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: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

1. Objetivo

1.1 A presente Política tem como objetivo dispor os pilares, atribuições e procedimentos voltados a garantir a segurança da informação no âmbito das atividades desenvolvidas pelo Metrus.

2. Abrangência

2.1 Esta Política aplica-se a todos os colaboradores, temporários, diretores, conselheiros, consultores, prestadores de serviços e demais contratados do Metrus, no desempenho de suas respectivas atividades.

3. Diretrizes

3.1 Princípios da Segurança da Informação

Na gestão corporativa do Metrus as informações são tratadas como verdadeiros ativos. Diante disto, o usuário da informação deve tratá-las, em todo o seu ciclo de vida (produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte), de modo ético e responsável, aplicando o tratamento adequado ao nível de classificação da informação, bem como zelar pela preservação dos seguintes princípios e pilares:

a. Confidencialidade: somente pessoas autorizadas possuam acesso às informações;

b. Disponibilidade: assegurar o funcionamento e a utilização plena de sistemas e ativos para as pessoas autorizadas;

c. Integridade e exatidão das informações: sem modificações de caráter não autorizado, durante toda a cadeia de processamento;

d. Autenticidade: identificação da informação e do usuário de ativos;

e. Respeito à Privacidade e Proteção de Dados, da inviolabilidade da intimidade, da autodeterminação informativa; da liberdade de expressão e de informação, de comunicação e de opinião; da honra e da imagem; do desenvolvimento econômico, tecnológico e da inovação, em alinhamento estratégico e operacional com a "Política de Proteção e Governança de Dados Pessoais" e com a "Política de Gestão de Riscos";

f. Conformidade à legislação brasileira e demais instrumentos normativos relacionados à segurança da informação e à proteção de dados pessoais.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

3.2 Do tratamento da segurança da informação pelo Metrus

Toda informação gerada, custodiada, manipulada, utilizada ou armazenada, em formato digital ou físico, e seus suportes (sistemas, rede, arquivo, depósitos) será classificada e organizada, a fim de garantir a disponibilidade e confidencialidade das informações.

Independentemente da forma apresentada, compartilhada ou armazenada, os ativos de informação devem ser utilizados apenas para a sua finalidade devidamente autorizada.

As informações devem ter classificação de segurança e medidas de proteção aplicáveis de acordo com critérios estabelecidos quando da sua criação, utilização, custódia e descarte, bem como com o nível de confidencialidade e criticidade para gestão da segurança.

Para assegurar a proteção adequada das informações tratadas pelo Metrus, todos os dados criados internamente ou recebidos de fontes externas devem ser classificados conforme seu grau de sensibilidade e o potencial impacto decorrente de seu acesso, uso ou divulgação não autorizados.

A classificação da informação deve seguir os seguintes níveis:

- **Confidencial:** Abrange dados altamente sensíveis cujo acesso deve ser restrito. O vazamento pode causar prejuízos financeiros, legais ou reputacionais ao Metrus.

Exemplos: estratégias de negócio, assuntos de reuniões dos conselhos, dados financeiros não divulgados e contratos sigilosos.

O acesso é restrito a colaboradores, fornecedores e prestadores de serviço previamente autorizados.

Deve haver contrato vigente e assinatura de Termo de Responsabilidade para o tratamento dessas informações.

- **Interna:** Inclui informações destinadas exclusivamente ao uso interno do Metrus, que, embora não sejam críticas, não devem ser divulgadas ao público externo. São dados utilizados no desempenho das atividades institucionais e operacionais da Entidade.

O acesso é permitido a todos os colaboradores, fornecedores e prestadores de serviço do Instituto, desde que no exercício de suas funções.

Não requer medidas de segurança tão rigorosas quanto aquelas aplicáveis as informações confidenciais. No entanto, deve ser protegida contra divulgação indevida. Caso seja necessária sua divulgação, esta deverá ser previamente autorizada pela Coordenadoria de Tecnologia da Informação e Coordenadoria Jurídica e de Conformidade.

- **Pública:** Dados que podem ser livremente divulgados ao público sem causar prejuízo ao Metrus ou às partes envolvidas.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

Exemplos: Conteúdo institucional do site do Metrus, comunicados de imprensa, relatórios anuais e materiais de marketing e campanhas.

As diretrizes estabelecidas nesta política visam o incentivo à implementação de uma cultura de proteção de dados no Metrus.

3.3 Da Propriedade Intelectual

Os recursos utilizados/produzidos pelos usuários, como os "*designs*", criações ou procedimentos desenvolvidos pelos colaboradores, bem como toda e qualquer informação sob a guarda do Metrus, independentemente da origem (se coletada diretamente ou obtida através de terceiros) são consideradas de propriedade intelectual do Instituto. Portanto, tais informações não podem ser interpretadas como de uso pessoal, devendo o usuário utilizá-la única e exclusivamente para as finalidades constantes do contrato de trabalho.

Neste sentido, os equipamentos, meios de comunicação e sistemas estão sujeitos a monitoramento, sendo certo que eventuais informações de cunho pessoal tratadas por esses meios serão abrangidas por referido controle, pela sua indissociabilidade.

3.4 Da Concessão de Acessos

A concessão de acessos se subdivide nas seguintes categorias:

Concessão ou Revogação de acesso à rede de dados do Metrus, deverá ser formalizado através de e-mail enviado pela Coordenadoria de Gestão de Pessoas - CPA, conforme instrumento normativo "Norma de Acesso à Rede Interna de Dados".

Concessão ou Revogação de acesso Remoto à rede de dados do Metrus ocorre paralelamente à Concessão ou Revogação de acesso solicitada pela Coordenadoria de Gestão de Pessoas - CPA conforme instrumento normativo "Norma de Acesso Remoto à Rede de Dados".

Concessão ou Revogação de acesso à rede sem fio (wi-fi) deverá ser formalizada através da abertura via sistema de chamado e seguirá os critérios previstos no instrumento normativo "Norma de Acesso à Rede Sem Fio".

Concessão de acesso às imagens do CFTV (Circuito Fechado de TV) do Metrus deverá ser formalizada conforme critérios previstos no "Manual de Delegação de Autoridade - MDA".

Revisão de acesso ocorrerá anualmente mediante critérios previstos no instrumento normativo próprio.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

3.5 Da Rastreabilidade

A Coordenadoria de Tecnologia da Informação - CTI mantém controle de rastreabilidade, como logs e trilhas de auditoria, mantendo registro dos acessos e modificações realizadas em arquivos e sistemas utilizados.

- **Login de acesso**: log de acessos à rede ficam registrados no servidor e ficam disponíveis por 1 dia.
- **Arquivos da rede:** log de gravação de arquivos ficam registrados no servidor e disponíveis por 1 dia.
- **Base dados previdência**: log das principais tabelas inerentes ao negócio ficam armazenadas para pronta busca por 90 dias. Período maior fica armazenado em fita de backup solicitada sob demanda.
- **Base dados saúde**: log alteração das tabelas ficam armazenados por tempo indeterminado enquanto o contrato com fornecedor do sistema estiver em vigor.

Os logs e registros conforme descrição acima de temporalidade, são armazenados e preservados em ambiente seguro, a fim de preservar a cadeia de custódia dos dados mantidos pelo Metrus.

3.6 Da Segurança Cibernética

A Coordenadoria de Tecnologia da Informação - CTI avalia, monitora e implementa melhorias aos riscos associados às informações que mantém sob sua guarda, como objetivo de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Também são avaliados previamente os riscos e os impactos na segurança da informação no desenvolvimento de novos produtos ou reformulação de processos, bem como na contratação de fornecedores quando com estes houver a troca de informações.

3.7 Do Plano de Continuidade de Negócios (PCN)

O Metrus mantém plano de contingência, visando a garantia absoluta da disponibilidade das informações e a continuidade do negócio, inclusive na ocorrência de incidentes ou ameaças à segurança conforme “Política de Gestão de Continuidade de Negócio”.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

3.8 Dos Procedimentos de Segurança da Informação

Os procedimentos de segurança da informação estão subdivididos nos itens:

3.8.1 Ambiente Físico

Os colaboradores deverão possuir cuidado com a exposição de arquivos em papel. Nenhuma informação confidencial deve ser deixada à vista seja em papel ou quaisquer dispositivos, eletrônicos ou não.

Ao se ausentar da estação de trabalho, os colaboradores deverão guardar no seu armário ou colocar o documento em papel com a face em branco virada para cima.

O usuário somente poderá imprimir o documento quando necessário. Depois de enviado para impressão e liberado no equipamento, deve recolher o documento imediatamente.

Ao atestar que um documento ou impressão não será mais necessário, ou após a sua digitalização, o usuário deverá destruir os documentos através das fragmentadoras de papel disponíveis no Metrus.

3.8.2 Comunicação Verbal Dentro e Fora do Instituto

O colaborador deverá seguir as diretrizes da “Política de Comunicação”, do “Guia de Comunicação” e do “Guia de Boas Práticas nas Redes Sociais” ou contatar a Gerência de Comunicação e Relacionamento - GCR.

3.9 Segurança do Ambiente lógico

3.9.1 Utilização de Senhas

Somente usuários autorizados poderão acessar as informações e sistemas do Metrus. O usuário é responsável pela sua chave de acesso, sua senha e por todos os acessos e operações realizadas através destas, não podendo fornecer a qualquer pessoa dentro ou fora do Metrus sob o risco de eventual vazamento de informações e penalidades previstas pelo normativo “Norma de Proteção e Governança de Dados Pessoais”.

As chaves de acesso deverão possuir robustez de segurança, com combinação de números, letras e caracteres especiais, as chaves de acesso deverão ser atualizadas no prazo de 90 (noventa) dias.

A chave de acesso é pessoal e intransferível, devendo o colaborador manter o sigilo de acesso e em nenhuma circunstância, compartilhar a senha com demais colaboradores e terceiros.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

As chaves de acesso devem ser genéricas, sendo vedado o uso de senhas iguais ou similares às utilizadas em plataformas externas, como redes sociais, e-mails, bancos, dentre outros.

Em relação às chaves de acesso de terceiros, estes devem ter ciência, através dos gestores dos contratos, dos procedimentos da Política de Segurança da Informação, devendo prezar pelo seu cumprimento.

É vedada a utilização de e-mails corporativos com o domínio do Metrus por terceiros. Também, é proibido o uso da assinatura padrão do Instituto por terceiros.

3.9.2 Sistemas

A Coordenadoria de Tecnologia da Informação – CTI realizará periodicamente testes e atualização de Cópia de segurança (*Backup*) das informações constantes nos sistemas utilizados pelo Metrus para fins de recuperação em caso de desastres.

É proibida a execução de programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

É vedada a execução de programas, instalação de equipamentos, armazenamento de arquivos ou promoção de ações que possam facilitar o acesso de usuários não autorizados à rede corporativa do Metrus.

É vedado o envio de informações confidenciais (autorizadas) para e-mails externos sem a utilização de mecanismo de proteção.

Os procedimentos acima estão descritos nos instrumentos normativos “Cópias de Segurança e Recuperação de Dados” e “Realização de Backup e Restauração de Dados em Fita”.

3.9.3 Arquivos e Diretórios

A utilização dos arquivos e diretórios pelo Metrus deverá observar o controle de acesso lógico aos diretórios, devendo o usuário somente possuir acesso ao estritamente necessário para o desempenho da função.

Quando necessário o compartilhamento de arquivos com dados sensíveis internamente, deverão ser utilizados através da utilização de senha ou medida de segurança equivalente, que impeça o acesso indevido pelos demais usuários, conforme instrumento normativo “Manual de Compartilhamento de Arquivos com Segurança”.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

3.9.4 Estação de Trabalho

As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

O usuário deve resguardar o ambiente de trabalho conforme previsto na "Política de Proteção e Governança de Dados Pessoais".

3.9.5 Equipamentos Portáteis

Como parte das medidas de proteção da informação adotadas pelo Metrus, todos os notebooks corporativos disponibilizados para uso profissional são obrigatoriamente criptografados. Essa prática visa garantir a confidencialidade e a integridade dos dados armazenados nos dispositivos, mesmo em situações de perda, furto ou roubo.

A entrada e a saída de equipamentos portáteis nas dependências do Metrus, mas não pertencentes ao Instituto, quando da necessidade de acesso à rede, deverá ser formalizado à Coordenadoria de Tecnologia da Informação - CTI para habilitação à rede de dados específica para acesso à internet. Equipamento de terceiros é vedado o acesso à rede de dados do Metrus.

Dispositivos de armazenamento portáteis, como por exemplo pendrives, hd's externos, cd's, entre outros, de propriedade de terceiros devem estar sujeitos a vistorias pela Coordenadoria de Tecnologia da Informação - CTI, permitindo checar os controles de vírus e salvamento de arquivos à rede corporativa. Caso o terceiro não permita tal checagem, o acesso à rede será vetado.

Equipamentos de terceiros devem ser levados ao suporte para serem verificadas a atualização do antivírus e existência de vírus. É responsabilidade da área contratante encaminhar o terceiro para a referida verificação de segurança.

Equipamentos portáteis de propriedade do Metrus devem usar mecanismos de proteção física provido pela Coordenadoria de Tecnologia da Informação para proteger as informações, bem como os equipamentos.

É vedada a utilização de equipamentos portáteis próprios dos colaboradores para acesso à internet, rede corporativa ou sistemas do Metrus, exceto se expressamente autorizado pela Coordenadoria de Tecnologia da Informação - CTI.

Visando uma maior segurança no processo de entrada e saída de notebooks de propriedade do Metrus, recomenda-se a adoção dos seguintes procedimentos:

- Armazenamento do equipamento no porta-malas ou em local não visível, quando em deslocamentos de carro;

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

- Ao movimentar-se com o equipamento, se possível, não utilizar malas convencionais para notebook;
- Não colocar o notebook em carrinhos de aeroporto/despachar junto à bagagem;
- Em locais públicos (recepção de hotéis, restaurantes e aeroportos etc.), manter o notebook próximo e sempre à vista, não se distanciando do equipamento;
- Evitar a utilização do notebook em locais públicos;
- Nos hotéis, preferencialmente, guardar o notebook no cofre, caso disponível;
- Avaliar a necessidade de levar o equipamento em qualquer deslocamento.

3.9.6 Softwares

Toda instalação de software no Metrus deve ser solicitada via sistema de chamados, analisada e aprovada pela Coordenadoria de Tecnologia de Informação – CTI conforme previsto no "Manual de Delegação de Autoridade".

É proibido o uso de softwares ilegais (sem licenciamento) nos computadores do Metrus.

O uso de softwares de mensageria deve ser utilizado apenas como ferramenta de produtividade, para comunicação online no exercício da função do usuário.

A Coordenadoria de Tecnologia da Informação - CTI poderá valer-se-á desta política para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso ou ilícito, em atendimento à Lei 9.609/98 (Lei do Software).

3.9.7 Equipamentos de informática

Todo equipamento de informática deve ser adquirido mediante homologação prévia pela Coordenadoria de Tecnologia da Informação - CTI. O usuário deve zelar pela conservação dos equipamentos de informática sob sua responsabilidade.

Somente poderão ser conectados à rede corporativa os equipamentos fornecidos pelo Instituto.

Toda manutenção ou reparo – seja de hardware ou software – deverá ser requisitado à Coordenadoria Tecnologia da Informação - CTI, mediante abertura via sistema de chamado, ainda que o usuário tenha conhecimento da medida a ser adotada.

A Coordenadoria de Tecnologia da Informação - CTI manterá inventário dos equipamentos utilizados, sejam próprios, alugados ou leasing e poderá a qualquer momento solicitar a

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

devolução dos equipamentos cedidos ou verificação das condições deles, devendo estes ser entregues ou apresentados em perfeitas condições de uso e conservação.

3.10 Utilização da Rede Corporativa

O acesso à rede corporativa é protegido através de chave de acesso e senha.

Todos os arquivos inerentes às atividades do colaborador ficam gravados na rede, em pasta de trabalho da área. Inexiste backup dos arquivos gravados no computador(local). Os usuários devem administrar os seus arquivos gravados, excluindo aqueles que não são mais necessários para a sua finalidade. Neste sentido, não é responsabilidade da CTI a recuperação de arquivos salvos no computador.

Arquivos que estão na rede, na pasta P: (publico), são de caráter temporário para agilizar a transferência entre as áreas não podendo ficar permanentemente nessa pasta. Arquivos com mais de 1 (uma) semana hospedados serão excluídos através de processo automatizado.

É vedada a gravação de arquivos particulares (músicas, filmes, fotos, etc.) nos drivers de rede, pois ocupam o espaço comum limitado do departamento. Caso a Coordenadoria de Tecnologia da Informação - CTI localize tais arquivos, poderá excluir sem aviso prévio.

3.11 Acesso Wireless

O acesso à rede corporativa também pode ser realizado através da rede wireless (wi-fi), bem como essa rede fornece acesso à consultores e visitantes com a devida proteção para estes prestadores acessarem estritamente o ambiente de internet protegido pelas regras de *firewall*.

As orientações para a correta utilização dos recursos de rede estão descritas no instrumento normativo “Acesso à Rede Sem Fio do Metrus”.

3.12 Uso de Mídias Removíveis e da porta USB

É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

Tendo em vista a possibilidade de mídias removíveis serem utilizadas para a fuga de informações corporativas confidenciais, o usuário, caso necessite de forma imprescindível utilizar de tal mecanismo, deve justificar e requerer a aprovação do seu superior imediato através da abertura via sistema de chamado à Coordenadoria de Tecnologia da Informação - CTI.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

Os usuários de mídias removíveis serão diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação conforme previsto na LGPD.

3.13 Uso da Internet

O acesso à internet nas dependências do Metrus é feito através da rede corporativa, sendo vetada a utilização de qualquer outro recurso para acesso à internet pelos equipamentos do Metrus.

O acesso é monitorado pela Coordenadoria de Tecnologia da Informação – CTI podendo ser levado ao conhecimento pelos diretores e gestores quando necessário.

O Metrus não se responsabiliza por problemas ocasionados ao fornecimento de informações pessoais de seus usuários, como números de cartão de créditos ou contas e senhas.

O Metrus se reserva o direito de monitorar o uso de cada recurso tecnológico por qualquer motivo comercial ou profissional legítimo, por razões de segurança, em caso de violação ou de suspeita de violação deste padrão empresarial, de acordo com a lei e com a “Política de Proteção e Governança de Dados Pessoais” do Metrus, quando aplicável.

As orientações para a correta utilização dos recursos de rede estão descritas na norma “Utilização de Internet”.

3.14 Correio Eletrônico (E-Mail)

O sistema de correio eletrônico deve ser utilizado exclusivamente para atividades relacionadas ao Metrus.

As mensagens por e-mail deverão seguir a “Política de Comunicação”.

As orientações para a correta utilização dos recursos de rede estão descritas na norma “Correio Eletrônico”.

3.15 Antivírus

Todos os equipamentos conectados à rede corporativa do Metrus são constantemente monitorados e protegidos contra vírus, malwares e outras ameaças. Neste sentido, a implementação de antivírus nos servidores e estações são atualizados automaticamente.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

Em caso de qualquer suspeita de vírus, o colaborador deverá imediatamente consultar a Coordenadoria de Tecnologia da Informação -CTI, sobre os procedimentos necessários para reparo do arquivo e/ou equipamento.

A varredura por vírus é realizada diariamente nas estações de trabalho e servidores.

3.16 Aplicativos

Todos os aplicativos instalados nas estações de trabalho foram previamente homologados e testados pela Coordenadoria Tecnologia da Informação - CTI, sendo proibido o uso de aplicativos com outra finalidade senão ao desempenho de atividades para realização dos trabalhos.

A Coordenadoria de Tecnologia da Informação – CTI, deverá ser consultada previamente sempre que necessária a aquisição, homologação, desenvolvimento e instalação ou remoção de aplicativos nos equipamentos do Metrus.

É vedada a cópia, alteração ou utilização de quaisquer aplicativos de propriedade ou licenciados ao Metrus cuja finalidade não seja a pretendida.

Quaisquer iniciativas de uso corporativo de aplicativos pela internet ou aplicativos que interagem com provedores externos (nuvem de dados) e que utilizem ou façam integração com dados provenientes ou de propriedade do Metrus, deve estar em conformidade com a “Política de Proteção e Governança de Dados Pessoais” e “Código de Ética” publicados na Intranet.

3.17 Uso de Inteligência Artificial (IA)

Para garantir a segurança da informação e a proteção dos dados de todos os nossos stakeholders a utilização da inteligência artificial deve ocorrer de forma responsável e alinhada às políticas internas. É imprescindível que, ao realizar pesquisas ou atividades que envolvam inteligência artificial, não sejam utilizados dados pessoais ou sensíveis dos participantes e beneficiários, bem como quaisquer informações confidenciais do Instituto. O uso de tais dados deve ser restrito e autorizado, sempre respeitando a legislação vigente e os princípios de privacidade e confidencialidade. Além disso, os funcionários devem assegurar que as ferramentas de inteligência artificial sejam empregadas apenas para fins legítimos, evitando qualquer ação que possa comprometer a segurança, a integridade ou a reputação da organização.

A utilização da inteligência artificial (IA) deve seguir alguns cuidados para garantir a segurança, a ética e a conformidade. Aqui estão alguns princípios para o uso da IA:

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

Princípios para o Uso da IA

- **Transparência**
  O uso de tecnologias de IA deve ser comunicado de forma clara e acessível a todos os usuários, internos e externos, sempre que aplicável.
- **Privacidade e Proteção de Dados**
  Os dados utilizados por sistemas de IA devem estar em total conformidade com a Lei Geral de Proteção de Dados (LGPD) e demais legislações pertinentes.
- **Responsabilidade**
  Toda decisão automatizada deve contar com supervisão humana e dispor de mecanismos que permitam sua revisão e contestação, quando necessário.
- **Segurança**
  Os sistemas de IA devem ser protegidos contra acessos não autorizados, manipulação indevida de dados e usos maliciosos.
- **Complementaridade Humana**
  A IA deve atuar como ferramenta de apoio ao trabalho humano, não devendo substituir funções críticas sem uma avaliação prévia de riscos e impactos.

Restrições ao Uso de IA

- É expressamente proibido o uso de IA para gerar, manipular ou disseminar conteúdos falsos, discriminatórios ou que violem direitos fundamentais.
- O uso de ferramentas de IA externas com dados do Metrus é restrito e requer autorização prévia da Coordenadoria de Tecnologia da Informação.

3.18 Monitoramento

Os recursos de informação serão submetidos a processos de monitoramento e auditoria para a verificação quanto à aderência da "Política de Segurança da Informação" e o comportamento do usuário quanto ao uso dos recursos.

O resultado do monitoramento dos recursos pode ser utilizado como evidência de suporte para futuras ações disciplinares.

Os usuários declaram no ato de admissão estarem cientes de suas obrigações quanto à utilização dos recursos tecnológicos disponibilizados e manuseio das informações sensíveis como previsto no "Código de Ética" e "Política de Proteção e Governança de Dados Pessoais" do Metrus.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

3.19 Incidentes de Segurança

Todas as violações de segurança devem ser relatadas imediatamente à Coordenadoria de Tecnologia da Informação – CTI conforme previsto no instrumento normativo "Reporte de Incidentes de Segurança".

Caso o incidente envolva a exposição de dados pessoais sob a guarda do Metrus, também deverá ser comunicado imediatamente ao Encarregado de Dados Pessoais (DPO) do Metrus, conforme previsto na "Política de Proteção e Governança de Dados Pessoais".

4. Responsabilidades

4.1 Divulgação

Esta Política será divulgada na intranet para todos os colaboradores e a todos os usuários da informação que mantém relação com o Metrus (conselheiros, dirigentes, integrantes de Comitês, temporários), visando à conscientização com relação à Segurança da Informação.

4.2 Sanções

As violações a esta política estarão sujeitas às sanções disciplinares e na legislação vigente no Brasil, sem aviso prévio, as quais sujeitarão ao usuário medidas administrativas e legais cabíveis como notificação do usuário até rescisão do contrato de trabalho para empregados ou rescisão do contrato para prestadores de serviço ou parceiros.

O usuário infrator poderá ser notificado e a ocorrência comunicada ao seu gestor imediato, à Diretoria correspondente e à Presidência.

4.3 Colaboradores (Colaboradores, conselheiros, estagiários e prestadores de serviços)

- Cumprir fielmente esta Política.
- Zelar pelo sigilo das informações de que faz uso, devendo utilizá-las somente para fins profissionais.
- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizadas;

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

- Buscar orientação do gestor imediato e da Coordenadoria de Tecnologia da Informação em caso de dúvidas relacionadas à segurança da informação;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Metrus;
- Cumprir as leis e as normas internas que regulamentam os aspectos de propriedade intelectual e comunicar imediatamente à Coordenadoria de Tecnologia da Informação na ocorrência de qualquer suspeita de incidente de segurança.

4.4 Gestores e Diretores (Diretorias, Gerências e Coordenações)

- Primordialmente, cabe às Diretorias, Gerências e Coordenações a gerência dos ativos do Metrus;
- Garantir o devido conhecimento e cumprimento das diretrizes desta Política;
- Comunicar imediatamente eventuais casos de violação de segurança da informação;
- Prezar pelo devido controle de acesso dos colaboradores aos sistemas e recursos do Metrus, de acordo com as funções desempenhadas.

4.5 Coordenadoria de Tecnologia da Informação - CTI

- Capacitar os colaboradores do instituto para utilizarem adequadamente os ativos de informação e garantir a disponibilidade destes;
- Divulgar informações acerca das responsabilidades administrativas, legais e sanções decorrentes da indevida utilização dos recursos disponibilizados;
- Realizar campanhas contínuas de conscientização de Segurança da Informação para a monitoração e controle destas diretrizes.
- Divulgar esta Política aos terceiros e prestadores de serviços, temporários visando a segurança da informação no Metrus como gestora desta Política.
- Gerenciar a capacidade do ambiente de TI para garantir a disponibilidade dos recursos aos colaboradores.
- Encaminhar à Coordenadoria de Riscos e Controles a identificação de conflitos de interesses ou necessidade de segregação de função de diferentes perfis.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

- Realizar periodicamente testes de vulnerabilidade e invasão promovendo as adequações necessárias emitidas nos relatórios de validação.
- Manter sistema de monitoria do ambiente interno de TI, coletando as atividades de todos os usuários durante os acessos à internet.

4.6 Coordenadoria Jurídica e de Conformidade - CJC

A Coordenadoria Jurídica e de Conformidade mantém um processo formal de gestão dos Termos de Confidencialidade assinados por Conselheiros e membros dos Comitês, com o objetivo de assegurar o compromisso com a proteção das informações sensíveis às quais esses agentes têm acesso no exercício de suas funções.

- A assinatura do Termo de Confidencialidade é obrigatória antes do início das atividades.
- Os termos devem ser armazenados e gerenciados de forma segura.
- A renovação ocorre a cada início de mandato, no momento da posse, podendo, no entanto, ser exigida em outros momentos, conforme diretrizes internas ou alterações regulatórias.

5. Definições

Aplicativo: Conjunto de programas de computador desenvolvidos internamente ou adquiridos de terceiros.

Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Sistema de Chamado: É o sistema cuja função serve para o registro de uma solicitação ou suporte ao usuário que contém todas as informações inerentes ao atendimento, possibilitando seu acompanhamento.

Chave de Acesso: Identificação do usuário no ambiente informatizado.

Confidencialidade: É aquela informação que, por sua natureza, deva ser de conhecimento restrito e, portanto, requeira medidas especiais para sua segurança.

Equipamentos portáteis: "Laptops" e demais equipamentos com poder de processamentos que possam ser transportados pelo usuário.

Estação de trabalho: Microcomputador ou notebook utilizado para acesso e manuseio de informações e aplicativos.

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

Homologação: Processo de avaliação e aprovação técnica de equipamento de informática e de aplicativo que antecede sua aquisição.

Inventário: Levantamento e registro individualizado de equipamentos de informática e de aplicativos.

Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.

Acesso remoto: Utilização de aplicativos de produção por usuários devidamente autorizados fora das instalações do Metrus, por meio de VPN, com intuito de dar continuidade às atividades desempenhadas.

Rede corporativa: Conjunto de recursos de informação de uso corporativo, disponibilizados pela Tecnologia da Informação.

Senha: Código secreto do usuário que autêntica a identidade de uma chave de acesso.

Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.

Softwares de Mensageria: São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

Terceiros: Funcionários de empresas contratadas que prestam serviços ao Metrus.

USB (Universal Serial Bus): É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

Usuário: Pessoa autorizada e capacitada para utilizar os recursos de informação do Metrus.

VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna.

Wireless Fidelity (Wi-fi): Extensão da rede corporativa de dados propagada via tecnologia de ondas de rádio, sem contato físico para acesso.

Inteligência Artificial(IA): é um ramo da ciência da computação que se dedica à criação de sistemas capazes de realizar tarefas que normalmente exigiriam inteligência humana. Essas

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

tarefas incluem: raciocínio lógico, aprendizado (machine learning), reconhecimento de padrões, compreensão de linguagem natural, percepção visual e auditiva e tomada de decisões.

6. Documentação de referência

Nome do documento	Código	Armazenamento
Código de Ética e Conduta	-	Intranet Metrus
Política de Comunicação	POL-GCR-001	Intranet Metrus
Política de Gestão de Continuidade de Negócios	POL-CTI-001	Intranet Metrus
Política de Gestão de Riscos	POL-CRC-001	Intranet Metrus
Guia de Comunicação	-	Intranet Metrus
Guia de Boas Práticas nas Redes Sociais	-	Intranet Metrus
Política de Proteção e Governança de Dados Pessoais	POL-CRC-003	Intranet Metrus
Acesso à Rede Interna de Dados do Metrus	NOR-05-006	Intranet Metrus
Acesso à Rede Sem Fio do Metrus	NOR-CTI-002	Intranet Metrus
Compartilhamento de Arquivos com Segurança	MAN-CTI-004	Intranet do Metrus
Cópias de Segurança e Recuperação de Dados	NOR-CTI-004	Intranet Metrus
Correio Eletrônico	NOR-CTI-008	Intranet Metrus
Manual de Delegação de Autoridade	MAN-CRC-01	Intranet Metrus
Realização de Backup e Restauração de Dados em Fita.	MAN-CTI-008	Intranet Metrus
Reporte de Incidentes de Segurança	NOR-07-014	Intranet Metrus
Gestão de Acessos à Rede e Sistemas	NOR-CTI-006	Intranet Metrus
Utilização de Internet	NOR-CTI-001	Intranet Metrus

7. Anexos

Anexo 1 – Modelo de Termo de Confidencialidade e Sigilo

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: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

8. Histórico do documento

Versão nº	Descrição	Responsável	Assinatura	Data da aprovação
01	Revisão	CTI: Coordenadoria de Tecnologia da Informação	-	01/12/2010
02	Alterações: • *Revisão geral de conteúdo;* • *Formatação e padronização;* • *Codificação de POL-05-001 para POL-CTI-002.*	CTI: Coordenadoria de Tecnologia da Informação	RD nº 023/2021 Ata da 792º Reunião Ordinária da Diretoria Executiva Ato da Diretora Presidente AP nº 009/2021	25/05/2021
03	Alterações: • *Revisão geral de conteúdo;* • *Exclusão da norma de Armazenamento de Arquivos;* • *Inclusão da Norma de Gestão de Acessos à Rede e Sistemas;* • *Inclusão do manual de Compartilhamento de Arquivos com Segurança.*	Aprovação do Documento	RD Nº 930/2024 Reunião Ordinária da Diretoria Executiva Ato da Diretora Presidente AP nº 12/2024	27/05/2024
04	Alterações: • *Inclusão do item 4.6;* • *Inclusão do anexo no*	Revisão: Analista de Tecnologia da Informação	DocuSigned by: Fausto Dias Pinheiro 6A2DA055B28E4A9...	18/06/2025
		Análise Preliminar: Analista de Conformidade Sr.	Assinado por: Denise da Conceição Pereira ID52E9FFEE9A4C3...	

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: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

	item 7; • *Inclusão de tópicos nos itens 3.2 e 3.9.5.* • *Inclusão de IA no item 3.17.* • *Inclusão no item 5 - Definições.*	Aprovação: Coordenador de Tecnologia da Informação	Assinado por: Arnaldo dos Santos Recacho 9A35ED7EA15343A...	
		Aprovação do Documento:	RD Nº 974 /2025 Reunião Ordinária da Diretoria Executiva Ato da Diretora Presidente AP nº 012/2025	

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: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

Anexo I – Termo de Confidencialidade e Sigilo

TERMO DE CONFIDENCIALIDADE E SIGILO

NOME:	
CPF:	
ÓRGÃO:	
TITULAR/SUPLENTE:	
MANDATO:	

Eu, acima descrito(a), assumo o compromisso de manter confidencialidade e sigilo sobre todas as informações e documentos confidenciais a que tiver acesso durante o exercício do mandato na Entidade Fechada de Previdência Complementar: Metrus – Instituto de Seguridade Social, inscrito no CNPJ sob n.º 44.857.357/0001-66 e registrado sob o n.º 38066-1 na Agência Nacional de Saúde Suplementar – ANS. Por este Termo de Confidencialidade e Sigilo comprometo-me:

1. A não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;
2. Comprometo-me a manter a integridade e a confidencialidade das informações, não as divulgando sem a estrita observância das responsabilidades inerentes ao exercício do mandato no qual fui investido(a).
3. A proteger todos os dados pessoais aos quais venha a ter acesso no exercício de minhas funções, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD). Comprometo-me a não utilizar, compartilhar ou divulgar tais dados para qualquer finalidade além daquelas estritamente relacionadas às atividades que realizo no âmbito do Comitê de Ética, e adotarei todas as medidas de segurança, técnicas e administrativas, aptas a proteger esses dados de acessos não autorizados, vazamentos ou quaisquer formas de tratamento ilícito ou inadequado.
4. A não me apropriar de material confidencial e/ou sigiloso, de informações e documentos pessoais que venham a estar disponíveis;
5. A não repassar o conhecimento das informações que tiver acesso, responsabilizando-me por todas as pessoas que vierem a ter acesso às informações por meu intermédio, e me obrigando, assim, a ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas;
6. A não divulgar de nenhuma maneira ou por qualquer meio as informações e/ou documentos a que tiver acesso.
7. Entende-se como informação e documentos confidenciais: quaisquer informações, dados, processos, cadastros, fluxogramas, ou outros materiais de propriedade do Metrus – Instituto de Seguridade Social.

DS FDP Rubrica DDCP Rubrica ADSR

Instrumento Normativo			
Tipo: **Política**	**Nome:** **Política de Segurança da Informação**		**Código:** POL-CTI-002
Área gestora: CTI – Coordenadoria de Tecnologia da Informação	**Vigência:** A partir da data de aprovação do documento	**Validade:** 3 anos	**Versão:** 04

8. Comprometo-me a zelar pela guarda do sigilo das credenciais de acesso e solicitar o seu cancelamento caso ocorra qualquer alteração da representatividade legal que hoje detenho.

Declaro que recebi as instruções necessárias para acesso e utilização à área restrita do site do Metrus (Portal de Governança) e utilização do serviço de correio eletrônico.

Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o(a) abaixo assinado(a) ciente de todas as sanções administrativas, judiciais e penais que poderão advir.

Estou ciente de que a confidencialidade é obrigatória mesmo após o encerramento do mandato.

Declaro, também, estar ciente da minha responsabilidade quanto a este documento e as informações nele contidas.

São Paulo, xx de xxxx de xxxx.

NOME COMPLETO