Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

METRUS
INSTITUTO DE SEGURIDADE SOCIAL
Al. Santos, 1827 - 17º andar | Cerqueira César | CEP 01419-909 | São Paulo - SP - Brasil
Tel.: (11) 3371-3439 | Central de Relacionamento: 0800 016 05 98 | www.metrus.org.br
CNPJ nº 44.857.357/0001-66 | Inscrição Estadual: Isento

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

1. Introdução

A Lei 13.709/2018 – Lei Geral de Proteção de Dados - LGPD regula o tratamento de dados pessoais, nos meios digitais ou físicos, realizado por pessoas naturais ou jurídicas, de direito público ou privado, visando proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da pessoa natural.

Esta norma, em aderência à LGPD, dispõe sobre os preceitos básicos da lei e as regras que devem ser observadas em todas as atividades que envolvam a coleta, o acesso ou o tratamento de dados pessoais de participantes, assistidos, beneficiários, colaboradores, diretores, conselheiros, prepostos da entidade, bem como de quaisquer outras pessoas físicas cujos dados se tornem acessíveis em razão das atividades realizadas.

2. Objetivo

Orientar os colaboradores à prática de proteção dos dados pessoais acessíveis no âmbito das operações do Metrus, assegurando que sejam sempre tratados em observância aos princípios da boa-fé, finalidade, adequação e necessidade, bem como livre acesso, segurança, prevenção e não discriminação, de modo a preservar a transparência ao titular dos dados sobre o tratamento de seus dados pessoais, à luz da LGPD e das melhores práticas de governança e mitigação de riscos.

3. Abrangência

Esta norma aplica-se à todas as áreas do Instituto e deve ser observada por todos aqueles que atuem em nome do Metrus nas atividades e funções que envolvam os dados pessoais.

DS GDSG DS DDCP DS JV DS ALG

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

4. Regras

4.1 Tratamento de dados pessoais

Todo e qualquer tratamento de dados pessoais realizado no Metrus, ou a pedido do mesmo, deve observar a Política de Proteção e Governança de Dados Pessoais, bem como os princípios de tratamento e as bases legais previstas, respectivamente, nos arts. 6º, 7º e 11 da LGPD.

Na ocorrência de tratamento com base em legítimo interesse, são requisitos indispensáveis:

- A proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais;

- A utilização dos dados pessoais estritamente necessários para o atendimento à finalidade pretendida;

- Adoção das medidas para garantir, ao titular, a transparência do referido tratamento de dados, como inclusão de cláusulas contratuais e obtenção de consentimentos e autorizações.

4.2 Coleta de dados pessoais

A coleta de dados pessoais deve ser destinada a atender propósitos específicos e legítimos, observada limitação aos dados pessoais mínimos necessários para atendimento às respectivas finalidades, de modo a assegurar que:

- O titular dos dados pessoais deve ser informado através de Aviso de Privacidade, por contrato, por e-mail ou pessoalmente, de maneira clara e específica sobre como seus dados serão tratados e para quais finalidades;

- O tratamento é adequado e seguro ao contexto em que os dados pessoais foram coletados; e

- Há indispensabilidade dos dados pessoais coletados para atingir àquela finalidade pretendida.

DS GDSG DS DDCP DS JV DS alg

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

4.3 Coleta de dados pessoais de crianças e adolescentes

Na coleta de dados de crianças e adolescentes, inclusive beneficiários dos planos de benefícios e de saúde e dependentes de colaboradores e diretores do Metrus, as áreas do Metrus devem adotar procedimentos para certificar que a coleta de dados e o consentimento para o tratamento de dados é realizado diretamente pelos pais ou responsáveis legais.

Observada a legislação que rege as operações de previdência e de saúde e as informações necessárias para operacionalização do escopo dos contratos firmados com o Metrus, dados pessoais de participantes e/ou beneficiários menores de 18 (dezoito) anos não poderão ser disponibilizados a terceiros.

4.4 Compartilhamento de dados pessoais

O compartilhamento de dados pessoais do Metrus é classificado em três níveis: amplo, restrito e específico, de acordo com a categoria e a confidencialidade dos dados, bem como o enquadramento do tratamento realizado.

O compartilhamento de dados deve ocorrer com base na Política de Proteção e Governança de Dados Pessoais, devendo, o receptor dos dados, garantir o adequado tratamento e segurança dos dados pessoais recepcionados.

O compartilhamento de dados pessoais pelo Metrus deve ocorrer apenas quando se fundamentar a partir de uma das bases legais previstas no art. 7º ou art. 11 da LGPD.

Os contratos e convênios com terceiros, para os quais haja o compartilhamento de dados pessoais, devem conter cláusulas específicas dispondo sobre a observância à proteção e governança de dados pessoais e medidas de minimização de riscos.

4.5 Compartilhamento de dados sensíveis

O compartilhamento de dados pessoais sensíveis é permitido nas seguintes hipóteses, com a devida observância às disposições do item 4.4 desta norma:

- Para possibilitar, ao seu beneficiário e seus dependentes, a prestação de serviços assistência à saúde, nos termos contratados;

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

- Portabilidade de dados quando solicitado pelo titular;

- A realização de transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde e assistência à saúde;

- Quando devidamente autorizado pelo titular.

4.6 Compartilhamento de dados com a administração pública

Nos casos em que houver o recebimento de informações constantes em bases de dados controlados pela Administração Pública, os integrantes do Metrus deverão se assegurar, além do atendimento das finalidades e princípios compatíveis com as atividades realizadas, que:

- Se trate de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei de Acesso à Informação (Lei nº 12.527/2011);

- Nos casos em que os dados forem acessíveis publicamente;

- Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;

- Na hipótese de a transferência dos dados objetivar exclusivamente para a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Ainda, na ocorrência de tais casos, a entidade deverá realizar comunicação à Autoridade Nacional de Proteção de Dados conforme item 4.9 desta norma.

4.7 Transferência internacional

Nos casos em que se fizer necessária a realização de transferência internacional de dados pessoais, é cabível conferir previamente a existência, no país de destino, de norma ou dever de proteção de dados pessoais, em observância ao fiel cumprimento das disposições e requisitos estabelecidos neste Normativo, bem como na regulação específica prevista pela ANPD.

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

4.8 Eliminação de dados pessoais

O tratamento e armazenamento de dados pessoais somente estão autorizados pelo período necessário à realização das finalidades que motivaram a coleta e tratamento de tais dados, bem como para cumprimento de obrigações contratuais e legais, observada a sua indisponibilidade, quando do término do tratamento, em sistemas, redes ou pastas físicas do Metrus.

Os dados pessoais e ou dados pessoais sensíveis tratados pela entidade devem ser mantidos enquanto existir relação jurídica com o respectivo titular, exceto nos casos em que, por observância a legislação ou regulamentação, seja necessária a conservação por prazo superior, findo o qual os dados pessoais serão eliminados.

A eliminação de documentos contendo dados pessoais deverá seguir o procedimento especificado na tabela de temporalidade do Metrus.

Havendo determinação por parte de autoridade pública ou judicial para a manutenção de informações relacionadas às pessoas físicas, o Metrus deverá atender ao mandamento, procedendo com a exclusão de forma segura, após passado o período determinado.

4.9 *Encarregado de Dados Pessoais - Data Protection Officer* - DPO

O Encarregado de Dados Pessoais – *Data Protection Officer* (DPO) indicado como responsável pelo canal de comunicação entre o Metrus, os titulares de dados pessoais (participantes, assistidos, beneficiários, colaboradores, fornecedores, dirigentes e prepostos), partes interessadas e a ANPD, deve prestar os esclarecimentos necessários sobre este Normativo e sua aplicação, casos excepcionais e boas práticas a serem adotadas permanentemente por colaboradores, diretores, conselheiros, fornecedores e parceiros do Metrus.

Eventuais violações ao tratamento de dados pessoais, bem como às normas da LGPD deverão ser reportados ao DPO imediatamente.

4.10 Direitos dos titulares e canal de gerenciamento de solicitações

É assegurado o acesso facilitado e claro às informações sobre o tratamento de dados pessoais realizados pelo Metrus, sempre que solicitado pelo titular dos dados.

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

As solicitações relativas aos direitos de privacidade e proteção de dados dos titulares deverão ser efetuadas e encaminhadas ao canal de gerenciamento de solicitações, conduzido pelo DPO.

Devem ser adotados procedimentos de identificação e autenticação das solicitações realizadas, atendendo somente após confirmada a identidade do titular, ainda que se necessário a solicitação de documentos adicionais para tal atendimento.

4.11 Comitê de Riscos e Controles

O Comitê de Riscos e Controles do Metrus é composto pelo Diretor Presidente como coordenador do Comitê, pelo responsável pela área de Riscos e Controles Internos, como vice-coordenador, e pelos responsáveis das áreas de Previdência, Técnica de Saúde, Investimentos, Comunicação e Relacionamento, Conformidade e Jurídico, Tecnologia, e como membros convidados o responsável pela área de Controladoria e Encarregado de Dados Pessoais (DPO).

O Comitê terá o papel de deliberar sobre as diretrizes e regras para o tratamento de dados no Metrus, auxiliar o DPO no desempenho de suas funções, e promover a conscientização interna sobre os procedimentos envolvendo dados pessoais e segurança da informação.

4.12 Comunicação de Incidente de Segurança

Nos casos em que for identificado incidente de violação a tratamento de dados pessoais, classificado como risco relevante, é responsabilidade do Encarregado de Dados Pessoais (DPO) o reporte à Autoridade Nacional de Proteção de Dados (ANDP), no prazo de até 03 dias, utilizando o Formulário de Comunicação de Incidente de Segurança – Anexo 1, relatando o incidente e os mecanismos de mitigação de risco adotados.

A Coordenadoria de Riscos e Controles deve realizar monitoramento do compartilhamento externo dos dados pessoais, realizado por meio de sistema e encaminhar relatório trimestral aos gestores para conhecimento e análise.

DS GDSG DS DDCP DS JV DS alg

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

4.13 *Privacy by design*

A todo projeto ou operação desenvolvido pela ou sob demanda do Metrus devem ser incorporados os conceitos e práticas de *privacy by design* (privacidade desde a concepção), para garantia da governança e proteção dos dados pessoais do usuário.

4.14 Programa de Privacidade de Dados Pessoais

A Coordenadoria de Riscos e Controles deve promover o Programa de Privacidade de Dados Pessoais, que possui quatro pilares que são: (i) a adequação dos documentos e formulários do Instituto à LGPD; (ii) a participação do DPO no Comitê de Riscos e Controles; (iii) o monitoramento das práticas de LGPD por meio de testes de efetividade; e (iv) treinamento e conscientização dos colaboradores do Metrus em relação aos fundamentos da LGPD.

5. Considerações Finais

5.1 Boas práticas para governança e proteção de dados pessoais

Além da observância aos preceitos e regras contidas neste Normativo, deverão ser adotadas medidas de boas práticas que assegurem a proteção e a governança de dados pessoais, inclusive para que:

- As solicitações de áreas internas, fornecedores e parceiros sejam atendidos, sempre que possível, sem a identificação dos titulares de dados pessoais ou mediante pseudonimização;
- Dados pessoais não sejam expostos em reuniões de comissões, comitês e grupos de trabalho;
- Os dados pessoais sensíveis relativos à saúde dos beneficiários (titulares e dependentes) sejam acessíveis tão somente aos colaboradores que atuem em atividades que envolvam diretamente o tratamento de tais dados;
- Os titulares de dados pessoais não sejam identificados em reuniões dos Conselhos Deliberativo e Fiscal quando não for essencial à análise dos assuntos sob debate ou deliberação de tais órgãos de governança, mantida a pseudonimização;
- Arquivos contendo dados pessoais não sejam impressos, exceto quando imprescindível para assinatura ou outra providência que não possa ser realizada sem que haja impressão dos dados pessoais – hipótese em que os papéis devem ser destruídos após o seu tratamento ou atingimento de finalidade, na forma prevista neste Normativo;
- Papéis, arquivos, dossiês e pastas físicos contendo dados pessoais sejam guardados com segurança e não sejam reutilizados, ainda que para rascunho;

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

- Haja o registro das operações de tratamento de dados pessoais e dados pessoais sensíveis realizadas pelos operadores de dados pessoais (fornecedores) em seu nome;
- Sejam utilizados mecanismos para assegurar que o contato telefônico está sendo realizado diretamente com o titular de dados ou seu representante legal e que os endereços eletrônicos utilizados para troca de informações não sejam e-mails de terceiros;
- Sejam solicitados apenas os dados pessoais e documentos comprobatórios mínimos para a realização da operação em andamento, inclusive para fins de realização de novas adesões e prospecções;
- Não haja a disponibilização de dados pessoais para terceiros, ainda que pais ou familiares.

6. Definições

DADO PESSOAL: informação que, isolada ou associada a outras, identifique ou que possa identificar uma pessoa natural;

DADO PESSOAL SENSÍVEL: informação sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

DADO PSEUDONIMIZADO: informação sobre um titular de dados que somente o identifica quando associada a informação adicional relativa ao titular, mantida separadamente pelo controlador em ambiente controlado e seguro;

DADO ANONIMIZADO: trata-se de remoção ou substituição de informações identificáveis como nomes, números de identificação etc por outros códigos aleatórios visando tornar impossível a identificação direta ao qual os dados se referem.

TITULAR DE DADOS PESSOAIS: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, inclusive participantes, assistidos, beneficiários, colaboradores, conselheiros, diretores, fornecedores – quando pessoas físicas - e demais prepostos da entidade;

TRATAMENTO DE DADOS PESSOAIS: operação realizada com dados pessoais, que abarca a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados pessoais;

AGENTES DE TRATAMENTO DE DADOS: controlador, pessoa natural ou jurídica, de direito público ou privado, a quem compete a tomada de decisões referentes ao tratamento de dados pessoais, e o operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome ou a pedido do controlador;

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

INSTRUMENTOS CONGÊNERES: Instrumento Jurídico elaborado para parcerias e convênios.

DATA PROTECTION OFFICER - DPO (Encarregado de Dados Pessoais): pessoa indicada pelo controlador ou operador encarregado para atuar como canal de comunicação com titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD);

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANDP): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

7. Documentação de Referência

Nome do documento	Código	Armazenamento
Lei Geral de Proteção de Dados Pessoais Nº13.709 de 14 de Agosto de 2018.	Lei 13.709/2018	www.planalto.gov.br
Lei de Acesso a Informação Nº12.527 de 18 de novembro de 2011.	Lei 12.527/2011	www.planalto.gov.br
Política de Proteção e Governança de Dados Pessoais	POL-CRC-003	Site e Intranet do Metrus
Resoluções CD/ANPD Nº 15 de 24 de abril de 2024.	CD/ANPD Nº 15/2024	www.gov.br
Resolução CD/ANPDNº 18 de 16 de julho de 2024.	CD/ANPD Nº 16/2024	www.gov.br
Resolução CD/ANPDNº 19 de 23 de agosto de 2024.	CD/ANPD Nº 19/2024	www.gov.br

8. Anexo

Anexo 1 – Formulário de Comunicação de Incidente de Segurança.

DS GDSG DS DDCP DS JV DS alg

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

METRUS
INSTITUTO DE SEGURIDADE SOCIAL
Al. Santos, 1827 - 17º andar | Cerqueira César | CEP 01419-909 | São Paulo - SP - Brasil
Tel.: (11) 3371-3439 | Central de Relacionamento: 0800 016 05 98 | www.metrus.org.br
CNPJ nº 44.857.357/0001-66 | Inscrição Estadual: Isento

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

9. Histórico do Documento

Versão nº	Descrição	Responsável	Assinatura	Data
Inicial	Emissão	Coordenadora de Riscos e Controles Internos	-	12/02/2021
01	Alterações: • *Adequação dos membros do Comitê de Riscos e Controles no item 4.11;* • *Inclusão do monitoramento referente ao compartilhamento dos dados pessoais pela CRC no item 4.12;* • *Inclusão do Item 4.14 – Programa de Privacidade de Dados Pessoais;* • *Inclusão da definição de Dado Anonimizado no item 6;e* • *Inclusão de novas resoluções CD/ANPD no item 7.*	Revisão: Coordenadora de Riscos e Controles Internos	DocuSigned by: Gisleine de Souza Garbo 8D1A7695A757476...	25/09/2024
		Análise Preliminar: Analista de Conformidade Sr.	DocuSigned by: Denise da Conceição Pereira 1D52E9FFEE9A4C3...	
		Aprovação Inicial: Coordenadora Jurídica e de Conformidade	DocuSigned by: Juliana Grasiela Vicentin 53E682E43B0847C...	
		Aprovação do documento: Diretora Presidente	DocuSigned by: Alexandra Leonello Granado 5A4539034CB2465...	

Docusign Envelope ID: 6FE97939-4472-462A-8CB2-E6CA11077817

METRUS
INSTITUTO DE SEGURIDADE SOCIAL
Al. Santos, 1827 - 17º andar | Cerqueira César | CEP 01419-909 | São Paulo - SP - Brasil
Tel.: (11) 3371-3439 | Central de Relacionamento: 0800 016 05 98 | www.metrus.org.br
CNPJ nº 44.857.357/0001-66 | Inscrição Estadual: Isento

Instrumento Normativo			
Tipo: **Norma**	**Nome:** **Proteção e Governança de Dados Pessoais**		**Código:** NOR-CRC-001
Área : **CRC – Coordenadoria de Riscos e Controles**	**Vigência:** A partir da data de aprovação	**Validade:** 3 anos	**Versão:** 01

ANEXO 1 – Formulário de Comunicação de Incidente de Segurança

FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

INFORMAÇÕES DE CONTATO

Nome do Colaborador	
Área de Atuação	
Nº de Contato	
E-mail	

DETALHES DO INCIDENTE

Data e horário	
Local	
Breve descrição de como foi identificado	
Tipos de informações envolvidas (Descrever se o incidente envolve dados de participantes, assistidos, beneficiários, empregados, dentre outros e quais dados identificados até o momento)	
Suportes afetados pelo incidente (Sistemas)	
Estimativa de pessoas afetadas pelo incidente	
Havia alguma medida de segurança protegendo os dados pessoais? (Descrever se o objeto do incidente estava protegido por senha, criptografia ou anonimização, dentre outras possibilidades)	
Há algum parceiro (Fornecedor) envolvido?	
É de seu conhecimento se o incidente foi contido?	

Data	
Assinatura do colaborador	

PARA PREENCHIMENTO PELO ENCARREGADO DE DADOS (DPO)

Descrição do incidente	
Análise de risco	
Medidas adotadas	
Justificativa sobre as Medidas adotadas	
Necessidade de Melhorias identificadas	

Data	
Assinatura do Encarregado de Dados (DPO)	

Confidencial – compartilhamento restrito

DS GDSG DS DDCP DS JV DS ALG