3º TERMO ADITIVO AO CONTRATO Nº 2023/030.0 CELEBRADO ENTRE A CÂMARA DOS DEPUTADOS E A EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA S.A. – DATAPREV.

A CÂMARA DOS DEPUTADOS, inscrita no CNPJ/MF sob o nº 00.530.352/0001-59, estabelecida na Praça dos Três Poderes, Brasília – DF, neste ato representada por seu Diretor Administrativo, Sr. MAURO LIMEIRA MENA BARRETO, denominado CONTRATANTE, e a EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA S.A. – DATAPREV, com sede na cidade de Brasília-DF, no Setor de Autarquias Sul, Quadra 01, blocos E/F – Asa Sul, CEP: 70.070-931, inscrita no CNPJ sob o nº 42.422.253/0001-01, neste ato representada por seu Superintendente de Relacionamento Comercial e Mercados, Sr. SAULO MILHOMEM DOS SANTOS, portador da carteira de identidade nº 15573572007 GEJSPC/MA e do CPF n° 945.198.383-04 e por seu Gerente Executivo do Departamento de Relacionamento Comercial/DERC, Sr. ROGÉRIO DE ALMEIDA GOMES, portador da carteira de identidade nº 4116928 DGPC/GO e do CPF n° 956.134.551-04, doravante denominada CONTRATADA, resolvem, nos termos da legislação que aplicável a esta contratação, celebrar o presente Termo Aditivo ao Contrato nº 2023/030.0, mediante as cláusulas e condições a seguir enunciadas

CLÁUSULA PRIMEIRA – DO OBJETO

O presente Termo Aditivo tem por objeto incluir ao Contrato nº 2023/030.0 o Acordo de Níveis de Segurança, anexo a este Termo Aditivo.

CLÁUSULA SEGUNDA - DA RATIFICAÇÃO

Permanecem inalteradas as demais Cláusulas e condições estabelecidas no Contrato e que não foram modificadas, de modo expresso, por este Instrumento.

E por estarem as partes, CONTRATANTE e CONTRATADA, de pleno acordo com o disposto neste instrumento, assinam o presente Termo Aditivo para um só efeito legal.

CONTRATANTE

MAURO LIMEIRA MENA BARRETO:48427861168

Assinado de forma digital por MAURO LIMEIRA MENA BARRETO:48427861168
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=(EM BRANCO), ou=41473958000187, ou=presencial, cn=MAURO LIMEIRA MENA BARRETO:48427861168
Dados: 2025.11.06 20:08:38 -03'00'

. MAURO LIMEIRA MENA BARRETO
Diretor Administrativo

CONTRATADA

SAULO MILHOMEM DOS SANTOS:94519838304

Assinado de forma digital por SAULO MILHOMEM DOS SANTOS:94519838304
Dados: 2025.11.05 15:10:52 -03'00'

SAULO MILHOMEM DOS SANTOS
Superintendente

ROGERIO DE ALMEIDA GOMES:95613455104

Assinado de forma digital por ROGERIO DE ALMEIDA GOMES:95613455104
Dados: 2025.11.05 09:59:18 -03'00'

ROGÉRIO DE ALMEIDA GOMES
Gerente Executivo

ANEXO

ACORDO DE NÍVEIS DE SEGURANÇA

1. OBJETIVO

1.1 O presente documento visa endereçar responsabilidades para implementação do Acordo de Níveis de Segurança na relação contratual da DATAPREV com seus clientes.

1.2 As definições previstas neste documento aplicam-se a:

1.2.1 Todos os serviços de TI pertencentes ou custodiados pela DATAPREV;

1.2.2 Todos os contratos, convênios, acordos, termos e outros instrumentos congêneres celebrados pela DATAPREV.

2. DIRETRIZES

2.1 Durante toda a execução contratual as partes devem realizar ações que garantam:

2.1.1 A preservação da imagem da CONTRATANTE e da DATAPREV e de seus respectivos colaboradores;

2.1.2 A disseminação da cultura de Segurança da Informação e de Privacidade;

2.1.3 Que o nível, a complexidade e as ações de Segurança da Informação sejam adequadas ao valor dos ativos e informações, considerando os riscos a que estão expostos;

2.1.4 Que as ações de Segurança da Informação estejam alinhadas às diretrizes do Governo Federal em matéria de segurança da informação, bem como às disposições dos seguintes documentos e atos normativos:

2.1.4.1 ABNT NBR ISSO 20000-1:2020 – Sistemas de gestão de serviços – Requisitos;

2.1.4.2 Marco Civil da Internet – Lei nº 12.965, de 23 de abril de 2014 e Decreto nº 8.771, de 11 de maio de 2016;

2.1.4.3 Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, de 14 de agosto de 2018;

2.1.4.4 Estratégia Nacional de Segurança Cibernética – e-Ciber – Decreto nº 10.222, de 05 de fevereiro de 2020;

2.1.4.5 Política Nacional de Segurança da Informação – PNSI Decreto nº 9.637, de dezembro de 2018;

2.1.4.6 Norma Técnica ABNT/NBR ISO/IEC 27.001:2018 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerenciamento de Segurança da Informação – Visão Geral e Vocabulário – 5ª edição;

2.1.4.7 Norma Técnica ABNT/NBR ISO/IEC 27.002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação;

2.1.4.8 Norma Técnica ABNT/NBR ISO/IEC 27.701:2020 – Tecnologia da Informação – Técnicas de Segurança – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines;

2.1.4.9 Norma Técnica ABNT/NBR ISO/IEC 27.014:2013 – Tecnologia da Informação – Técnicas de Segurança – Governança de Segurança da Informação;

2.1.4.10 Norma Técnica ABNT NBR 16167:2013 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento da informação;

2.1.4.11 Norma Técnica ABNT NBR ISO/IEC 22301:2020 – Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos;

2.1.4.12 Lei de Acesso à Informação – Lei nº 12.527, de 18 de novembro de 2011, Decreto nº7.724, de 16 de maio de 2012 e Decreto nº 7.845, de 14 de novembro de 2012;

2.1.4.13 Marco Civil da Internet – Lei nº 12.965, de 23 de abril de 2014 e Decreto nº 8.771,de 11 de maio de 2016;

2.1.4.14 Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, de 14 de agosto de 2019;

2.1.4.15 Estratégia Nacional de Segurança Cibernética – e-Ciber – Decreto nº 10.222, de 05 de fevereiro de 2020;

2.1.4.16 Política Nacional de Segurança da Informação – PNSI Decreto nº 9.832, de 12 de junho de 2019;

2.1.4.17 Governança no compartilhamento de dados no âmbito da administração pública federal – Decreto nº 10.046, de 9 de outubro de 2019;

2.1.4.18 Instrução Normativa GSI Nº 1, atualizada em 27 de maio de 2020;

2.1.4.19 Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021;

2.1.4.20 Normas Complementares da IN Nº1 do GSI, DSIC/GSI/PR nº 4 a n° 21;

2.1.4.21 Portaria GSI/PR nº 93, de 18 de outubro de 2021 – Glossário de Segurança da Informação;

2.1.4.22 Código de Conduta Ética e Integridade vigente;

2.1.4.23 Política de Continuidade de Negócios da DATAPREV vigente;

2.1.4.24 Política de Gestão de Riscos e Controles Internos vigente;

2.1.4.25 Política de Integridade Corporativa da DATAPREV vigente;

2.1.4.26 Política de Divulgação de informações da DATAPREV vigente;

2.1.4.27 Política Anticorrupção vigente;

2.1.4.28 Política de Porta-Vozes vigente;

2.1.4.29 Norma Técnica ABNT NBR ISO/IEC 27000 – Tecnologia da Informação – Técnicas de Segurança;

2.1.4.30 Norma Técnica ABNT/NBR ISO/IEC 27.001:2018 – Tecnologia da Informação –

Técnicas de Segurança – Sistemas de Gerenciamento de Segurança da Informação – Visão Geral e Vocabulário – 5ª edição;

2.1.4.31 Norma Técnica ABNT/NBR ISO/IEC 27.002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação;

2.1.4.32 Norma Técnica ABNT/NBR ISO/IEC 27.701:2020 – Tecnologia da Informação – Técnicas de Segurança – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines;

2.1.4.33 Norma Técnica ABNT/NBR ISO/IEC 27.014:2013 – Tecnologia da Informação – Técnicas de Segurança – Governança de Segurança da Informação;

2.1.4.34 Norma Técnica ABNT NBR 16167:2013 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento da informação;

2.1.4.35 Norma Técnica ABNT NBR ISO/IEC 22301:2020 – Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos.

2.1.5 Que a Segurança da Informação esteja efetivamente incorporada, desde a concepção e por todo ciclo de vida, em todos os processos executados no âmbito do contrato.

3. DO CONTROLE DE ACESSO AOS DADOS

3.1 A gestão de acesso utiliza processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais e privilégios para contas de usuário, de administrador e de serviços de ativos da informação. Assim, os processos de concessão e revogação de acessos devem ser criticamente analisados e validados periodicamente.

3.2 Os controles de acesso aos serviços e dados devem ser estabelecidos pela DATAPREV.

3.3 O controle de acesso para serviços de TI legados ou serviços de TI gerenciais deve observar as seguintes condições:

3.3.1 O acesso dos usuários, quando suportado pelo sistema, deve ser realizado via VPN (Virtual Private Network – Rede Privada Virtual) e Certificado Digital A3.

3.3.2 A autenticação multifator (MFA), quando suportada pelo sistema, deve ser utilizada no processo de autenticação do acesso remoto.

3.3.3 É responsabilidade da CONTRATANTE comunicar à DATAPREV a relação de servidores "Autorizadores" que possuem permissão para solicitar o cadastramento, renovação e interrupção de acesso VPN para "Usuários Solicitantes" vinculados ao órgão, após o preenchimento e assinatura de "Termo de Responsabilidade e Compromisso".

3.3.4 A CONTRATANTE deve solicitar a interrupção imediata do acesso VPN do usuário desligado por qualquer motivo.

3.3.4.1 Nas Nas evoluções sistêmicas, deverão ser priorizados ajustes que possibilitem a implantação de acesso via VPN e Certificado Digital A3, bem como a utilização de autenticação multifator (MFA).

3.4 O controle de acesso para serviços de TI transacionais deve observar as seguintes condições:

3.4.1 O acesso dos usuários, quando suportado pelo sistema, deve ser realizado via GERID (Gerenciador de acessos) e Certificado Digital A3.

3.4.2 Na concessão de acesso a servidores, empregados, estagiários ou terceirizados devem ser observados os princípio da necessidade de conhecer e do privilégio mínimo, ou seja, o usuário deverá ter acesso apenas aos ativos e informações essenciais para a execução de suas atribuições.

3.4.3 O perfil de administrador deve ser exclusivo para usuários responsáveis pela execução de tarefas específicas na administração de ativos de informação.

3.4.3.1 Excepcionalmente, o privilégio de administrador nos equipamentos locais pode ser fornecido, em caráter provisório.

3.4.4 A CONTRATANTE deve solicitar a interrupção imediata do acesso a serviços de TI transacionais por usuários ou administradores desligados de suas funções por qualquer motivo, devendo o processo de revogação de acesso ser igualmente realizado de imediato.

3.4.4.1 Compete ao CONTRATANTE a comunicação imediata sobre desligamentos, férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

4. DA PREVENÇÃO DE INCIDENTES

4.1 A DATAPREV deve adotar todas as medidas necessárias para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações a serem tratadas nos sistemas disponibilizados.

4.2 A CONTRATANTE deve abster-se de replicar ou realizar cópias de segurança (backups de dados) fora de ambientes seguros e certificados.

4.3 A CONTRATANTE deve comunicar imediatamente a detecção de eventos de segurança que impactem na operação dos sistemas ou comprometimento de dados e preservar as evidências para as devidas apurações.

4.4 A utilização de robôs nos serviços de TI está condicionada ao alinhamento prévio das partes.

4.4.1 A utilização de robôs em desconformidade com a cláusula 4.4 acarretará a desconsideração do Acordo de Nível de Serviço (ANS) contratado para o respectivo serviço para efeitos de glosa e sanções administrativas.