

Instrumento Normativo			
Tipo: Política	Nome: Política de Segurança da Informação		Código: POL-GTI-002
Área gestora: GTI – Gerência de Tecnologia da Informação	Vigência: A partir da data de aprovação do documento	Validade: 3 anos	Versão: 05

1. Objetivo

Estabelecer os princípios, diretrizes e responsabilidades para a proteção das informações do Metrus – Instituto de Seguridade Social, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e a conformidade legal no tratamento das informações, em alinhamento à legislação vigente, especialmente à Lei Geral de Proteção de Dados Pessoais (LGPD).

2. Abrangência

Esta Política aplica-se a todos os colaboradores, dirigentes, conselheiros, membros de comitês, estagiários, temporários, prestadores de serviços, fornecedores e quaisquer terceiros que tenham acesso às informações ou aos ativos de informação do Metrus, independentemente do meio ou formato.

3. Diretrizes de Segurança da Informação

3.1. Princípios da Segurança da Informação

As informações do Metrus são tratadas como ativos estratégicos e devem ser protegidas durante todo o seu ciclo de vida. A Segurança da Informação é orientada pelos seguintes princípios:

- **Confidencialidade:** acesso restrito a pessoas autorizadas;
- **Integridade:** proteção contra alterações não autorizadas;
- **Disponibilidade:** acesso às informações e sistemas quando necessário;
- **Autenticidade:** garantia da identidade do usuário e da origem da informação;
- **Privacidade e Proteção de Dados Pessoais:** respeito aos direitos dos titulares;
- **Conformidade Legal e Normativa:** observância às leis e normas aplicáveis.

3.2. Classificação da Informação



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

Toda informação criada, recebida ou custodiada pelo Metrus deve ser classificada pelo seu responsável, conforme seu grau de sensibilidade e impacto potencial:

- **Confidencial:** informações sensíveis cujo acesso indevido pode causar prejuízos legais, financeiros ou reputacionais;
- **Interna:** informações de uso restrito ao ambiente institucional;
- **Pública:** informações passíveis de divulgação externa sem restrições.

A classificação orienta a definição das medidas de proteção e controle aplicáveis.

3.3. Propriedade Intelectual

As informações, sistemas, documentos, criações e recursos desenvolvidos ou utilizados no exercício das atividades profissionais são de propriedade do Metrus e devem ser utilizados exclusivamente para fins institucionais.

3.4. Concessão, Revisão e Revogação de Acessos

O acesso às informações e sistemas será concedido conforme o princípio do menor privilégio, mediante autorização formal, sendo revisado periodicamente e revogado quando cessada a necessidade.

3.5. Rastreabilidade e Logs

O Metrus mantém mecanismos de rastreabilidade, como logs e trilhas de auditoria, para registro de acessos e alterações em sistemas e ativos de informação. Os prazos de retenção e critérios de guarda são definidos em normativos específicos, observando requisitos legais e regulatórios.

3.6. Segurança Cibernética

A Gerência de Tecnologia da Informação - GTI é responsável por avaliar, monitorar e tratar riscos cibernéticos, adotando controles técnicos e administrativos para prevenção, detecção e resposta a incidentes de segurança.

3.7. Continuidade de Negócios

O Metrus mantém Plano de Continuidade de Negócios e procedimentos de contingência para assegurar a continuidade das operações e a disponibilidade das informações.

3.8. Mesa e Tela Limpa

Os usuários devem adotar práticas de mesa e tela limpa, evitando exposição indevida de informações físicas ou digitais, especialmente aquelas classificadas como confidenciais.

3.9. Comunicação e Uso de Recursos Tecnológicos

A utilização de e-mail, internet, redes, sistemas, dispositivos e demais recursos tecnológicos deve ocorrer exclusivamente para fins profissionais, em conformidade com as políticas e normas internas.

3.10. Uso de Inteligência Artificial

O uso de soluções de Inteligência Artificial deve ocorrer de forma ética, responsável e alinhada às políticas internas, sendo vedada a utilização de dados pessoais, sensíveis ou informações confidenciais sem autorização formal. Toda decisão automatizada relevante deve contar com supervisão humana.

3.11. Monitoramento e CFTV

Os recursos tecnológicos e sistemas de CFTV podem ser monitorados para fins de segurança, auditoria e conformidade, respeitados os limites legais, a privacidade e os direitos dos titulares de dados.

3.12. Incidentes de Segurança da Informação

Todo incidente ou suspeita de incidente de segurança deve ser reportado imediatamente à Gerência de Tecnologia da Informação - GTI. Incidentes que envolvam dados pessoais devem ser comunicados também ao Encarregado de Dados Pessoais (DPO) através da Coordenadoria de Riscos e Controles – CRC.

3.13. Gestão de Vulnerabilidades e Atualizações de Segurança

Adotar processos formais para **identificação, avaliação, tratamento e monitoramento de vulnerabilidades** em seus ativos de informação, incluindo sistemas, aplicações, infraestrutura tecnológica e dispositivos utilizados no ambiente corporativo.

As atualizações e correções de segurança (**patches**) devem ser tratadas de forma **priorizada, baseada em risco**, considerando a criticidade dos ativos, o impacto ao negócio e os requisitos legais e regulatórios aplicáveis.

4. Responsabilidades

4.1 Colaboradores e Usuários

- Cumprir esta Política e demais normativos;
- Proteger as informações sob sua responsabilidade;
- Reportar incidentes ou suspeitas de falhas de segurança.
- As credenciais de acesso aos sistemas, aplicações e demais recursos tecnológicos do Metrus são de uso pessoal, individual e intransferível. É expressamente proibido compartilhar, ceder, emprestar, divulgar ou permitir o conhecimento da senha ou de quaisquer credenciais de acesso a terceiros, inclusive a outros colaboradores, prestadores de serviços ou estagiários.

- É expressamente proibida a cópia, extração, armazenamento, transferência, compartilhamento ou envio de informações, dados, documentos ou arquivos classificados como confidenciais, restritos ou de uso interno do Metrus para fins particulares ou sem a devida autorização.

4.2 Gestores e Diretores

- Garantir o cumprimento desta Política em suas áreas;
- Autorizar acessos conforme necessidade funcional;
- Comunicar incidentes relevantes.

4.3 Gerência de Tecnologia da Informação – GTI

- Implementar e manter controles de segurança;
- Promover conscientização em Segurança da Informação;
- Monitorar o ambiente tecnológico e tratar vulnerabilidades.

4.4 Coordenadoria Jurídica e de Conformidade - CJC

- Gerenciar Termos de Confidencialidade;
- Apoiar a conformidade legal e regulatória relacionada à Segurança da Informação.

5. Sanções

O descumprimento desta Política poderá resultar em sanções administrativas, disciplinares, contratuais e legais, conforme legislação vigente e normativos internos.

6. Definições

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

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

CFTV - Circuito Fechado de Televisão: É um sistema de monitoramento por câmeras que transmite imagens para um conjunto restrito de dispositivos, como monitores, gravadores ou computadores.



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

7. Documentação de Referência

Nome do documento	Código	Armazenamento
Código de Ética	-	Site e Intranet Metrus
Política de Gestão de Continuidade de Negócios	POL-CTI-001	Intranet Metrus
Política de Gestão de Riscos	POL-CRC-001	Intranet Metrus
Política de Proteção e Governança de Dados Pessoais	POL-CRC-003	Intranet Metrus

8. Anexos

“Não Aplicável”.



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

9. Histórico do documento

Versão nº	Descrição	Responsável	Assinatura	Data da aprovação
01	Revisão	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.	Aprovação do Documento	RD nº 023/2021 Ata da 792ª 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 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 do Documento	RD Nº 974 /2025 Reunião Ordinária da Diretoria Executiva Ato da Diretora Presidente AP nº 012/2025	18/06/2025
05	Alterações: Revisão do conteúdo visando tornar as diretrizes mais objetivas e estratégicas, direcionando os aspectos operacionais e os detalhes para os instrumentos normativos específicos.	Revisão: Gerente de Tecnologia da Informação	Assinado por: <i>Arnaldo dos Santos Ricacho</i> 9A35ED7EA15343A...	29/07/2026
		Análise Preliminar: Analista de Conformidade Sr.	Assinado por: <i>Denise da Conceição Pereira</i> 1D52E9EEFE9A4C3	
		Aprovação do Documento:	1022ª Reunião Ordinária da Diretoria Executiva Ato da Diretora Presidente AP nº 011/2026	