TRIGO es consciente de que el procesamiento de información es clave para prestar sus servicios y que debe mantenerse la seguridad y protección de la información recopilada, manejada y compartida. Nuestra dirección está comprometida no solo a garantizar el cumplimiento de los requisitos aplicables (legales, regulatorios y de clientes, proveedores, empleados y otras partes interesadas), sino también a mejorar continuamente el sistema de gestión para garantizar la disponibilidad, integridad y confidencialidad de la información sensible.

Para ello, nos esforzamos por:

- Identificar y gestionar riesgos y oportunidades de seguridad de la información.
- Sensibilizar a los empleados sobre los riesgos y desarrollar una cultura de seguridad de la información mediante formaciones, comunicaciones y el intercambio de lecciones aprendidas para mantener a cada empleado de nuestra organización al día con las mejores prácticas de seguridad.
  - → TRIGO pretende garantizar para finales del 2027 que al menos el 90% de sus empleados hayan recibido formación en ciberseguridad.
- Proteger los datos personales en cumplimiento de nuestro deber legal.
- Desplegar y mantener infraestructuras y sistemas digitales de IT estables, seguros y altamente disponibles, apoyados por una estrategia integral de ciberseguridad, que incluye el control de procesos externalizados.
- Detectar, informar y responder eficazmente a incidentes de seguridad de la información.
- Desplegar y mantener infraestructuras y sistemas digitales de IT estables, seguros y altamente disponibles, apoyados por una estrategia integral de ciberseguridad, que incluye el control de procesos externalizados.
- Monitorizar continuamente nuestro entorno informático mediante una combinación de herramientas internas de monitorización y plataformas externas de cibervaloración que proporcionan visibilidad continua sobre nuestra exposición a vulnerabilidades y amenazas.
  - → TRIGO pretende mantener una calificación mínima de ciberseguridad de 750 sobre 1000, medida por plataformas independientes de clasificación cibernética, reflejando un control sólido sobre su superficie externa de ataque y un esfuerzo continuo para identificar y remediar vulnerabilidades.
- Realizar auditorías de seguridad periódicas para garantizar la eficacia de los controles implementados y promover la mejora continua.
- Probar y mantener los planes de recuperación ante desastres para nuestros sistemas informáticos operativos.

Esta política es redactada por el director de Seguridad de la Información en coordinación con el Responsable de Protección de Datos del Grupo y aprobada por el CEO y el subdirector. Esta política está respaldada por varias políticas, procesos y recursos para garantizar su implementación.

Se aplica a todas las entidades de TRIGO en todo el mundo, incluidos todos los empleados, contratistas y terceros que accedan a los sistemas de información de TRIGO.

Su implementación se basa en un modelo de responsabilidad compartida:

- La función de IT del Grupo es responsable de definir, desplegar y mantener infraestructuras globales de IT, medidas de ciberseguridad, actividades de monitorización y capacidades de recuperación ante desastres.
- Las entidades y usuarios locales son responsables de cumplir con las normas definidas, proteger los activos de información y contribuir a la gestión de riesgos e incidentes de seguridad de la información.

Por lo tanto, aunque algunos controles se gestionan de forma centralizada a nivel de Grupo, el director general de cada entidad es responsable de la correcta aplicación de esta política dentro de su ámbito.

El Grupo también promueve la mejora continua mediante el seguimiento de indicadores relevantes e implementación de acciones correctivas cuando sea necesario.

Esta política está sujeta a una revisión anual como parte del proceso de Revisión de Gestión. Esta revisión tiene en cuenta cuestiones internas y externas, eventos e impactos significativos en la seguridad, así como la dirección estratégica del Grupo, para garantizar la relevancia, eficacia y mejora continua de la política.

Confiamos en que todos nuestros empleados adopten los comportamientos adecuados y contribuyan a la mejora de nuestras prácticas de seguridad escalando ideas de mejora.

Matthieu RAMBAUD
CEO

Benoît LEBLANC
Deputy CEO

Versión #	Fecha de aplicabilidad (dd/mm/aa)	Página(s)	Descripción del cambio
A	07/15/26	Todas	El contenido inicialmente incluido en las relaciones públicas de los documentos. TÍO. WW.09.EN-A Seguridad de la información (versión del 3 de abril de 2023). Este nuevo documento también introduce objetivos cuantitativos.