

## POLÍTICA DE INFORMACIÓN XM

### Objetivo

Declarar las decisiones empresariales de la gestión de la información y el conocimiento como activo crítico y estratégico, para el desarrollo de los negocios en sus necesidades presentes y futuras, que requieren ser conservados, protegidos en procura de la sostenibilidad, la construcción de sinergias y la continuidad de la operación de XM S.A. E.S.P.

### Objetivo general del sistema de gestión de seguridad de la información

Proveer los mecanismos de gestión de la información para la preservación de los criterios de confidencialidad, integridad, disponibilidad de la información de una manera sistemática, estructurada y documentada mediante la gestión del riesgo; con el fin de asegurar la continuidad del negocio, el cumplimiento de los objetivos estratégicos de XM S.A. E.S.P y brindar confianza a los grupos de interés.

### Declaraciones

Para cumplir con la política de seguridad de la información, se establecen las siguientes declaraciones, basadas en la estrategia definida por la organización y respaldadas por las mejores prácticas de la norma ISO 27001:2022, que rige nuestro sistema de gestión de seguridad de la información.

- Establecemos mecanismos para salvaguardar la información, cumpliendo la normatividad que regula a ISA y sus empresas, y en especial a aquella que tiene en su línea de negocio alojamiento y servicios de información de terceros, con criterios de neutralidad, disponibilidad, integridad, confidencialidad, transparencia y confiabilidad.
- En la prestación de los servicios del Centro Nacional de Despacho (CND), del Administrador del Sistema de Intercambios Comerciales (ASIC) y del Liquidador y Administración de Cuentas (LAC) respetamos el principio de neutralidad, para lo lograrlo se implementan mecanismos que garantizan un trato igualitario e imparcial a todos los agentes del mercado, esto incluye el acceso igual, simultáneo y completo a la información de carácter público relacionada con dichos servicios.
- Damos un tratamiento riguroso a la información confidencial de fuentes internas o de terceros y en especial la de nuestros colaboradores, asegurando el cumplimiento de la ley de protección de datos personales de nuestros grupos de interés.
- En la prestación de los servicios CND, ASIC y LAC, manejamos la información con estricta confidencialidad y reserva. Para lograrlo, hemos establecido mecanismos que garantizan una administración neutral y transparente de la información relacionada con estos servicios. Sin embargo, esto no impide que los colaboradores que participan directamente en la prestación de estos servicios lleven a cabo

sesiones de capacitación y transferencia de conocimiento técnico, excluyendo información específica de los servicios CND, ASIC y LAC, al interior de XM.

- Nos abstenemos de compartir total o parcialmente la información a la que tenemos acceso relacionada con los servicios CND, ASIC y LAC, con terceros y en particular con Interconexión Eléctrica S.A. E.S.P, sus filiales, subsidiarias y Ecopetrol S.A., y que: i) no sea de conocimiento público; ii) tenga valor comercial para la estrategia competitiva del titular y iii) su divulgación total o parcial tenga efectos sobre el nivel de competencia en el mercado.
- La información restringida o confidencial, solo puede usada por el personal previamente autorizado para el desempeño de sus funciones.
- Garantizamos el acceso a la información que requieran las autoridades para el desarrollo de sus funciones.
- Establecemos estrategias y prácticas para la gestión del conocimiento que permitan capturar, mantener y transferir el saber y la memoria institucional.
- El compromiso de la alta dirección y la participación de los líderes es fundamental para alcanzar los objetivos y desarrollar el programa de cultura de seguridad de la información.
- En XM, valoramos las obras intelectuales, creaciones e invenciones de nuestros empleados y otros activos relacionados con la información y el conocimiento, ya que forman parte de nuestros derechos patrimoniales. Además, cumplimos con la legislación de Propiedad Intelectual e Industrial, así como con los convenios, acuerdos y tratados pertinentes, junto con los compromisos voluntarios que XM haya asumido.
- Implementamos controles de seguridad que nos permiten utilizar herramientas de inteligencia artificial de manera segura, minimizando los riesgos asociados a estas aplicaciones. Estas medidas incluyen la evaluación continua de riesgos, la capacitación regular de nuestro colaboradores y proveedores en el uso ético y seguro de la inteligencia artificial IA. Además, nos aseguramos de cumplir con todas las regulaciones y mejores prácticas del sector para proteger nuestra información.
- Reconocemos los riesgos cibernéticos que pueden atentar contra la seguridad de la información y nos comprometemos a gestionarlos cumpliendo la normatividad vigente, los requisitos exigidos por los clientes y el mercado, capacitando a nuestros empleados en esta materia e implementando mecanismos tecnológicos y de procesos para mitigarlos.
- Implementamos medidas de administración a nivel tecnológico, procesos y personas que permitan mitigar los riesgos de ataques cibernéticos, fuga de información, o relacionados con la inteligencia artificial, protegiendo la confidencialidad, integridad y disponibilidad de los activos de información, nuestra buena imagen y reputación de la marca.
- Definimos y mantenemos actualizado el gobierno y los lineamientos de seguridad conforme a los cambios organizacionales y tecnológicos.



- Identificamos, clasificamos y etiquetamos los activos de información generados por los procesos de negocio, siguiendo los criterios de clasificación de la información y las medidas de protección definidas por la organización.
- Implementamos controles en el proceso de selección y contratación de colaboradores y proveedores. Estas medidas se aplican tanto en la vigencia del contrato como en la modificación y finalización de estos.
- Estamos preparados para detectar y responder ante eventos e incidentes de seguridad de la información.
- Realizamos seguimiento, buscamos la conformidad y evaluamos continuamente el sistema de gestión de seguridad de la información, a través del análisis de indicadores de desempeño establecidos.
- Asignamos los accesos físicos y lógicos a cada usuario de acuerdo con el desarrollo de sus funciones, roles y responsabilidades basados en el principio del mínimo privilegio.
- Los colaboradores, proveedores y usuarios de terceras partes deben cumplir plenamente con los roles y responsabilidades establecidos por XM en relación con la seguridad de la información y el manejo responsable de la inteligencia artificial tanto si trabajan en las instalaciones de la organización como de forma remota.
- Periódicamente realizamos auditorías internas para garantizar que la organización funcione según las normas y directrices establecidas.
- Promovemos la responsabilidad de nuestros colaboradores y proveedores con la gestión de la información y el conocimiento, asegurando el cumplimiento de los criterios definidos y la mejora continua de nuestros procesos y del sistema de gestión de la seguridad de la información.

### Roles y Responsabilidades

La Junta Directiva, a través de esta política, establece las bases para el uso estratégico y responsables de la información, el conocimiento y la inteligencia artificial en la organización. Este marco sólido de gobernanza permite la gestión efectiva de los riesgos asociados a su uso, promoviendo la innovación y la eficiencia operativa asegurando el cumplimiento de las regulaciones y mejores prácticas de seguridad.

Todos los colaboradores de la organización son responsables de la aplicación de esta política en su ámbito de actuación acorde con los modelos de gestión, normatividad interna y protocolos definidos para tal fin.

Cuando se realicen cambios en la estructura o de roles, cada empleado es responsable de entregar la documentación y sus responsabilidades correspondientes. Adicionalmente, el directivo deberá gestionar la actualización de los perfiles de accesos lógicos, de acuerdo con los procedimientos establecidos.



Esta información pertenece a XM S.A E.S.P. y es para uso exclusivo del destinatario intencional. Esta comunicación puede contener información reservada o de acceso privilegiado. Si usted ha recibido esta información por error, equivocación u omisión favor notificar en forma inmediata al remitente y eliminar dicha información o mensaje con sus anexos. La utilización, copia, impresión, retención, divulgación, reenvío o cualquier acción tomada sobre este mensaje y sus anexos queda estrictamente prohibida y puede ser sancionada legalmente.



XM es responsable de valorar, clasificar y determinar el tratamiento de la información considerando, entre otras, sus características de confidencialidad, integridad y disponibilidad y la gestión de los riesgos asociados con la protección de la información y el conocimiento.

DocuSigned by:

*Maria Nohemi Arboleda*

8C5FE3FDBEBC4CE

**MARIA NOHEMI ARBOLEDA ARANGO**

Gerente General

VERSIÓN ACTUAL	FECHA DE REVISIÓN	DESCRIPCIÓN DE CAMBIOS	RESPONSABLE ELABORACIÓN	RESPONSABLE APROBACIÓN
01	2015/04/24	Aprobación de la política de acuerdo con el acta 125 de la reunión de la Junta Directiva Ordinaria.	Equipo de Diseño Organizacional	Ana Mercedes Restrepo Múnera
02	2020/08/26	Cambia a versión 02, se realiza actualización de las declaraciones y se incluye roles y responsabilidades. Aprobación de la política de acuerdo con el acta 204 del 27 de enero de 2021 en reunión con la Junta Directiva Ordinaria.	Equipo de Diseño Organizacional	Ana Mercedes Restrepo Múnera
03	2022/01/03	Cambia a versión 03, se realiza actualización de las declaraciones y se incluye roles y responsabilidades. Aprobación de la política de acuerdo con el acta 37 del 29 de noviembre de 2021 en reunión extraordinaria de asamblea General de accionistas.	Equipo de Diseño Organizacional	Juan Camilo Arbeláez Zapata (Encargado)
04	2024/06/19	Cambia a versión 04, se realiza actualización general de la política de información y se incluyen los objetivos de seguridad de la información y se complementan los requisitos de la norma ISO 27001:2022. Aprobación de la política de acuerdo con el acta 251 del 31 de julio 2024 en reunión con la Junta Directiva Ordinaria.	Equipo de Seguridad de la información.	Lina María Betancur Peña (Encargada)
05	2025/03/14	Cambia a versión 05, se incorpora en las declaraciones referentes al tema de inteligencia artificial. Aprobación de la política realizada en sesión de Junta Directiva No. 260 del 26 de marzo de 2025.	Equipo de Seguridad de la información	Ana Mercedes Restrepo Múnera