DERICHEBOURG

POLÍTICA DE USO DE LA INTELIGENCIA ARTIFICIAL



Grupo DERICHEBOURG ENVIRONNEMENT

Grupo POLY-ENVIRONNEMENT

Índice

1 Objetivos y ámbito de aplicación de la política 3
1.1 Objeto de la política 3
1.2 Personas afectadas 3
1.3 Situaciones y herramientas contempladas 4
1.4 Actualización y evolución de la política 4
2 Definiciones 5
2.1 Herramienta de inteligencia artificial (IA) 5
2.2 Dato personal 5
2.3 Herramientas de IA de alto riesgo 5
2.4 Contenido generado por IA / creación asistida por IA 5
2.5 Seguridad de los tratamientos 5
2.6 Confidencialidad y protección de datos 5
3 Principios éticos y generales de utilización de las herramientas de IA 6
3.1 Principio ético fundamental 6
3.2 Finalidad, proporcionalidad y no discriminación 6
3.3 Respeto de los derechos fundamentales y de la vida privada 6
3.4 Obligación de seguridad y prevención de riesgos laborales 6
3.5 Enfoque de RSE y sobriedad digital 7
4 Derechos y obligaciones del empleador 8
4.1 Implantación de medidas técnicas y organizativas 8
4.2 Evaluaciones de impacto y evaluación de riesgos 8
4.3 Información y consulta de los representantes de los trabajadores 8
4.4 Información individual de los empleados 8
4.5 Formación y sensibilización 9
5 Utilización responsable, confidencialidad y seguridad de las herramientas de IA 10
5.1 Principios 10
5.2 Prohibición de determinados usos 12
5.3 Utilización de herramientas de IA externas o personales 12
5.4 Cooperación y comunicación de incidencias 13
6 Transparencia, supervisión humana y técnica, y derecho a la explicación 14
6.1 Supervisión humana y técnica de las herramientas de IA de alto riesgo 14
6.2 Derecho a la explicación 14
7 Gobernanza interna de la IA 15
7.1 Comité de gobernanza de la IA 15
7.2 Composición del comité de gobernanza de la IA 16
8 Procedimientos de alerta y gestión de incidentes 17
8.1 Comunicación de incidentes 17
8.2 Gestión de las alertas 17
9 Entrada en vigor, difusión y revisión 18
9.1 Información a los usuarios 18
9.2 Revisión 18
Anexo: Soluciones de inteligencia artificial autorizadas 19

1 Objetivos y ámbito de aplicación de la política

1.1 Objeto de la política

La presente política tiene por objeto **definir las normas de utilización de las herramientas de inteligencia artificial** (en adelante, herramientas de IA o herramientas de IA de alto riesgo) en el seno del grupo DERICHEBOURG ENVIRONNEMENT y del grupo POLY-ENVIRONNEMENT (en adelante denominados conjuntamente el «Grupo»), con el fin de:

- proteger los derechos y libertades de los empleados, los candidatos, los clientes, los usuarios y cualquier tercero afectado;
- garantizar el cumplimiento de la normativa aplicable, en particular el Reglamento (UE) 2016/679 (RGPD), la Ley de protección de datos y libertades digitales, el Código de trabajo y el Reglamento (UE) 2024/1689 sobre inteligencia artificial;
- regular la recopilación y el tratamiento de datos, especialmente de datos personales, en el marco de la utilización de herramientas de IA;
- prevenir los riesgos laborales, en particular los psicosociales, relacionados con la implantación de la IA en el trabajo;
- organizar la gobernanza interna de la IA, la transparencia y la supervisión humana de las herramientas de IA utilizadas.

1.2 Personas afectadas

La presente política se aplica a todos los siguientes colectivos:

- los empleados del Grupo, con independencia de su modalidad contractual (contratos indefinidos, contratos de duración determinada, aprendices y trabajadores en formación en alternancia);
- los administradores y representantes legales;
- los becarios y el personal puesto a disposición;
- en su caso, los proveedores de servicios y subcontratistas, cuando accedan a los sistemas de información del Grupo o utilicen herramientas de IA, ya sean proporcionadas por el Grupo o utilizadas por el proveedor en el marco de la prestación del servicio, siempre que su uso afecte a datos, información o actividades del Grupo, sin perjuicio de las obligaciones contractuales específicas que les correspondan.

1.3 Situaciones y herramientas contempladas

La política abarca todos los usos profesionales de las herramientas de IA, en particular:

- las herramientas de IA **generativa** (texto, imagen, audio, vídeo, código, etc.);
- las herramientas de IA de **apoyo a la toma de decisiones o de elaboración de perfiles** (por ejemplo, en los procesos de selección, la gestión del rendimiento, la planificación y la asignación de tareas);
- las herramientas de IA que puedan calificarse como **«herramientas de IA de alto riesgo»** en el sentido del Reglamento (UE) 2024/1689, en particular cuando se utilicen para la gestión del personal, la evaluación del rendimiento o la vigilancia de los trabajadores;
- las herramientas de IA **integradas en equipos de trabajo** (exoesqueletos, dispositivos inteligentes portátiles, etc.);
- cualquier otra herramienta o funcionalidad basada en técnicas de IA y utilizada en un contexto profesional, incluso cuando sea accesible a través de servicios en línea.

Usos personales de las herramientas de IA:

Las herramientas de IA puestas a disposición por el Grupo están destinadas a un uso profesional.
No obstante, se tolera un uso personal ocasional y razonable, siempre que no afecte a la actividad profesional del usuario ni al funcionamiento o la seguridad de los sistemas del Grupo.
Este uso deberá respetar todas las normas de seguridad, confidencialidad y protección de datos previstas en la presente política.

1.4 Actualización y evolución de la política

Elaborada en el marco de la política de seguridad y cumplimiento del Grupo, la presente política recuerda las principales normas jurídicas, propone principios éticos y establece buenas prácticas que deben respetarse en el uso profesional de la IA. Habida cuenta de la rápida evolución de las tecnologías de IA y del marco jurídico aplicable, está previsto que se revise periódicamente, en las condiciones especificadas en el artículo 9.2.

2 Definiciones

2.1 Herramienta de inteligencia artificial (IA)

Aplicación, servicio o funcionalidad basada en técnicas de inteligencia artificial que permite analizar datos, generar contenido, formular recomendaciones, automatizar tareas o ayudar a los usuarios a realizar sus actividades.

2.2 Dato personal

Se entenderá por **«dato personal»** toda información relativa a una persona física identificada o identificable, en el sentido del RGPD.

2.3 Herramientas de IA de alto riesgo

Se consideran **«herramientas de IA de alto riesgo»** aquellas que pertenecen a las categorías enumeradas en los anexos del Reglamento (UE) 2024/1689, en particular las utilizadas en el ámbito del empleo, la gestión de los trabajadores y el acceso al empleo, así como aquellas que tengan un impacto significativo en los derechos fundamentales.

2.4 Contenido generado por IA / creación asistida por IA

El **«contenido generado por IA»** es el contenido producido de forma autónoma por una herramienta de IA, sin una intervención humana creativa significativa.
La **«creación asistida por IA»** es una obra o contenido realizado con ayuda de una herramienta de IA, en el que una persona física ejerce elecciones creativas que reflejan su personalidad (selección de los datos de entrada, configuración, modificaciones sustanciales del resultado, etc.).

2.5 Seguridad de los tratamientos

Conjunto de medidas técnicas y organizativas que garantizan la disponibilidad, la integridad, la confidencialidad y la trazabilidad de los datos tratados por las herramientas de IA, y que previenen cualquier acceso no autorizado, pérdida o alteración.

2.6 Confidencialidad y protección de datos

Obligación de garantizar que los datos solo sean accesibles para las personas debidamente autorizadas y que su tratamiento mediante herramientas de IA respete los principios del RGPD (licitud, minimización y limitación de la finalidad, entre otros), así como el nivel de confidencialidad aplicable a los datos en cuestión.

3 Principios éticos y generales de utilización de las herramientas de IA

3.1 Principio ético fundamental

Tal como establece el artículo 1 de la Ley n.º 78-17, de 6 de enero de 1978, relativa a la informática, los ficheros y las libertades: «La informática debe estar al servicio de todos los ciudadanos. (…) No debe atentar contra la identidad humana, los derechos humanos, la vida privada ni las libertades individuales o públicas».
La inteligencia artificial puede ayudar a los empleados en sus análisis, pero las decisiones finales, especialmente las valoraciones críticas, deben seguir siendo exclusivamente humanas. **La IA: una herramienta de apoyo, nunca un decisor.** Todo usuario autorizado a recurrir a la IA debe tener presente este principio fundamental: **la IA debe estar al servicio de las personas, y no al revés**.

3.2 Finalidad, proporcionalidad y no discriminación

La utilización de las herramientas de IA debe perseguir **finalidades determinadas, explícitas y legítimas**, y no desviarse hacia otros fines incompatibles. Los datos tratados deben ser adecuados, pertinentes y limitados a lo necesario en relación con las finalidades perseguidas.
Las herramientas de IA de alto riesgo no podrán utilizarse para aplicar discriminaciones directas o indirectas, en particular en materia de selección de personal, remuneración, evaluación, promoción o extinción del contrato. Los usuarios deberán velar por **detectar y corregir** cualquier contenido manifiestamente sesgado, discriminatorio, engañoso u ofensivo generado por una herramienta de inteligencia artificial.

3.3 Respeto de los derechos fundamentales y de la vida privada

Las herramientas de IA de alto riesgo deberán utilizarse de forma que se respeten la **dignidad humana, la vida privada, la libertad de expresión, la igualdad entre mujeres y hombres y el principio de no discriminación**.

Los sistemas de vigilancia o seguimiento de los empleados basados en IA solo podrán implantarse respetando el Código del Trabajo, el RGPD y la Ley de Protección de Datos y Libertades Digitales, y deberán ser proporcionales al objetivo perseguido.

3.4 Obligación de seguridad y prevención de riesgos laborales

El Grupo aplica las medidas necesarias para garantizar la seguridad y proteger la salud física y mental de los empleados. A tal efecto, **evalúa y previene los riesgos** que puedan derivarse de la utilización de herramientas de IA.

Las herramientas de IA están destinadas a ayudar a los empleados en el desempeño de sus funciones. No sustituyen el análisis, el razonamiento ni los conocimientos especializados de los empleados.

3.5 Enfoque de RSE y sobriedad digital

La IA consume grandes cantidades de energía y agua, especialmente para la refrigeración continua de los centros de datos; su impacto medioambiental es innegable. Se invita a cada usuario a utilizar estas herramientas de forma responsable, teniendo en cuenta su impacto ecológico, y a priorizar, cuando proceda, soluciones alternativas que consuman menos energía (motores de búsqueda, bases de datos documentales internas, etc.).

4 Derechos y obligaciones del empleador

4.1 Implantación de medidas técnicas y organizativas

El Grupo implanta las medidas técnicas y organizativas adecuadas para garantizar:

- la **seguridad de los tratamientos** de datos efectuados mediante herramientas de IA (confidencialidad, integridad, disponibilidad y resiliencia);
- la **trazabilidad** de los usos de las herramientas de IA;
- una **supervisión humana y técnica efectiva** de las herramientas de IA;
- el **respeto de los derechos de las personas** afectadas (derecho a la información, de acceso, de rectificación, de oposición, etc.).

4.2 Evaluaciones de impacto y evaluación de riesgos

Cuando la utilización de una IA pueda entrañar un riesgo elevado para los derechos y libertades de las personas (en particular, en caso de elaboración de perfiles, decisiones automatizadas o uso de herramientas de IA de alto riesgo), el Grupo realizará, antes de su implantación, una **evaluación de impacto relativa a la protección de datos (EIPD)** y, cuando proceda, una **evaluación de impacto sobre los derechos fundamentales (FRIA)**, de conformidad con el Reglamento (UE) 2024/1689.

4.3 Información y consulta de los representantes de los trabajadores

Cuando así lo exija la ley, el empleador consultará al comité social y económico (CSE) antes de implantar herramientas de IA que puedan tener un impacto significativo en la organización, la gestión y el control de la actividad de los empleados.

4.4 Información individual de los empleados

El Grupo proporcionará a cada empleado **información clara, accesible y comprensible** sobre:

- la existencia de las herramientas de IA utilizadas en el marco de la relación laboral;
- las finalidades perseguidas;
- los datos tratados y su período de conservación;
- la existencia de posibles decisiones individuales automatizadas, incluida la elaboración de perfiles, y los derechos asociados (derecho a no ser objeto de una decisión basada exclusivamente en un tratamiento automatizado, salvo las excepciones previstas en el artículo 22 del RGPD);

- el derecho a obtener una explicación sobre las decisiones significativas adoptadas con ayuda de herramientas de IA de alto riesgo, de conformidad con el Reglamento (UE) 2024/1689 y la jurisprudencia europea relativa al «derecho a la explicación».
- El Grupo velará por que los empleados que utilicen, supervisen o administren herramientas de IA reciban las medidas adecuadas de información, sensibilización o formación que les permitan adquirir un nivel suficiente de competencia en materia de IA, conforme a los requisitos del artículo 4 del Reglamento (UE) 2024/1689. Estas medidas abarcarán, en particular, las capacidades, las limitaciones, los riesgos, los posibles sesgos, las normas de seguridad, la protección de los datos personales, los requisitos de supervisión humana y las buenas prácticas de utilización de las herramientas de IA puestas a disposición en la empresa.

4.5 Formación y sensibilización

El Grupo organizará actividades de formación y sensibilización sobre el funcionamiento de las herramientas de IA, sus limitaciones y sus riesgos, así como sobre las buenas prácticas de utilización (especialmente en el caso de la IA generativa), con el fin de permitir que los empleados utilicen estas herramientas de forma consciente y segura.

5 Utilización responsable, confidencialidad y seguridad de las herramientas de IA

5.1 Principios

Los usuarios se comprometen a utilizar las herramientas de IA puestas a su disposición únicamente en el desempeño de sus funciones, para los fines profesionales autorizados por el Grupo, respetando la presente política, el reglamento interno, la política de seguridad de los sistemas de información y todas las políticas y procedimientos de seguridad aplicables.
La utilización de las herramientas de IA deberá ajustarse a los requisitos de confidencialidad, seguridad de la información, protección de datos personales y propiedad intelectual, así como a las obligaciones legales, reglamentarias y contractuales aplicables a la empresa.
A tal efecto, cada usuario se compromete a respetar los siguientes principios:

- **utilizar únicamente las herramientas de IA validadas por la Dirección de Sistemas de Información e incluidas en el anexo de la presente política;**
- no introducir nunca datos personales en una herramienta de IA; únicamente podrán tratarse en las herramientas de IA aprobadas por la empresa los datos personales estrictamente necesarios para las actividades profesionales; queda prohibido utilizar datos sensibles (datos de salud, datos disciplinarios, datos confidenciales de RR. HH., datos nacionales de identificación, etc.);
- no transmitir nunca información confidencial, secretos comerciales, datos sensibles, documentos internos ni ninguna otra información cuya divulgación pudiera perjudicar a la empresa, a sus clientes, proveedores, socios o empleados, salvo que exista una autorización expresa y se apliquen las garantías adecuadas;
- considerar que toda información profesional es, por principio, confidencial y no transmitir a una IA información que no pudiera comunicarse a un tercero;
- respetar las normas de control de acceso y no compartir nunca con terceros sus credenciales, contraseñas ni derechos de acceso;
- velar por el respeto de los derechos de propiedad intelectual al utilizar herramientas de IA, tanto en lo que respecta a los contenidos introducidos como a los contenidos generados;
- tener presentes las limitaciones de las herramientas de IA, en particular los riesgos de errores, alucinaciones, sesgos, inexactitudes u obsolescencia de la información generada;
- no tomar nunca decisiones que comprometan a la empresa o a una persona afectada basándose exclusivamente en un resultado generado por una IA;

- verificar sistemáticamente, con espíritu crítico y una supervisión humana adecuada, la exactitud, la coherencia, la pertinencia, la conformidad normativa y la adecuación a las necesidades profesionales de los contenidos generados;
- adaptar, completar o corregir los resultados generados por la IA antes de utilizarlos o difundirlos;
- actuar con transparencia respecto al uso de la IA cuando el contenido generado (textos, imágenes, vídeos, etc.) esté destinado a comunicarse, indicándolo expresamente (por ejemplo: «elaborado con una herramienta de IA»);
- asumir la plena responsabilidad de los trabajos realizados con ayuda de una herramienta de IA, incluso cuando esta solo haya contribuido a su elaboración.

El incumplimiento de estas disposiciones, especialmente cuando dé lugar a la divulgación de información protegida o a una vulneración de las normas de seguridad, confidencialidad o protección de datos, podrá dar lugar a acciones civiles o penales.

Documentos de referencia

Los requisitos mencionados en esta política se detallan en los siguientes documentos, disponibles en la intranet documental del Grupo o a través de la Dirección de Sistemas de Información:

- Política de Seguridad de los Sistemas de Información (PSSI);
- Política de uso de los recursos informáticos y de telecomunicaciones;
- Política de protección de datos personales;
- Política de clasificación y tratamiento de la información;
- Procedimiento de gestión de accesos y permisos;
- Catálogo de herramientas de IA autorizadas.

✓ HACER

• Utilizar únicamente las herramientas de IA autorizadas por el Grupo.
• Verificar sistemáticamente la exactitud, la pertinencia y la conformidad de los contenidos generados.
• Aplicar el espíritu crítico y tener en cuenta las limitaciones de las herramientas de IA (errores, sesgos, alucinaciones e información incompleta u obsoleta).
• Proteger las propias credenciales y aplicar las normas de seguridad de la empresa.
• Garantizar una supervisión humana antes de difundir cualquier contenido o tomar decisiones basadas en un resultado generado por la IA.
• Actuar con transparencia respecto al uso de la IA cuando el contexto lo exija.

❌ NO HACER

• Utilizar una herramienta de IA no autorizada para actividades profesionales.
• Crear o utilizar una cuenta personal de IA en el marco de una actividad profesional.
• Introducir datos personales (véase más arriba), información confidencial, secretos comerciales o información estratégica en una herramienta de IA que no esté expresamente autorizada para ello.
• Transmitir código fuente, arquitecturas técnicas o información sensible sin autorización previa.
• Difundir o reutilizar contenido generado por IA sin una verificación humana adecuada.
• Basar una decisión profesional exclusivamente en una respuesta generada por una herramienta de IA.

5.2 Prohibición de determinados usos

En particular, los usuarios tienen prohibido:

- utilizar una herramienta de IA para clasificar, preseleccionar o evaluar candidaturas, analizar currículos, evaluar el rendimiento individual de un empleado, determinar una remuneración o tomar decisiones relativas a la movilidad, la promoción, las sanciones disciplinarias o la extinción del contrato de trabajo, sin la validación previa del Grupo y al margen de los procedimientos y herramientas oficialmente autorizados;
- recurrir a una herramienta de IA para eludir las normas de seguridad, los procedimientos internos, los mecanismos de control o las medidas de cumplimiento implantadas por la empresa;
- utilizar una herramienta de IA para crear, difundir o facilitar la producción de contenidos discriminatorios, que inciten al odio, difamatorios o engañosos, o que atenten contra la dignidad de las personas, su vida privada o los derechos de propiedad intelectual de terceros;
- utilizar cualquier herramienta de IA cuyo uso esté prohibido por la normativa aplicable, en particular por el Reglamento (UE) 2024/1689 (Reglamento de IA), o que persiga finalidades contrarias a los principios fundamentales de la empresa y a los derechos y libertades de las personas.

5.3 Utilización de herramientas de IA externas o personales

En el marco de sus actividades profesionales, los usuarios únicamente podrán utilizar las herramientas de IA puestas a su disposición o expresamente autorizadas por el Grupo.

Queda prohibido utilizar herramientas de IA accesibles en línea mediante una cuenta personal.

En cualquier caso, está prohibido introducir en una herramienta de IA no autorizada información confidencial, secretos comerciales, datos personales, información amparada por el secreto profesional o cualquier otro contenido cuya divulgación pudiera perjudicar los intereses de la empresa o los derechos de terceros.
Cuando se autorice una herramienta de IA externa, el usuario seguirá siendo responsable tanto de los contenidos que introduzca en ella como del uso que haga de las respuestas generadas.

5.4 Cooperación y comunicación de incidencias

Los usuarios colaborarán con el Grupo en la aplicación de la presente política y comunicarán **sin demora** cualquier incidente, uso indebido o riesgo identificado relacionado con la utilización de la IA.

6 Transparencia, supervisión humana y técnica, y derecho a la explicación

6.1 Supervisión humana y técnica de las herramientas de IA de alto riesgo

Las herramientas de IA de alto riesgo estarán sujetas a una supervisión humana y/o técnica efectiva, controlada por el comité de IA. Las personas encargadas de este control recibirán **información y formación suficientes** para comprender las capacidades y limitaciones del sistema, interpretar correctamente sus resultados y decidir no seguirlos o corregirlos cuando sea necesario para proteger los derechos de las personas afectadas.

6.2 Derecho a la explicación

Todo empleado que sea objeto de una decisión significativa basada en los resultados de una IA de alto riesgo tendrá derecho a obtener **explicaciones claras y pertinentes** sobre el papel de las herramientas de IA en dicha decisión y sobre los principales elementos en los que se fundamenta, de conformidad con el Reglamento (UE) 2024/1689 y la jurisprudencia europea.

7 Gobernanza interna de la IA

7.1 Comité de gobernanza de la IA

Con el fin de garantizar un uso controlado, conforme a la normativa y responsable de las herramientas de IA, el Grupo ha creado un comité de gobernanza de la IA.

El comité de gobernanza de la IA se encarga de dirigir, coordinar y supervisar la utilización de las herramientas de IA en el seno del Grupo. A tal efecto, desempeña, entre otras, las siguientes funciones:

- inventariar, evaluar y mantener actualizado el registro de las herramientas de IA utilizadas, sometidas a prueba o autorizadas en el seno del Grupo;
- velar por que los usos y las herramientas de IA cumplan los requisitos legales, reglamentarios e internos aplicables, especialmente en materia de protección de datos personales, propiedad intelectual, ciberseguridad, derecho laboral e inteligencia artificial;
- identificar, evaluar y realizar el seguimiento de los riesgos asociados a la utilización de herramientas de IA y coordinar, cuando sea necesario, las evaluaciones de impacto y las medidas de control de riesgos;
- examinar los nuevos casos de uso, formular recomendaciones y decidir las condiciones de su implantación;
- prestar apoyo a las distintas áreas de negocio en el despliegue, la utilización y la mejora continua de las herramientas de IA;
- promover actividades de sensibilización, formación y familiarización con la inteligencia artificial;
- recibir, analizar y realizar el seguimiento de las comunicaciones, alertas, incidentes o incumplimientos relacionados con la utilización de herramientas de IA, y proponer las medidas correctivas o preventivas adecuadas;
- realizar un seguimiento de las novedades normativas, tecnológicas y éticas relacionadas con la inteligencia artificial;
- proponer cualquier modificación de la presente política y del marco de gobernanza de la IA para tener en cuenta la evolución normativa, tecnológica y organizativa, así como las experiencias adquiridas mediante su utilización.

7.2 Composición del comité de gobernanza de la IA

El comité de gobernanza de la IA está integrado por miembros permanentes que representan las siguientes funciones:

Secretario/a general
Delegado de Protección de Datos (DPO)
Director/a de Recursos Humanos (DRH)
Director/a de Sistemas de Información (DSI)
Responsable de Seguridad de los Sistemas de Información (RSSI)
Responsable de Ciberseguridad
Responsable de Sistemas y Redes
Responsable de Relaciones Laborales
Asesor/a jurídico/a

En función de los asuntos tratados, el comité podrá contar con la participación de cualquier otra área o experto interno cuya intervención se considere útil (protección de datos, cumplimiento normativo, compras, áreas de negocio afectadas, representantes de los trabajadores, director del proyecto, etc.).

8 Procedimientos de alerta y gestión de incidentes

8.1 Comunicación de incidentes

Todo usuario que detecte o sospeche la existencia de un incidente, un funcionamiento incorrecto, un riesgo de discriminación, una vulneración de la vida privada, una violación de la protección de datos, un problema de seguridad o cualquier uso no conforme de una herramienta de IA deberá comunicarlo sin demora, de conformidad con los procedimientos internos de gestión de incidentes y alertas vigentes en la empresa.

A continuación, las comunicaciones se remitirán a los órganos competentes (Dirección de Sistemas de Información, DPO, comité de gobernanza de la IA, Recursos Humanos o canal interno de denuncias), en función de su naturaleza y nivel de gravedad.

Ningún usuario que haya comunicado de buena fe, de conformidad con los procedimientos internos aplicables, un riesgo, un incidente o un uso no conforme de una herramienta de IA podrá ser objeto de represalias, directas o indirectas, amenazas o intentos de aplicación de tales medidas por haber realizado dicha comunicación.

8.2 Gestión de las alertas

El Grupo, a través del comité de gobernanza de la IA, se compromete a **examinar sin demora las comunicaciones recibidas**, adoptar, si fuera necesario, medidas correctivas (suspensión del sistema, modificación de los parámetros, refuerzo de los controles, etc.) y, cuando así lo exija la ley, notificar las violaciones de datos a la CNIL y, en su caso, a las personas afectadas.

9 Entrada en vigor, difusión y revisión

9.1 Información a los usuarios

La presente política se pondrá en conocimiento de todos los empleados por cualquier medio adecuado.
Sus disposiciones también serán aplicables, cuando proceda, a los proveedores externos, consultores, subcontratistas y, en general, a cualquier persona autorizada a acceder a los sistemas de información o a las herramientas de IA del Grupo.
A tal efecto, las obligaciones correspondientes se incorporarán a las cláusulas contractuales, los compromisos de confidencialidad o cualquier otro documento contractual adecuado.

9.2 Revisión

Habida cuenta de la rápida evolución de las tecnologías de IA y del marco jurídico aplicable, la presente política podrá revisarse periódicamente.
Toda modificación sustancial se comunicará a los usuarios y, en su caso, dará lugar a una nueva consulta al CSE.

Cualquier cláusula de la política que, como consecuencia de la evolución de las disposiciones legales, reglamentarias o convencionales aplicables al Grupo, pasara a ser contraria a estas quedará automáticamente invalidada.

Entrará en vigor el 19 de octubre de 2026.

Anexo: Soluciones de inteligencia artificial autorizadas

Únicamente podrán utilizarse en el ámbito profesional las soluciones que figuran a continuación o cualquier otra solución expresamente validada por la Dirección de Sistemas de Información. Esta lista se mantiene actualizada por el comité de gobernanza de la IA y se comunica a los usuarios.

Copilot Chat (licencia empresarial de Derichebourg)
Categoría: Asistente de inteligencia artificial integrado en el entorno Microsoft 365.
Usos autorizados:

- Redacción, síntesis y reformulación de contenidos
- Búsqueda de información en el entorno Microsoft 365
- Asistencia en la preparación de documentos, presentaciones y análisis
- Automatización de determinadas tareas ofimáticas

Aspectos que deben tenerse en cuenta:

- Verificar sistemáticamente los contenidos generados antes de utilizarlos
- Respetar las normas de clasificación de la información y de confidencialidad
- Tratar únicamente información cuyo uso esté autorizado conforme a las políticas de seguridad de la empresa
- Tener presente que las respuestas pueden contener errores, sesgos o información incompleta

GitHub Copilot
Categoría: Asistente para el desarrollo de *software*.
Usos autorizados:

- Generación de código y asistencia en su escritura
- Ayuda en la documentación técnica
- Revisión y mejora de scripts o programas

Aspectos que deben tenerse en cuenta:

- Verificar sistemáticamente el código generado antes de integrarlo
- Respetar los requisitos de seguridad de las aplicaciones y las normas de desarrollo seguro
- Velar por el respeto de los derechos de propiedad intelectual aplicables a los componentes de *software* utilizados
- No introducir código fuente ni información técnica sensible sin autorización previa

Teams Premium (licencia empresarial de Derichebourg)
Categoría: Asistente para la transcripción y síntesis de reuniones.
Usos autorizados:

- Transcripción automática de reuniones
- Generación de actas y resúmenes
- Identificación de las acciones y decisiones adoptadas durante las reuniones

Aspectos que deben tenerse en cuenta:

- Informar a los participantes cuando se active una transcripción o grabación
- Respetar los requisitos de confidencialidad aplicables a las comunicaciones
- Verificar y validar las actas generadas antes de su difusión

- Respetar los períodos de conservación establecidos por la empresa
- No utilizar estas funcionalidades para tratamientos que puedan corresponder a usos de alto riesgo o estar prohibidos por la normativa

DeepL (licencia empresarial de Derichebourg) y Google Translate
Categoría: Traducción y asistencia lingüística.
Usos autorizados:
- Traducción de documentos profesionales
- Revisión y mejora de la redacción
- Asistencia en la comunicación multilingüe

Aspectos que deben tenerse en cuenta:
- Evitar la transmisión de datos personales e información confidencial o sensible
- Verificar sistemáticamente la calidad y el sentido de las traducciones generadas
- Respetar los derechos de propiedad intelectual asociados a los contenidos traducidos
- Realizar una validación humana antes de cualquier difusión externa

CrowdStrike SIEM
Categoría: Ciberseguridad y detección de amenazas.
Usos autorizados:
- Análisis de eventos de seguridad
- Correlación y detección de incidentes
- Identificación de actividades sospechosas o maliciosas

Aspectos que deben tenerse en cuenta:
- Respetar las normas de protección de datos y registro de eventos
- Limitar los datos recopilados a lo estrictamente necesario
- Verificar la legitimidad y la proporcionalidad de los tratamientos realizados
- Garantizar el respeto de los permisos de acceso a la información de seguridad

Lexis+ con Protégé (ediciones LexisNexis)
Categoría: Investigación documental y seguimiento jurídico asistidos por IA.
Usos autorizados:
- Búsqueda de información jurídica
- Seguimiento normativo
- Asistencia en el análisis documental y normativo

Aspectos que deben tenerse en cuenta:
- Verificar las referencias legales y reglamentarias proporcionadas
- No utilizar los resultados como único fundamento de una decisión jurídica
- Mantener una validación humana de los análisis y las recomendaciones generados