

|                                                                                   |                                                                                           |                |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|----------------|
|  | <b>POLÍTICA DE USO RESPONSABLE DE INTELIGENCIA<br/>ARTIFICIAL, HERRAMIENTAS DIGITALES</b> | POL-GRMS-GD-15 |
|                                                                                   |                                                                                           | Versión 1      |
|                                                                                   |                                                                                           | 20/05/2026     |
|                                                                                   |                                                                                           | Página 1 de 5  |

## 1. OBJETO

Global Risk ha establecido la presente Política que tiene como finalidad establecer los lineamientos para el uso responsable, seguro, ético y legal de herramientas de Inteligencia Artificial (IA), plataformas digitales, recursos tecnológicos institucionales y modalidades de teletrabajo y trabajo híbrido, garantizando:

- a. La protección de la información y los datos personales.
- b. La continuidad operativa y seguridad digital.
- c. El cumplimiento de la normativa colombiana vigente.
- d. La protección de los derechos laborales y de privacidad.
- e. El uso ético y transparente de tecnologías emergentes.

## 2. ALCANCE: Esta Política aplica a:

- a. Todos los trabajadores, empleados, directivos, practicantes, contratistas y terceros vinculados a la compañía.
- b. El uso de dispositivos institucionales o personales utilizados para actividades laborales.
- c. Plataformas digitales, sistemas de información, redes, correos electrónicos y herramientas de IA generativa o automatización.
- d. Actividades realizadas de manera presencial, remota, híbrida o en teletrabajo.

## 3. MARCO NORMATIVO COLOMBIANO

La presente Política se fundamenta, entre otras, en las siguientes disposiciones normativas colombianas vigentes:

### a. Protección de datos y seguridad digital

- i. Constitución Política de Colombia (Artículos 15 y 20).
- ii. Ley 1581 de 2012 – Protección de Datos Personales.
- iii. Decreto 1377 de 2013.
- iv. Ley 1266 de 2008 – Habeas Data.
- v. Ley 1273 de 2009 – Delitos Informáticos.
- vi. Circular Externa 003 de 2018 de la SIC.
- vii. Circular externa de la Superintendencia de Vigilancia y seguridad privada 20240000245 del 14 de febrero de 2024 SARLAFT 2.0
- viii. Ley 2105 DE 2022 Programa de transparencia y ética empresarial (PTEE)

### b. Teletrabajo y trabajo híbrido/remoto

- i. Ley 1221 de 2008 – Teletrabajo.
- ii. Decreto 1227 de 2022.
- iii. Ley 2121 de 2021 – Trabajo Remoto.
- iv. Ley 2088 de 2021 – Trabajo en Casa.

|                                                                                   |                                                                                       |                |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------|
|  | <b>POLÍTICA DE USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL, HERRAMIENTAS DIGITALES</b> | POL-GRMS-GD-15 |
|                                                                                   |                                                                                       | Versión 1      |
|                                                                                   |                                                                                       | 20/05/2026     |
|                                                                                   |                                                                                       | Página 2 de 5  |

- v. Código Sustantivo del Trabajo.
- vi. Normativa del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST).

#### 4. DEFINICIONES

**Inteligencia Artificial (IA):** Tecnologías capaces de generar contenido, automatizar procesos, analizar información o asistir decisiones mediante modelos computacionales.

**Herramientas digitales:** Aplicaciones, plataformas, software, servicios en la nube y sistemas tecnológicos utilizados para actividades laborales.

**Teletrabajo:** Modalidad laboral regulada legalmente en la que el trabajador desarrolla actividades mediante TIC sin presencia física permanente en la empresa.

**Trabajo híbrido:** Esquema flexible que combina trabajo presencial y remoto según las necesidades organizacionales.

**Trabajo en casa:** Habitación ocasional, temporal o excepcional para desempeñar funciones fuera del lugar habitual de trabajo.

#### 5. PRINCIPIOS DE USO RESPONSABLE

**a. Legalidad y cumplimiento normativo:** Toda utilización de herramientas digitales e IA deberá ajustarse a:

- i. La legislación colombiana vigente.
- ii. Contratos laborales y acuerdos de confidencialidad.
- iii. Políticas internas institucionales.
- iv. Normas de protección de datos y ciberseguridad.

**b. Transparencia:** Cuando sea relevante, deberá informarse que determinados contenidos, análisis o materiales fueron generados o asistidos por IA.

**c. Supervisión humana:** Las herramientas de IA no sustituyen el criterio profesional ni la responsabilidad humana. Toda información crítica deberá ser validada por personal competente.

**d. Seguridad de la información:** Toda persona usuaria deberá proteger:

- i. Información confidencial.
- ii. Datos personales.
- iii. Información financiera.
- iv. Información estratégica y comercial.
- v. Credenciales y accesos institucionales.

**e. Uso ético:** Queda prohibido utilizar IA o herramientas digitales para:

- i. Desinformación.
- ii. Discriminación.
- iii. Acoso.
- iv. Suplantación.
- v. Fraude.
- vi. Manipulación indebida.

|                                                                                   |                                                                                       |                |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------|
|  | <b>POLÍTICA DE USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL, HERRAMIENTAS DIGITALES</b> | POL-GRMS-GD-15 |
|                                                                                   |                                                                                       | Versión 1      |
|                                                                                   |                                                                                       | 20/05/2026     |
|                                                                                   |                                                                                       | Página 3 de 5  |

vii. Actividades ilícitas.

f. **Minimización de riesgos:** Solo podrán utilizarse plataformas autorizadas o aprobadas por la compañía para fines laborales.

## 6. USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

a. **Usos permitidos:** Podrán utilizarse herramientas de IA para:

- i. Redacción y apoyo documental.
- ii. Automatización de tareas.
- iii. Organización de la información.
- iv. Investigación preliminar.
- v. Apoyo creativo y analítico.
- vi. Atención de consultas internas.
- vii. Desarrollo tecnológico autorizado.

Siempre que exista validación humana, no se vulneren derechos de terceros y no se comparta información confidencial.

b. **Usos prohibidos:** Está prohibido:

- i. Ingresar datos sensibles o confidenciales en plataformas no autorizadas.
- ii. Delegar decisiones jurídicas, financieras, médicas, disciplinarias o estratégicas exclusivamente a IA.
- iii. Generar contenido falso o engañoso.
- iv. Utilizar IA para plagio o fraude académico/laboral.
- v. Compartir credenciales institucionales.
- vi. Usar herramientas sin licencia o no autorizadas.

7. **PROTECCIÓN DE DATOS PERSONALES:** Todo trabajador vinculado a la compañía deberá cumplir las políticas de tratamiento de datos personales, tal como se especifica en las políticas del Sistema de Gestión de Global Risk MS LTDA. De igual manera, la compañía podrá restringir plataformas, monitorear remotamente a través de accesos virtuales e implementar auditoria en el momento que sea requerido.

## 8. TELETRABAJO, TRABAJO HÍBRIDO Y SEGURIDAD DIGITAL

a. **Condiciones generales:** Las modalidades remotas deberán garantizar:

- i. Disponibilidad.
- ii. Seguridad de la información.
- iii. Cumplimiento de objetivos.
- iv. Protección de datos institucionales.

b. **Obligaciones del trabajador:** El colaborador deberá:

|                                                                                   |                                                                                           |                |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|----------------|
|  | <b>POLÍTICA DE USO RESPONSABLE DE INTELIGENCIA<br/>ARTIFICIAL, HERRAMIENTAS DIGITALES</b> | POL-GRMS-GD-15 |
|                                                                                   |                                                                                           | Versión 1      |
|                                                                                   |                                                                                           | 20/05/2026     |
|                                                                                   |                                                                                           | Página 4 de 5  |

- i. Mantener conexión segura a internet.
- ii. Utilizar antivirus y sistemas actualizados.
- iii. Proteger equipos y accesos.
- iv. Evitar el uso compartido de dispositivos institucionales.
- v. Resguardar información física y digital.
- vi. Reportar incidentes tecnológicos inmediatamente.

**c. Uso de dispositivos personales:** Cuando se autorice el uso de equipos personales, los colaboradores deberán cumplir estándares mínimos de seguridad, tal como es establece en la política de ciberseguridad y seguridad de la información y recursos ofimáticos de Global Risk.

**d. Videollamadas y entornos virtuales:** En el caso de requerirse reuniones virtuales, el colaborador deberá proteger la confidencialidad, teniendo presente que no se podrán grabar sesiones sin previa autorización y evitará compartir información reservada en espacios públicos o distintos a los aprobados por Global Risk.

**9. PROPIEDAD INTELECTUAL Y DERECHOS DE AUTOR:** Los contenidos generados con apoyo de IA deberán, respetar derechos de autor y licencias, ser revisados antes de publicación y reconocer fuentes cuando corresponda.

Los desarrollos y documentos generados en ejercicio de funciones laborales podrán considerarse propiedad de la compañía conforme a la legislación aplicable y contratos suscritos.

**10. INCUMPLIMIENTO:** El incumplimiento de esta Política podrá dar lugar a:

- a. Medidas disciplinarias tal como se describe en el Reglamento Interno de trabajo de Global Risk.
- b. Generar la suspensión inmediata de los accesos.
- c. Terminación contractual.
- d. Acciones civiles, laborales, administrativas o penales según corresponda.

La política aplica a todos los trabajadores de la empresa, independientemente del tipo de contrato o modalidad de vinculación, incluyendo trabajo presencial, remoto, híbrido o en misión y asociados de negocio. Se firma a los veinte (20) días del mes de mayo del año 2026 en la ciudad de Bogotá D.C.

ORIGINAL FIRMADO POR REPRESENTANTE LEGAL

**YIRA LUZ CASTAÑEDA PATIÑO**  
REPRESENTANTE LEGAL  
GLOBAL RISK MANAGEMENT SOLUTIONS LTDA



|                                                                                   |                                                                                           |                |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|----------------|
|  | <b>POLÍTICA DE USO RESPONSABLE DE INTELIGENCIA<br/>ARTIFICIAL, HERRAMIENTAS DIGITALES</b> | POL-GRMS-GD-15 |
|                                                                                   |                                                                                           | Versión 1      |
|                                                                                   |                                                                                           | 20/05/2026     |
|                                                                                   |                                                                                           | Página 5 de 5  |

### **CONTROL DE CAMBIOS**

| <b>Fecha de actualización</b> | <b>Responsable de cambio</b>    | <b>Motivo del cambio</b>          |
|-------------------------------|---------------------------------|-----------------------------------|
| 20 de mayo de 2026            | Ivon Castañeda<br>(Sub Gerente) | Creación del documento<br>SG BASC |