Maia
5	2.0	Every Cybersecurity and GRC Solutions	07/06/2024	Aprovação do documento	Mailton Silva
6	2.1	Every Cybersecurity GRC and Privacy Solutions	15/07/2025	Revisão e atualização do documento	Sedilaine Rocha
7	2.2	Every Cybersecurity GRC and Privacy Solutions	01/09/2025	Revisão e atualização do documento	Luciana Arruda
8	2.3	Every Cybersecurity GRC and Privacy Solutions	10/09/2025	Revisão e atualização do documento	Luciana Arruda
9	2.4	RIOPREVIDÊNCIA	29/07/2025	Revisão do anexo III	Adriana Santos
10	2.5	RIOPREVIDÊNCIA	03/09/2025	Aprovação do anexo III	Controlador
11	2.6	RIOPREVIDÊNCIA	19/09/2025	Aceite Técnico	Edson Maran, João Soares

Classificação: Público

12	2.7	RIOPREVIDÊNCIA	01/12/2025	Aprovação para publicação	Deivis Marcon Antunes

Obs.: Cópias impressas deste documento podem não corresponder à última versão aprovada e em uso. A versão mais atualizada pode ser encontrada no Portal do Rioprevidência

Classificação: Público

O Presidente do Fundo Único de Previdência Social do Estado do Rio de Janeiro (RIOPREVIDÊNCIA), no exercício das atribuições que lhe são conferidas, autoriza a presente Política de Segurança da informação - PSI, que entra em vigor na data de sua divulgação no site oficial, revogando-se todas as disposições em contrário.

CAPÍTULO I – ESCOPO E OBJETIVO

Art. 1º. Esta Política estabelece as diretrizes, competências e responsabilidades relativas à proteção da informação no âmbito do RIOPREVIDÊNCIA, com base na legislação vigente, nas normas técnicas aplicáveis e nas melhores práticas de segurança da informação e comunicações.

Art. 2º. O objetivo desta Política é assegurar a disponibilidade, integridade, confidencialidade, autenticidade e rastreabilidade das informações produzidas, recebidas, armazenadas ou transmitidas pelo RIOPREVIDÊNCIA, independentemente do meio ou formato utilizado.

Art. 3º. Esta Política aplica-se a todos os colaboradores, servidores, empregados públicos, estagiários, prestadores de serviços, fornecedores, consultores e quaisquer terceiros com acesso aos ativos de informação da autarquia.

CAPÍTULO II – CONCEITOS E DEFINIÇÕES

Art. 4º. Para os fins desta Política, aplicam-se os conceitos constantes no glossário, anexo I, em conformidade com as normas ABNT NBR ISO/IEC 27000, 27001 e 27002.

CAPÍTULO III – BASE LEGAL E NORMATIVA

Art. 5º. A presente Política foi estabelecida considerando as seguintes referências:

I. Lei nº 12.527/2011 – Lei de Acesso à Informação – LAI - Define diretrizes de transparência ativa e passiva, aplicável a todos os órgãos da administração pública.

II. Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, estabelece princípios, fundamentos e obrigações para o tratamento de dados pessoais, inclusive no setor público.

III. Lei nº 12.965/2014 – Marco Civil da Internet;

IV. Decreto nº 46.475/2018 – regulamenta o acesso às informações previstas na Constituição Federal;

V. Decreto nº 46.730/2019 – dispõe sobre a produção e tramitação eletrônica de documentos e processos administrativos na Administração Pública Estadual, e dá outras providências;

VI. Decreto nº 47.278/2020, art. 5º – atribui ao PRODERJ a competência para a Direção Geral do Sistema Estadual de Tecnologia da Informação e Comunicação – SETIC;

VII. DECRETO Nº 48.891 DE 10 DE JANEIRO DE 2024 que institui POLÍTICA DE GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DO ESTADO DO RIO DE JANEIRO

VIII. Portaria PRODERJ/PRE nº 825/2021 – institui a Política da Governança, a estratégia da governança e as normas do Plano Estratégico e Diretor de Tecnologia da Informação e Comunicação – PEDTIC, no âmbito do Poder Executivo da Administração Pública Estadual Direta e Indireta do Estado do Rio de Janeiro e dá outras providências;

IX. IN PRODERJ/PRE nº 02/2022 Regulamenta procedimentos de segurança da informação em TIC para órgãos e entidades do Executivo estadual.

X. Instrução Normativa PRODERJ/PRE nº 05/2024 – regulamenta os procedimentos para a contratação e celebração de acordos envolvendo soluções de Tecnologia da informação e Comunicação – TIC a serem observados pelos órgãos e entidades integrantes da Administração Direta e Indireta do Poder Executivo do Estado do Rio de Janeiro;

XI. Instrução Normativa PRODERJ/PRE nº 07/2025 - regulamenta os procedimentos de segurança da informação em soluções de Tecnologia da Informação e Comunicação (TIC) a serem adotados pelos órgãos e entidades integrantes da administração direta e indireta do poder executivo do Estado do Rio de Janeiro.

XII. ABNT NBR ISO/IEC 27001:2022 – especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização;

XIII. ABNT NBR ISO/IEC 27002:2022 – fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização;

XIV. ABNT NBR ISO/IEC 27701:2019 Extensão à ISO 27001 para gerenciamento da privacidade da informação (SGPI).

XV. DECRETO Nº 12.198, DE 24 DE SETEMBRO DE 2024 – Institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027 e a Infraestrutura Nacional de Dados, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

XVI. Instrução Normativa nº 1/2020, do Gabinete de Segurança Institucional da Presidência da República – que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

XVII. Instrução Normativa nº 14/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República – estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem;

CAPÍTULO IV – PRINCÍPIOS E DIRETRIZES

Art. 6º. A segurança da informação no Rioprevidência deve seguir os seguintes princípios: do acesso, da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, da privacidade, da auditabilidade e do não repúdio.

Art. 7º. Todas as informações e ativos de informação sob a guarda do RIOPREVIDÊNCIA devem ser protegidos contra acesso, uso, divulgação, modificação ou destruição não autorizados.

Art. 8º. Para os fins dispostos nesse documento, a segurança da informação abrange:

I. Segurança e Defesa Cibernética;
II. Segurança Física;
III. Proteção de dados organizacionais;
IV. Proteção de dados pessoais.

CAPÍTULO V – DIRETRIZES GERAIS

Art. 9º. A segurança da informação tem como principal diretriz a proteção dos ativos informacionais, de modo a garantir a continuidade do negócio, minimizar riscos, bem como maximizar o retorno sobre os investimentos e as oportunidades pertinentes.

Art. 10º. As diretrizes de segurança da informação consistem em considerar, prioritariamente, objetivos estratégicos, processos e requisitos legais da Rioprevidência.

Art. 11º. As diretrizes de segurança da informação descritas nesta Política deverão ser observadas por todos os colaboradores que executem atividades vinculadas ao Rioprevidência, durante todas as etapas do tratamento da informação — a saber, produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle.

Art. 12º. O cumprimento desta Política, bem como dos normativos que a complementam, poderá ser avaliado periodicamente por meio de verificações de conformidade, a serem realizadas por um grupo de trabalho formalmente instituído pelo Comitê Gestor de Tecnologia da Informação — com o objetivo de certificar o cumprimento dos requisitos de segurança da informação, bem como garantir a cláusula de responsabilidade e sigilo.

Art. 13º. O Rioprevidência deve criar, gerir, bem como avaliar critérios de tratamento da informação, de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 14º. Os contratos, convênios, acordos e instrumentos congêneres firmados pela Rioprevidência devem conter cláusulas que determinem a observância a esta Política e aos seus documentos complementares.

Art. 15º. O Rioprevidência deverá compreender ações e métodos que visem a estabelecer parâmetros adequados, relacionados à segurança e privacidade da informação, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais da organização.

CAPÍTULO VI – PAPÉIS E RESPONSABILIDADES

Art. 16º. Caberá ao Comitê Gestor de Tecnologia da Informação:

I. Assessorar na implementação das ações de segurança da informação na Rioprevidência;

II. Avaliar propostas e sugerir alterações na Política de Segurança da Informação (composta por diretrizes, normas e procedimentos relativos à segurança da informação na Rioprevidência), em conformidade com a legislação existente sobre o tema, submetendo-a à apreciação da autoridade competente;

III. Instituir Grupos de Trabalho, em caráter permanente ou temporário, para tratar de temas específicos relacionados à segurança da informação;
IV. Receber e analisar as comunicações referentes à quebra de segurança, apresentando pareceres à autoridade/órgão competente para análise e providências;
V. Apoiar a implementação de programas destinados à conscientização e à capacitação de recursos humanos em temas de segurança da informação e comunicações; e
VI. Apresentar soluções técnicas, de arquitetura e de infraestrutura, vinculadas à segurança da informação;
VII. Propor recursos necessários às ações de segurança da informação.

Art. 17º. Caberá à Gerência de Tecnologia da Informação e Comunicações (GERTIC):

I. Promover uma cultura de segurança da informação e comunicações;
II. Minutar documentos da Política de Segurança da Informação (composta por diretrizes, normas e procedimentos relativos à segurança da informação e comunicações na Rioprevidência), em conformidade com a legislação existente sobre o tema, submetendo-a à Presidência do Comitê Gestor de Tecnologia da Informação;
III. Coordenar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
IV. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança; e
V. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações.

Art. 18º. Caberá aos Gestores de Área do Rioprevidência:

I. Conscientizar, informar e incentivar os colaboradores sob sua supervisão a cumprirem as regras definidas nesta Política, atuando como um agente multiplicador;
II. Incorporar práticas de segurança e de privacidade informacionais nos processos de trabalho sob sua responsabilidade;
III. Manter (criar, alterar ou excluir) as contas de usuários sob sua responsabilidade, considerando a “necessidade de conhecer” associada à execução das respectivas atividades;

IV. Comunicar a Política de Segurança da Informação e, caso necessário, as normas complementares aos terceiros e aos fornecedores contratados — para apoiar tanto as operações quanto os processos; e

V. Incluir, nas especificações técnicas dos bens ou serviços contratados, regras que protejam a segurança e a privacidade informacionais — quando dados pessoais ou dados pessoais sensíveis estiverem envolvidos, requer-se observância às políticas, aos procedimentos internos e às diretrizes específicas sobre o tema.

Art. 19º. Caberá aos colaboradores do Rioprevidência:

I. Cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações da Rioprevidência;

II. Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

III. Assinar o Termo de Responsabilidade, formalizando a ciência e o aceite da Política de Segurança da Informação e Comunicações da Rioprevidência, bem como assumindo responsabilidade por cumpri-la;

IV. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela Rioprevidência;

V. Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Rioprevidência; e

VI. Comunicar imediatamente à GERTIC qualquer descumprimento ou violação desta Política e/ou de seus documentos complementares.

CAPÍTULO VII – DIRETRIZES DE SEGURANÇA

Art. 20º. Toda informação gerada, custodiada ou desenvolvida nas dependências do Rioprevidência, durante a execução das atividades diárias, deve ser considerada ativo de informação do órgão — sendo essenciais à condução das operações e, em última análise, à existência organizacional.

Art. 21º. Toda informação custodiada em ativos de tecnologia da informação deve possuir cópias de segurança (*backups*) guardadas em locais seguros, com controle de acesso e tempo de retenção definidos.

Art. 22º. Informações geradas, adquiridas ou custodiadas pela Rioprevidência deverão possuir classificação, a qual indique a necessidade, a prioridade e o nível esperado de proteção quanto ao respectivo tratamento.

Parágrafo primeiro – Toda informação armazenada ou mantida na organização deverá ser classificada de acordo com o seu valor, requisitos legais, sensibilidade e criticidade. Nesse sentido, é orientado que se tenha por parâmetros o Decreto nº 46.730/2019, o Decreto nº 46.475/2018 e a Lei nº 13.709/2018. Tais normativos indicam as seguintes categorias de confidencialidade: PÚBLICA, RESERVADA, SECRETA, ULTRASSECRETA ou PESSOAL. Isto posto, os gestores da informação devem assegurar que as classificações sejam revisadas periodicamente.

Parágrafo segundo – Não poderão ser incluídos no SEI-RJ documentos que possuam informações classificáveis nos níveis de sigilo estabelecidos nos art. 23 e 24 da Lei Federal nº 12.527/2011 e no art. 26 do Decreto Estadual nº 46.475/2018, a saber: ULTRASSECRETA, SECRETA e RESERVADA.

Art. 23º. Todos os servidores, terceiros e fornecedores — em qualquer vínculo, função ou nível hierárquico no Rioprevidência — são responsáveis pela segurança, pelo zelo e pelo bom uso dos ativos aos quais possuem acesso.

Parágrafo único – O Rioprevidência deverá adotar instrumentos de autodeclaração, os quais abordem a responsabilidade e o compromisso com o sigilo, bem como com a confidencialidade, tanto dos ativos quanto das informações manuseadas por todos os colaboradores.

Art. 24º. Todas as instalações e equipamentos devem ser protegidos contra acessos não autorizados. Para tanto, faz-se necessário que o Rioprevidência implemente controles de segurança capazes de impedir o acesso indevido aos ativos de informação organizacionais.

Art. 25º. Todos os colaboradores abarcados por esta Política deverão ter seus acessos (lógicos e físicos) aprovados, controlados, registrados, armazenados e adequados às necessidades inerentes ao respectivo cargo e função no Rioprevidência.

Art. 26º. As senhas são pessoais e intrasferíveis. Portanto, é vedado divulgá-las e/ou compartilhá-las com qualquer outro colaborador, seja interno ou externo — a fim de preservar os ativos de tecnologia da informação.

Parágrafo primeiro – O Rioprevidência deve adotar práticas de gerenciamento de senhas, tanto para usuários quanto para administradores. Nesse sentido, é recomendado forçar a alteração periódica

da credencial, definir um critério de complexidade, bem como impedir o uso de senhas utilizadas anteriormente.

Parágrafo segundo – O colaborador é responsável por todos os atos praticados com suas identificações — seja o seu nome na rede, seja seu carimbo, seja seu crachá, seja seu endereço de correio eletrônico, seja sua assinatura digital. Em vista disso, o colaborador responderá pela segurança dos ativos e processos sob sua responsabilidade, bem como por todos os atos executados com suas identificações, salvo se comprovado que o fato ocorreu sem o conhecimento ou consentimento.

CAPÍTULO VIII – DIRETRIZES ESPECÍFICAS

Art. 27º. Para cada diretriz considerada nas seções deste capítulo, convém observar a pertinência de se elaborarem procedimentos, normas, orientações e/ou manuais — que disciplinem ou facilitem o entendimento das orientações.

Seção I – Gestão de Ativos

Art. 28º. Todo ativo de informação do Rioprevidência deve:

I. Ser inventariado e protegido;

II. Possuir identificação formal do gestor do ativo de informação e do seu custodiante;

III. Ter as respectivas ameaças, vulnerabilidades e interdependências mapeadas.

Art. 29º. Nas dependências do Rioprevidência, tanto a entrada quanto a saída dos ativos de informação devem ser controladas, autorizadas e registadas.

Art. 30º. O Rioprevidência deve definir regras e processos para solicitação, bem como para o descarte, dos seus ativos de informação.

Art. 31º. O Rioprevidência deve implementar práticas e controles de segurança, aplicáveis à gestão remota dos seus ativos.

Art. 32º. Os ativos de informação da organização são equipados com medidas de autoproteção (ex.: antivírus, *firewalls*, criptografia e controle de acesso a configurações), sendo vedado ao colaborador desabilitá-las ou alterar suas configurações.

Art. 33º. O Rioprevidência deve implementar controles de segurança que impeçam a instalação e a utilização de *softwares* não homologados.

Art. 34º. O Rioprevidência e suas práticas de backup estão regidos pela Instrução Normativa PRODERJ/PRE n.º 03, de 28 de abril de 2022 em seu Art.13 que dispõe sobre obrigação do PRODERJ em realizar

os backups dos sistemas hospedados, devendo as responsabilidades das tarefas relacionadas aos backups, tais como a elaboração de scripts, periodicidade, execução e guarda, serem definidas de acordo com o modelo de administração de site ou portal com hospedagem no PRODERJ.

Art. 35º. O Rioprevidência poderá, no entanto, a qualquer tempo, instaurar internamente documento que orienta e dar outras tratativas acerca de práticas de Backup para fins normativos e de interesse público.

Seção II – Segurança Física e do Ambiente

Art. 36º. O acesso às instalações do Rioprevidência deverá ser controlado mediante sistemas de controle de acesso.

Art. 37º. As instalações físicas do Rioprevidência devem ser monitoradas de forma contínua — seja por sistemas de vigilância gerenciados internamente, seja por provedores de serviços de monitoramento (capazes de detectar acessos não autorizados ou comportamentos suspeitos).

Art. 38º. O Rioprevidência deverá estabelecer um perímetro de segurança, definindo os níveis necessários de segurança e proteção para cada área.

Art. 39º. Em todas as áreas de acesso restrito, o Rioprevidência deverá instalar barreiras de proteção adicional, as quais disponham de controle de acesso tanto para a entrada quanto para a saída.

Art. 40º. Todos os acessos devem ser revisados periodicamente pelo setor responsável.

Art. 41º. Tanto visitantes quanto fornecedores devem ser devidamente identificados e monitorados durante sua estadia nas instalações do Rioprevidência.

Art. 42º. A autorização de acesso às dependências deve ser encerrada ao término da visita (para acesso temporário) ou no momento de desligamento das funções (para contratados e prestadores de serviço).

Seção III – Controle de Acesso

Art. 43º. O Rioprevidência deverá definir regras de acesso aos dados e às informações. Nesse sentido, podem ser implementadas autenticações de usuários, senhas, criptografia, entre outros controles de segurança. Além disso, é prudente estabelecer restrições de acessos baseadas em níveis de autorização — garantindo, assim, a necessidade do conhecer para o cumprimento das atividades inerentes aos cargos dos colaboradores da organização.

Art. 44º. O Rioprevidência deverá criar e definir controles de segurança, a fim de garantir a exatidão dos registros de auditoria (logs) nos ativos de informação.

Art. 45º. Sempre que houver mudança nas atribuições de determinado colaborador, os seus privilégios de acesso (às informações e aos recursos computacionais) devem ser revisados de acordo com a "necessidade de conhecer" da nova função.

Parágrafo primeiro – Em caso de mudança na atribuição do colaborador, a área de tecnologia somente poderá realizar qualquer alteração de acesso após a publicação da realocação em Diário Oficial.

Art. 46º. Todos os acessos devem ser revisados periodicamente pelo setor responsável.

Art. 47º. Em caso de desligamento ou exoneração do colaborador, o gestor da área é o responsável por enviar o pedido de remoção dos respectivos acessos para a área de tecnologia.

Parágrafo único – Enquanto o pedido de revogação não for emitido para a área de tecnologia, o gestor da área poderá ser responsabilizado por qualquer ato praticado com o acesso do colaborador desligado ou exonerado.

Seção IV – Uso dos Recursos Tecnológicos

Art. 48º. Não é permitida a instalação de *softwares* não homologados nos equipamentos disponibilizados pelo Rioprevidência.

Art. 49º. O Rioprevidência deverá definir e implementar controles de segurança relacionados ao uso de dispositivos USB nos ativos de informação organizacionais.

Art. 50º. Os ativos de informação patrimoniados devem ser protegidos por trava ou por cadeado de segurança. Caso isso não seja possível, os equipamentos deverão ser guardados em local seguro com controle de acesso.

Parágrafo único – O Rioprevidência não se responsabilizará por nenhum ativo de informação não patrimoniado.

Art. 51º. Conforme **Instrução Normativa PRODERJ/PRE n.º 07, de 29 de maio de 2025** em seu **Art. 6º** "Toda informação custodiada em ativos tecnológicos nos órgãos e entidades estaduais deve possuir cópia de segurança (*backup*) e ser guardada em local protegido, para que não sejam alteradas, acessadas ou eliminadas indevidamente."

Art. 52º. Nenhum arquivo dissociado dos fins corporativos pode ser armazenado nem nos diretórios de rede, nem no próprio ativo de informação, sendo também proibido transmiti-los por e-mail ou por aplicativos de mensagens instantâneas.

Art. 53º. As informações corporativas não devem ser armazenadas localmente no computador, mas sim em local da rede corporativa destinado à sua unidade, conforme orientação do gestor correspondente.

Art. 54º. É proibido cadastrar o e-mail corporativo em sites ou aplicativos para utilização pessoal. Isto posto, o e-mail corporativo somente poderá ser utilizado em cadastros quando a finalidade estiver associada às atividades profissionais.

Art. 55º. A internet é uma concessão, devendo ser utilizada somente para fins corporativos e inerentes às atividades diárias de cada colaborador.

Art. 56º. O Rioprevidência deverá definir e implementar uma Política de Senhas, com complexidade que compreenda todas as aplicações organizacionais.

Art. 57º. O Rioprevidência deverá definir regras e diretrizes para a utilização tanto do correio eletrônico quanto das ferramentas de colaboração.

Art. 58º. O Rioprevidência tem o direito de, periodicamente, auditar os equipamentos utilizados por seus colaboradores — visando proteger e manter a integridade das informações organizacionais.

Art. 59º. Em caso de roubo ou furto de ativos da informação, o colaborador ou o terceiro deverá informar o ocorrido à área de Tecnologia, via procedimento estabelecido.

Seção V – Do Uso de Equipamentos Particulares e Dispositivos Móveis (BYOD)

Art. 60º. O Rioprevidência deverá definir regras e diretrizes quanto ao uso de equipamentos particulares, por parte de seus colaboradores, durante a execução de suas atividades diárias.

Parágrafo único – A organização deverá criar controles de segurança, a fim de garantir que equipamentos particulares tenham o mesmo nível de proteção dos equipamentos disponibilizados pelo Rioprevidência.

Art. 61º. Não é permitida a inclusão de *smartphones* na rede corporativa do Rioprevidência — o acesso desses equipamentos deverá ser restrito à rede de internet apartada.

Seção VI – Da Classificação da Informação

Art. 62º. Informações geradas, adquiridas ou custodiadas pela Rioprevidência, independentemente do formato, devem possuir classificação — para indicar a necessidade, a prioridade e o nível esperado de proteção quanto ao seu tratamento.

Art. 63º. A classificação da informação visa garantir seu tratamento adequado ao longo de todo o seu ciclo de vida, incluindo criação, tramitação, armazenamento, compartilhamento, arquivamento e descarte.

Art. 64º. O RIOPREVIDÊNCIA deverá adotar categorias de confidencialidade compatíveis com a legislação vigente, especialmente a Lei Federal nº 12.527/2011 (Lei de Acesso à Informação), o Decreto Estadual nº 46.475/2018 e a Lei nº 13.709/2018 (LGPD), a saber:

I. Informação Pública;
II. Informação Reservada (conforme Anexo I – Critérios de restrição à informação reservada);
III. Informação Secreta;
IV. Informação Ultrassecreta;
V. Informação Pessoal (nos termos da LGPD).

Art. 65º. O Rioprevidência deverá implementar um normativo específico, contendo regras e diretrizes sobre a classificação da informação na organização.

Parágrafo primeiro – A organização deverá determinar os responsáveis pela correta classificação das informações, bem como sua forma de circulação.

Parágrafo segundo – O normativo elaborado deve considerar todas as fases da informação, desde a concepção até o descarte

Seção VII – Da Segurança em Recursos Humanos

Art. 66º. O Rioprevidência deve definir, bem como implementar, controles de segurança e de privacidade da informação nos seus processos de Recursos Humanos.

Art. 67º. O Rioprevidência deve estabelecer, bem como documentar, processos permanentes de conscientização, capacitação e sensibilização em segurança e privacidade da informação.

Seção VIII – Da Gestão de Riscos

Art. 68º. O Rioprevidência deverá estabelecer regras para implementar um processo sistêmico de gerenciamento de riscos de Segurança da Informação — contemplando análise, avaliação, tratamento, aceitação e comunicação de riscos.

Parágrafo primeiro – O Gestor de Riscos de TI deve avaliar os riscos relativos à segurança dos ativos de informação, bem como a conformidade com exigências regulatórias ou legais.

Parágrafo segundo – Um documento normativo deverá ser elaborado para esse tema.

Seção IX – Da Continuidade de Negócio

Art. 69º. O Rioprevidência, mediante um processo sistêmico, deverá estabelecer regras e princípios que regulamentem a gestão da continuidade operacional. Isso fomentará uma resiliência organizacional capaz de responder efetivamente aos incidentes críticos de segurança e privacidade da informação.

Parágrafo único – Um documento normativo deverá ser elaborado para esse tema.

Seção X – Do Tratamento de Incidentes de Segurança da Informação

Art. 70º. O Rioprevidência deverá monitorar o ambiente cibernético da organização, a fim de tratar os incidentes de maneira proativa, reduzindo o tempo de resposta.

Art. 71º. O Rioprevidência deverá estabelecer regras para implementar um processo voltado à identificação e ao tratamento de incidentes de segurança da informação — contemplando as etapas de identificação, análise, avaliação, tratamento, comunicação, monitoramento, registro e relato.

Parágrafo único – Um documento normativo deverá ser elaborado para esse tema.

Art. 72º. O Rioprevidência poderá instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

Art. 73º. O RIOPREVIDÊNCIA deverá manter um processo estruturado e contínuo de monitoramento de seus ativos e ambientes tecnológicos, visando detectar, analisar, registrar e tratar proativamente incidentes de segurança da informação e de privacidade.

Art. 74º. O processo de tratamento de incidentes deve ser formalmente estabelecido, contendo, no mínimo, as seguintes etapas:

I. Identificação e categorização do incidente;
II. Análise técnica e avaliação do impacto;
III. Contenção, erradicação e recuperação;
IV. Comunicação e notificação aos atores internos e externos, quando aplicável.

V. Registro em base de dados de incidentes;

VI. Relato estruturado com causas, consequências e medidas adotadas.

VII. Adoção de lições aprendidas para prevenção de recorrência.

Parágrafo único. Deverá ser elaborado um documento normativo específico que defina os critérios de priorização, os canais de comunicação, as responsabilidades envolvidas e os fluxos de resposta.

Art. 75º. O RIOPREVIDÊNCIA poderá instituir formalmente uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR-RIOPREV), composta por servidores da área de tecnologia da informação, segurança da informação, comunicação institucional e áreas finalísticas, conforme a criticidade do incidente.

Seção XI – Da Criptografia

Art. 76º. É recomendado utilizar criptografia em serviços de rede e *web*, em redes e canais de comunicação de dados, em controles de segurança para autenticação nos sistemas, bem como em outros ambientes tecnológicos.

Art. 77º. Um processo formal deverá ser definido para proteger as chaves criptográficas corporativas. Nesse sentido, convém que os requisitos contemplem o gerenciamento ao longo de todo o ciclo de vida das credenciais (incluindo geração, armazenagem, arquivamento, recuperação, distribuição, retirada e destruição). Além disso, é prudente considerar a geração de registros e auditorias das atividades relacionadas.

Seção XII – Do Trabalho Remoto

Art. 78º. O Rioprevidência deverá criar regras que estabeleçam as formas, bem como os limites, de acessos que seus colaboradores possuirão, quando esses estiverem exercendo suas atividades de forma remota.

Art. 79º. As diretrizes desta Política também deverão ser cumpridas durante o trabalho remoto.

Art. 80º. O Rioprevidência deve implementar controles de segurança para tornar obrigatório o uso de VPN durante o trabalho remoto.

Seção XIII – Da Computação em Nuvem (*Cloud Computing*)

Art. 81º. A contratação de serviço em nuvem deverá atender aos requisitos desta Política, às normas previamente definidos pela área de tecnologia à legislação estadual, quanto à confidencialidade, propriedade, bem como localização dos dados armazenados.

Parágrafo primeiro – A empresa contratada poderá assegurar que segue padrões nacionais e internacionais de segurança em computação na nuvem.

Parágrafo segundo – O Rioprevidência deverá elaborar uma norma complementar, para uso de computação na nuvem.

Seção XIV – Mesa e Tela Limpas

Art. 82º. Documentos impressos contendo informações não públicas deverão ser armazenados, por todo colaborador, em local seguro com controle de acesso (cofre, armário, gavetas com chaves, entre outros).

Art. 83º. Os colaboradores deverão bloquear a tela do seu equipamento, sempre que se ausentarem da estação de trabalho.

Parágrafo único: O Rioprevidência poderá criar controles específicos de segurança para bloquear as telas dos ativos computacionais.

CAPÍTULO IX - DA AUDITORIA E CONFORMIDADE

Art. 84º. Todo colaborador (interno ou externo), na função de custodiante, está sujeito ao monitoramento e à auditoria das ações que realizar nos ativos integrantes do ambiente computacional da SEGOV. Tais medidas têm como objetivo detectar atividades anômalas ou não autorizadas, bem como investigar casos relacionados a incidentes, a auditorias e à ouvidoria.

Art. 85º. O Rioprevidência deverá estabelecer regras relativas à criação de um programa de auditoria para o processo de Gestão da Segurança da Informação. Essa iniciativa objetiva verificar o cumprimento dos procedimentos determinados nesta Política. Adicionalmente, visa à apuração dos controles implementados, de modo a constatar se atendem eficazmente à conformidade com os requisitos.

Art. 86º. Com base no relatório da auditoria e na análise crítica do Rioprevidência, um plano de ação poderá ser elaborado para estabelecer ações preventivas e corretivas — visando à melhoria contínua do processo de Gestão de Segurança da Informação.

Parágrafo único – Quando a auditoria de Segurança da Informação gerar resultados capazes de comprometer a segurança dos processos, a sua classificação poderá ser caracterizada como informação reservada.

CAPÍTULO X - DAS PENALIDADES

Art. 87º. Nos termos da legislação aplicável, a não observância desta Política e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicações, poderá acarretar (isolada ou cumulativamente) sanções administrativas, civis e penais — assegurados aos envolvidos o contraditório e a ampla defesa.

Parágrafo único – A aplicação das penalidades administrativas está sujeita à devida apuração em processo administrativo disciplinar, no qual serão observados os critérios de gravidade e reincidência dos atos de violação à Política de Segurança da Informação.

CAPÍTULO XI - DA VIGÊNCIA E ATUALIZAÇÃO

Art. 88º. Esta Política, bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma periódica ou sempre que se fizer necessário — não excedendo o período máximo de dois anos.

Parágrafo único – Qualquer atualização nesta Política deverá ser registrada no campo adequado do controle de versão que inicia o documento.

Anexo I: Glossário de conceitos e definições da Política de Segurança da Informação

Entende-se por:

I. **Alta Administração:** quadro diretivo do órgão, com legitimidade para representá-lo (ex.: diretores, vice-presidentes, presidentes, secretários, entre outros);
II. **Ambiente Cibernético:** inclui usuários, redes, dispositivos, *softwares,* processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes de computadores.
III. **Análise de risco:** processo por meio do qual se relacionam os eventos e respectivos impactos, bem como se avaliam as probabilidades de concretização desses cenários;
IV. **Ativo:** qualquer bem, tangível ou intangível, que tenha valor para a organização;
V. **Ativo de rede:** equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;
VI. **Ativos de Informação:** estações de trabalho, servidores, *softwares*, mídias e quaisquer equipamentos eletrônicos relacionados à tecnologia da informação e comunicação, bem como processos, pessoas e ambientes;
VII. **Autenticidade:** propriedade que assegura a fidedignidade da fonte da informação mediante processos de autenticação, os quais possibilitam confirmar a identidade de quem presta a informação;
VIII. ***Backup:*** cópia de segurança gerada com o objetivo de possibilitar o acesso ou a recuperação futura dos dados existentes;
IX. **Colaborador:** pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão da administração pública federal, formalizada por meio de assinatura de termo de responsabilidade;
X. **Computação em nuvem (*Cloud Computing*):** modelo de negócio, com escalabilidade e com mecanismos de gestão dos serviços, o qual disponibiliza (compartilha) recursos computacionais e serviços sob demanda — possibilitando configuração pelo próprio cliente, de acordo com a sua necessidade, e cobrando apenas pelo que foi consumido;
XI. **Confidencialidade:** propriedade pela qual se assegura que a informação esteja indisponível, bem como não seja revelada a pessoas, a sistemas, a órgãos ou a entidades não autorizados nem credenciados;
XII. **Conformidade:** aderência a um padrão previamente estabelecido e aceito como ideal;

XIII. **Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados para conceder ou bloquear o acesso ao uso de recursos físicos e computacionais — geralmente, requer procedimentos de autenticação;

XIV. **Controles de segurança:** medidas adotadas para evitar ou diminuir o risco de um ataque (ex.: criptografia, funções de *hash*, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão, *backups*, entre outros);

XV. **Criticidade:** nível de crise ou de impacto que podem advir da divulgação da informação ou do seu uso indevido;

XVI. **Defesa cibernética:** ações realizadas no espaço cibernético para proteger ativos de informação de interesse da Administração, bem como para obter dados úteis à produção de conhecimentos de inteligência;

XVII. **Disponibilidade:** garantia de que, quando requerido, a informação estará acessível às pessoas, aos processos automatizados, aos órgãos ou às entidades — nesse sentido, relaciona-se à prestação continuada de um serviço, sem interrupções no fornecimento de informações;

XVIII. **Dispositivos móveis:** qualquer equipamento ou acessório portátil capaz de se conectar à internet e/ou armazenar dados — incluindo *smartphones*, *tablets*, *notebooks*, *netbooks*, PDAs (*palmtops*), *pendrives,* CDs/DVDs, HDs externos e outras tecnologias semelhantes;

XIX. **Espaço cibernético:** espaço virtual composto por um conjunto de canais de comunicação da internet (entre outras redes de comunicação associadas à interconexão de dispositivos de TIC), e que engloba todas as formas de atividades digitais em rede — incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, quer humanas quer automatizadas, conduzidas nesse ambiente;

XX. **Gestão da conformidade:** conjunto de medidas que asseguram a conformidade de uma entidade às normas vigentes — ou seja, o cumprimento de todas as obrigatoriedades dos órgãos de regulamentação, obedecendo-se às políticas exigidas para a execução das atividades organizacionais;

XXI. **Gestor de Segurança da Informação:** servidor designado para coordenar e gerenciar as ações voltadas à segurança da informação no âmbito dos órgãos e entidades estaduais — com as competências previstas no art. 23 do instrumento normativo do qual este documento é anexo único;

XXII. **Incidente de Segurança da Informação:** qualquer evento adverso, confirmado ou sob suspeita, capaz de impactar a disponibilidade, a integridade, a confidencialidade ou a autenticidade de um ativo de informação, incluindo também qualquer outra violação;

XXIII. **Integridade:** é a fidedignidade da informação, a ser assegurada como garantia de que não houve modificações ou destruição não autorizadas, quer de forma acidental quer intencional;

XXIV. **Não repúdio:** propriedade de assegurar que, em um processo de envio e recebimento de informações, nenhum participante da informação (originador ou destinatário) possa, em momento posterior, negar sua respectiva atuação;

XXV. **Necessidade de Conhecer**: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade — a nomenclatura descreve a restrição de dados extremamente sigilosos, contexto em que mesmo os indivíduos com as credenciais necessárias só terão acesso à informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

XXVI. **Normas Complementares:** documentos que complementam e detalham os procedimentos e as instruções de segurança descritos nesta Política — nesse sentido, são subordinadas a este normativo e à legislação vigente;

XXVII. **Perímetro:** delimitação da área física ou lógica onde são aplicadas proteções contra acessos indevidos;

XXVIII. **Procedimentos Operacionais:** ações padronizadas a serem implementadas no âmbito dos órgãos, elaboradas baseando-se nas instruções tanto desta Política quanto do instrumento normativo ao qual está anexa, para fins de implementação de um sistema de controle, bem como de segurança, da informação e da comunicação;

XXIX. **Recursos de tecnologia da informação e comunicação:** diferentes formas de união entre *hardware* e *software*, presentes no oferecimento de aplicações ou serviços que interferem ou mediam os processos informacionais e comunicativos — ou seja, são conjuntos de bens e/ou serviços que apoiam processos de negócios mediante a conjugação de recursos, processos e técnicas empregados para obter, processar, armazenar, disseminar e utilizar informações;

XXX. **Resiliência:** capacidade de uma organização ou de uma infraestrutura de resistis aos efeitos de um incidente, ataque ou desastre, e retornar à normalidade das operações;

XXXI. **Risco:** resultado objetivo da combinação entre a probabilidade de ocorrência de um determinado evento e o impacto resultante;

XXXII. **Segurança cibernética:** conjunto de práticas para a proteção da informação armazenada nos computadores e aparelhos de computação, bem como transmitida por meio das redes de comunicação, incluindo internet e telefonia móvel;

XXXIII. **Segurança da Informação:** proteção da informação contra vários tipos de ameaças, objetivando garantir a continuidade dos processos computacionais, minimizando os riscos e maximizando a disponibilidade, integridade e confidencialidade;

XXXIV. **Segurança física:** adoção de medidas por meio de pessoas, equipamentos e procedimentos empregados com o objetivo de proteger ativos contra danos, roubos, sabotagens e outros prejuízos causados por ações humanas não autorizadas;

XXXV. **SEI-RJ (Sistema Eletrônico de Informação):** sistema oficial de autuação, produção, tramitação e consulta a documentos e a processos administrativos eletrônicos, no âmbito dos órgãos e das entidades da administração pública (tanto estadual quanto fundacional) do Estado do Rio de Janeiro, instituído pelo Decreto nº 46.730/2019;

XXXVI. **Sensibilidade:** grau de sigilo necessário à informação;

XXXVII. **Vulnerabilidade:** uma fraqueza em um ativo, ou grupo de ativos, de informação suscetível à exploração por uma ameaça (ex.: *data center* ao lado de um rio, portas destrancadas, atribuição errada de direitos de senha, falta de manutenção etc.).

Anexo II: Critérios de restrição à informação reservada

- comprometer atividades (art. 23, VIII, da Lei n° 12.527/11);
- conteúdo das propostas (art. 3º, §3º, da Lei n° 8.666/93);
- controle interno (art. 26, §3º, da Lei n° 10.180/01);
- direito autoral (art. 24, III, da Lei n° 9.610/98);
- documentos preparatórios (art. 7º, §3º, da Lei n° 12.527/11);
- informação pessoal (art. 31, da Lei n° 12.527/11);
- informação de adolescente (art. 143 e 247, da Lei n° 8.069/90 – ECA);
- informação para instruir processo arbitral (art. 27, parágrafo único, do Código de Ética);

- informação para instruir processo judicial (art. 27, parágrafo único, do Código de Ética);
- informações privilegiadas de sociedades anônimas (art. 155, §2º, da Lei nº 6.404/76);
- interceptação de comunicações telefônicas (art. 8º, caput, da Lei nº 9.296/96);
- investigação de responsabilidade de servidor (art. 150, da Lei nº 8.112/90);
- lei de mediação (art. 30, da Lei nº 13.140/15);
- livros e registros contábeis empresariais (art. 1.190, do Código Civil);
- operações bancárias (art. 1º, da Lei Complementar nº 105/2001);
- preservação da imagem (art. 12, §3º, do Decreto nº 46.336/18);
- proteção da propriedade intelectual de *software* (art. 2º, da Lei nº 9.609/98);
- proteção relativa às informações (art. 3º, XII, e art. 20, do Decreto nº 7.724/12);
- protocolo – pendente análise de restrição de acesso (art. 6º, III, da Lei nº 12.527/11);
- segredo industrial (art. 195, XIV, da Lei nº 9.279/96);
- segredo de justiça no processo civil (art. 189, do Código do Processo Civil);
- segredo de justiça no processo penal (art. 201, §6º, do Código do Processo Penal);
- segurança de instituições, autoridades e familiares (art. 23, VII, da Lei nº 12.527/11);
- sigilo bancário (art. 1º, da Lei Complementar nº 105/2001);
- sigilo das comunicações (art. 3º, V, da Lei nº 9.472/97);
- sigilo de empresa em situação falimentar (art. 169, da Lei nº 11.101/05);
- sigilo de inquérito policial (art. 20, do CPP);
- situação econômico-financeira de sujeito passivo (art. 198, caput, da Lei nº 5.172/66-CTN);
- índices de participação dos municípios – ICMS (art. 20, da Resolução SEFAZ nº 720/2014).

ANEXO III: TERMO DE RESPONSABILIDADE, CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO RIOPREVIDÊNCIA

DADOS DO USUÁRIO

- **Nome completo:**
- **Matrícula/ID Funcional:**
- **Cargo/Função:**
- **Departamento:**
- **Unidade/Agência:**
- **E-mail institucional:**

1. FINALIDADE

O presente Termo de Responsabilidade tem como finalidade estabelecer as obrigações do usuário no uso dos recursos tecnológicos, informacionais e institucionais disponibilizados pelo Fundo Único de Previdência Social do Estado do Rio de Janeiro - RIOPREVIDÊNCIA, com ênfase na segurança da informação, confidencialidade de dados, uso ético e responsável dos sistemas, e no cumprimento da legislação vigente, incluindo, mas não se limitando, à Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD).

Este termo abrange o uso de estações de trabalho, rede corporativa, internet, intranet, sistemas internos, ferramentas de comunicação institucional, e acesso a informações classificadas como sigilosas, estratégicas ou sensíveis, incluindo dados pessoais.

2. CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Declaro estar ciente e de acordo com a Política de Segurança da Informação do RIOPREVIDÊNCIA, bem como suas Diretrizes, Normas, Procedimentos e Instruções, disponíveis na Intranet – seção Política de Segurança.

Estou ciente de que todos os acessos realizados à internet e ao e-mail institucional são monitorados automaticamente[1], com o objetivo de garantir a segurança da informação e a integridade dos ativos institucionais.

Comprometo-me a utilizar os recursos tecnológicos de forma ética, responsável e exclusivamente para fins profissionais, ciente de que qualquer uso inadequado poderá resultar em sanções administrativas, civis e/ou penais.

3. USO DOS SISTEMAS E RECURSOS TECNOLÓGICOS

Declaro estar ciente de que:

a) O acesso aos sistemas é realizado por meio de credenciais individuais (login e senha), de uso pessoal, exclusivo e intransferível;

b) É proibido o compartilhamento de credenciais com terceiros, bem como o uso de credenciais de outros usuários;

c) Devo notificar imediatamente à área de Segurança da Informação qualquer situação de uso indevido, perda de senha, acesso não autorizado ou incidente de segurança;

d) É minha responsabilidade garantir o bloqueio da estação de trabalho quando estiver fora de uso e adotar boas práticas de segurança digital, como o uso de senhas seguras.

e) O uso da rede corporativa, dos sistemas institucionais e dos bancos de dados deve ser feito exclusivamente para fins profissionais, respeitando as normas internas de segurança da informação;

f) A área de trabalho física e digital deve ser mantida organizada e segura, evitando o acesso indevido a documentos, dispositivos ou informações sensíveis;

g) O acesso a bancos de dados deve ocorrer apenas quando autorizado e estritamente necessário para o desempenho das funções, sendo vedado o uso ou a divulgação não autorizada de qualquer informação obtida;

[1] Medida preventiva e necessária para proteger os sistemas, dados e informações da autarquia, conforme previsto nas normas internas e na legislação vigente

h) Toda atividade realizada nos recursos tecnológicos, incluindo acesso à internet, e-mail institucional, rede, sistemas e banco de dados, está sujeita a monitoramento com o objetivo de preservar a integridade, a confidencialidade e a disponibilidade das informações institucionais.

i) O armazenamento, transporte ou uso de arquivos institucionais fora da rede corporativa (como em dispositivos externos, pendrives, HDs externos ou serviços de nuvem não autorizados) deve ser evitado e, quando estritamente necessário, realizado somente com justificativa, autorização prévia da chefia imediata e adoção de medidas adequadas de segurança da informação, como criptografia e controle de acesso.

4. COMPROMISSO DE CONFIDENCIALIDADE E SIGILO

Comprometo-me a:

a) A não utilizar informações confidenciais às quais tiver acesso para obtenção de benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para repasse a terceiros;

b) A não realizar gravações, fotografias ou cópias de documentação, bases de dados, sistemas computacionais, informações ou outras tecnologias às quais tiver acesso, salvo mediante autorização expressa da chefia imediata;

c) A não me apropriar de material confidencial e/ou sigiloso, bem como de informações e documentos pessoais eventualmente disponíveis;

d) A não repassar ou compartilhar o conhecimento de informações obtidas, responsabilizando-me por quaisquer acessos a partir da minha intermediação, inclusive por eventuais danos ou prejuízos decorrentes da quebra de sigilo;

e) Não divulgar, por nenhum meio, informações e/ou documentos aos quais tenha tido acesso;

f) Considerar como confidenciais quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou demais materiais pertencentes ao Fundo Único de Previdência Social do Estado do Rio de Janeiro.

5. TRATAMENTO DE DADOS PESSOAIS E SENSÍVEIS

Quando o exercício de minhas funções envolver o acesso ou tratamento de dados pessoais, dados sensíveis ou informações sobre grupos vulneráveis, comprometo-me a:

a) Tratar tais dados em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), bem como demais normas internas e regulamentos aplicáveis;

b) Limitar o uso das informações estritamente à finalidade autorizada, observando os princípios de necessidade, adequação, finalidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas;

c) Não armazenar, compartilhar, transferir ou processar tais dados fora dos ambientes institucionais autorizados e protegidos, incluindo redes pessoais, dispositivos externos ou serviços de armazenamento em nuvem não homologados pela área de segurança da informação;

d) Notificar imediatamente à área de Segurança da Informação qualquer incidente de segurança, suspeita de vazamento, perda, acesso não autorizado ou uso indevido de dados pessoais ou sensíveis;

e) Zelar pela confidencialidade, integridade e disponibilidade das informações, mantendo o compromisso ético e legal mesmo após o encerramento do vínculo com o RIOPREVIDÊNCIA;

f) Atuar com responsabilidade e sigilo profissional, inclusive em situações que envolvam o descarte ou a eliminação de documentos físicos ou digitais que contenham dados pessoais.

6. MONITORAMENTO E AUDITORIA

Estou ciente de que:

a) O RIOPREVIDÊNCIA poderá monitorar acessos à rede, e-mail, sistemas e demais recursos institucionais, com a finalidade de garantir a segurança, a integridade e a conformidade das operações;

b) As informações registradas em sistemas e plataformas do RIOPREVIDÊNCIA são passíveis de auditoria e poderão ser utilizadas para fins legais e administrativos.

7. SANÇÕES PELO DESCUMPRIMENTO

O descumprimento das cláusulas deste Termo poderá acarretar:

- Aplicação de sanções administrativas e disciplinares, conforme previsto no código de ética do RIOPREVIDÊNCIA;
- Responsabilização civil e/ou penal, de acordo com a gravidade do ato e a legislação vigente, incluindo, mas não se limitando, à LGPD, sindicâncias e à Lei de Improbidade Administrativa.

8. VIGÊNCIA E DISPOSIÇÕES FINAIS

Este Termo entra em vigor na data de sua assinatura e permanecerá válido enquanto perdurar o vínculo do usuário com RIOPREVIDÊNCIA.

As obrigações de confidencialidade, sigilo e proteção das informações acessadas ou obtidas em razão desse vínculo permanecerão em pleno vigor mesmo após o seu encerramento, por prazo indeterminado, sendo o usuário integralmente responsável por qualquer uso indevido, divulgação não autorizada, vazamento ou compartilhamento de dados sigilosos.

O descumprimento das disposições deste Termo poderá sujeitar o usuário às sanções cabíveis nas esferas administrativa, civil e penal, conforme a legislação vigente, inclusive nos termos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), sem prejuízo de eventuais medidas disciplinares e ações judiciais por parte do RIOPREVIDÊNCIA.

O RIOPREVIDÊNCIA poderá atualizar suas normas internas e políticas de segurança da informação a qualquer momento, sem aviso prévio aos usuários.

Declaro, por fim, que li, compreendi e estou ciente das obrigações aqui assumidas, comprometendo-me a cumpri-las integralmente.

Assinado Digitalmente por:

www.rioprevidencia.rj.gov.br

RIOPREVIDÊNCIA

GOV RJ