

Instrucción sobre Privacidad y uso responsable de IA

1. Resumen

El Grupo Securitas tiene valores sólidos y comparte un gran sentido de responsabilidad hacia los clientes, empleados y comunidades: Ayudamos a hacer de su mundo un lugar más seguro. La presente *Instrucción sobre privacidad y uso Responsable de inteligencia artificial (IA)*, establece la estrategia y el compromiso de privacidad, protección de datos y uso responsable de la IA de Securitas.

El director general del grupo emitirá directivas o instrucciones adicionales sobre el procesamiento de datos personales y el uso responsable de la IA cuando corresponda. Las Instrucciones publicadas en virtud de dicha Política de privacidad e IA responsable, no limitan los requisitos de la Política del Grupo, sino que brindan más detalles en relación con la puesta en práctica de los requisitos en el país.

Esta Instrucción establece la adaptación de la Política emitida por el Grupo, y su aplicación por todos los empleados de Securitas Uruguay. Además de esta instrucción, se deberán cumplir con todas las leyes y regulaciones locales con respecto a la protección y el procesamiento de datos personales y las regulaciones y estándares aplicables con respecto al uso responsable de la IA. En la medida en que la Política del Grupo entre en conflicto con cualquier ley o reglamento local, prevalecerá la ley o reglamento local.

Resumen de los principales cambios desde la última revisión:

Sin cambios.

2. Principios de privacidad y protección de datos

En Securitas, nos comprometemos a salvaguardar la privacidad de nuestros clientes, empleados y cualquier persona física con la que interactuamos. En este sentido, nos comprometemos con los siguientes principios:

Transparencia: ser transparentes sobre cómo recopilamos y utilizamos los datos personales.

Legalidad y equidad: los datos deben procesarse donde exista una base legal y con un propósito comercial claro.

Minimización de datos: solo se deben procesar los datos necesarios, evitando la recopilación o retención excesiva.

Seguridad e integridad: las medidas adecuadas deben proteger los datos de pérdidas, accesos no autorizados o usos indebidos.

Respeto de los derechos: respete los derechos otorgados por los acuerdos contractuales y las leyes de privacidad y protección de datos aplicables.

Responsabilidad: cada entidad de Securitas debe demostrar el cumplimiento de las leyes de privacidad y las políticas internas y será responsable y debe ser capaz de demostrar el cumplimiento de los principios de esta Política de privacidad.

3. Principios de IA responsable

En Securitas, nos dedicamos al uso responsable de la IA en consonancia con nuestros valores fundamentales y normas éticas. Nos comprometemos con los siguientes principios:

Privacidad y Transparencia.

- Garantizar la confianza, la transparencia y la integridad en las soluciones de IA proporcionando información clara y precisa sobre los métodos, procesos y resultados de IA.
- Respetar la privacidad de los clientes, empleados y el público recopilando, utilizando y compartiendo datos que sean relevantes, necesarios y legales.



Igualdad y justicia.

- Promover la igualdad y la equidad mitigando los prejuicios, la discriminación o el daño en las soluciones de IA.
- Garantizar que las soluciones de IA sean inclusivas, accesibles y respetuosas con la diversidad y la dignidad humana.

Calidad de los datos y mitigación de sesgos.

- Mantener la vigilancia en el monitoreo y la mejora de la calidad de los datos en las aplicaciones de IA.
- Implementar un marco sólido de gobernanza de datos para garantizar la precisión, integridad y relevancia de los datos.

Seguridad y protección.

- Utilizar o desarrollar soluciones de IA que sean sólidas, resistentes y capaces de funcionar de forma fiable y coherente.
- Implementar medidas de seguridad para proteger los sistemas de IA del acceso no autorizado, la manipulación o el uso indebido.

Innovación y valor empresarial.

- Aprovechar el poder de la IA responsable para desbloquear la innovación y el valor empresarial tangible.
- Utilizar soluciones impulsadas por IA para elevar nuestras entregas internas a las partes interesadas.
- Mantenerse al día con los desarrollos técnicos y su impacto en nuestro negocio.

La 12.1 Instrucciones sobre Privacidad y uso Responsable de Inteligencia Artificial (IA), describe con más detalle los requisitos específicos y la orientación relacionada con la inteligencia artificial responsable.

4. Aplicabilidad

Esta Instrucción sobre privacidad e IA responsable se aplica a todos los empleados de Securitas Uruguay. La misma se comunicará e implementará, en la mayor medida posible, en todas las asociaciones comerciales (incluidos los socios de empresas conjuntas) y las relaciones contractuales de consultores.

5. Implementación y Responsabilidad

5.1. Privacidad de datos

Es responsabilidad de la función de Cumplimiento de Ética Empresarial proporcionar un marco a seguir para garantizar que gestionan adecuadamente los riesgos de privacidad en el negocio. Es responsabilidad del Gerente General, con sus asesores generales, garantizar que los requisitos de privacidad de esta instrucción (así como los requisitos de las leyes pertinentes) se implementen plenamente en el país. Esto implica la responsabilidad de:

Implementar los requisitos de privacidad de datos en los procesos (instrucciones y procedimientos), incluida la garantía de que se actualicen según sea necesario para reflejar cualquier cambio en las leyes, así como cambios en la Política definida por el Grupo.

Asignar aquellos recursos que se consideren necesarios para garantizar que los requisitos de esta Instrucción sean coordinados e implementados. Esto incluirá implementación de los procesos funcionales necesarios para, por ejemplo, recursos humanos, comunicaciones, asuntos legales, TI, ventas, Tecnología y propietarios de funciones de compras para garantizar que los proveedores y subcontratistas cumplan con nuestras políticas.

Garantizar que todas las personas relevantes estén capacitadas en los requisitos de la Política y las leyes aplicables en materia de procesamiento de datos personales, que deben revisarse periódicamente facilitar el asesoramiento sobre privacidad de datos a los empleados.

Es responsabilidad de todos los empleados del Grupo Securitas conocer y cumplir esta Instrucción.

5.2. IA responsable

Los principios de IA responsable son obligatorios para todas las entidades de Securitas y cada entidad que desarrolle u obtenga el derecho a utilizar soluciones de IA deberá, como mínimo, poder demostrar que cumple con los principios



o, si corresponde, con los requisitos legales, los compromisos con los clientes o los estándares de la industria. Sin embargo, se anima a todas las entidades de Securitas a esforzarse por alcanzar los más altos estándares de uso ético y responsable de la IA. Los principios reflejan nuestros valores fundamentales de integridad, vigilancia y ayuda, así como nuestro compromiso de respetar los derechos humanos y proteger los datos personales.

Es responsabilidad de la función de Cumplimiento de Ética Empresarial desarrollar un marco basado en los principios que todas las funciones globales comunes, las Divisiones, Unidades de Negocio y Países deben seguir para garantizar que gestionan adecuadamente los riesgos éticos de la IA en sus negocios.

Es responsabilidad del Gerente General de Securitas Uruguay, junto con la Directora de Legal, Riesgos y Cumplimiento, garantizar que Securitas Uruguay cumpla con los requisitos establecidos por la Política del Grupo, y las leyes locales en la materia.

6. Capacitación

Es responsabilidad de la Gerencia General, garantizar que se proporcione la formación adecuada periódicamente a todos los empleados pertinentes sobre *Privacidad de Datos e IA Responsable* de acuerdo con esta Instrucción 12. de *Privacidad y uso Responsable de Inteligencia Artificial (IA)*.

7. Informes y consecuencias de incumplimiento

Todos los empleados de Securitas deben informar cualquier sospecha de comportamiento inadecuado contrario a esta instrucción a su superior inmediato o, cuando esto no sea posible, al superior del superior, o “el defensor del empleado”, o al Director/a de Legal, Riesgos y Cumplimiento, o su equipo directo local, o al Director/a de Gestión Humana, o al Jefe/a de selección y desarrollo de personal o su equipo directo. Dichos canales serán accesibles a todo el personal, pudiendo recibir a demás consultas y denuncias vinculadas a inequidades de género, acoso sexual, acoso laboral, violencia doméstica, otras formas de discriminación. Ningún empleado sufrirá consecuencias negativas por cumplir con esta Instrucción, incluso si dicho cumplimiento resulta en la pérdida de negocios. Todos los eventos o sospechas reportados serán investigados de forma independiente y confidencial, y se les dará seguimiento, asegurando la trazabilidad en todos los casos, así como el registro y análisis estadístico de denuncias y consultas vinculadas a discriminación, con el fin de identificar oportunidades de mejora.

Si una persona denunciante no desea, o no puede, informar de una sospecha a su superior inmediato o a otro funcionario dentro de la organización, esa persona deberá Informar del problema a través de la Línea de Integridad de Securitas en <https://securitas.integrityline.com/> o Vía Correo electrónico a integrity@securitas.com.

Cualquier violación de esta instrucción o de las leyes locales aplicables dará lugar a medidas disciplinarias, que pueden incluir la terminación del empleo.

9 Revisión y seguimiento

El cumplimiento de esta Política por parte de todas las Empresas y Empleados de Securitas será monitoreado como parte del programa de cumplimiento de Ética Empresarial, así como mediante auditorías internas y externas y un seguimiento rutinario de todos los asuntos reportados que requieran resolución.