Información corporativa
Política de seguridad

Índice

Control de documentos

Índice

Control de documentos

Nombre del documento	Política corporativa de seguridad de la información
Clasificación	INTERIOR
Número de revisión	3.5
Fecha de revisión	05/12/2024
Custodio	Responsable de seguridad de la empresa
Aprobación	Foro Insights IS
Auditoría	Anual: Enterprise Security Manager
Siguiente revisión	Diciembre de 2025

1. Visión general

Esta política se basa en la norma ISO 27001:2022, norma internacional reconocida para la seguridad de la información. Esta norma garantiza que los Insights cumplen los siguientes principios de seguridad:

Confidencialidad Toda la información sensible estará protegida contra el acceso o la divulgación no autorizados.

Integridad Toda la información estará protegida de alteraciones o destrucciones accidentales, malintencionadas y fraudulentas; y,

Disponibilidad Los servicios de información estarán disponibles durante todo el horario acordado con los usuarios y estarán protegidos contra daños accidentales o malintencionados o denegación de servicio.

2. Propósito

El propósito de esta política es demostrar el compromiso que Insights Learning and Development tiene con la seguridad de los datos de los que es responsable y demostrar los controles y responsabilidades existentes para apoyar el Sistema de Gestión de Seguridad de la Información, SGSI, que tiene como marco principal la norma ISO 27001:2022.

3. Alcance

El alcance de esta política abarca a todas las partes internas y externas y respalda el compromiso continuado de Insights con la norma ISO 27001:2022.

4. Política

4.1 Responsabilidades del Ejecutivo

El Ejecutivo de Insights se compromete a satisfacer todos los requisitos aplicables dentro de esta política y a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), por lo que ha establecido esta política de seguridad de la información para que:

- se adecue al objetivo de Insights;
- incluye objetivos de seguridad de la información y proporciona el marco para establecer objetivos continuos de seguridad de la información.

Esta política de seguridad de la información estará disponible como información documentada; se comunicará dentro de Insights; y estará a disposición de las partes interesadas, según proceda.

El cumplimiento de esta política y de todas las demás políticas y procedimientos de seguridad es obligatorio para todo el personal.

El CEO aprueba esta política. El Foro de Seguridad de la Información es responsable de garantizar la aplicación y el cumplimiento de la política en todas las actividades incluidas en el ámbito del SGSI.

4.2 Liderazgo y compromiso

El Ejecutivo seguirá demostrando su liderazgo y compromiso con respecto al SGSI:

- garantizar que la política de seguridad de la información y los objetivos de seguridad de la información se establecen y son compatibles con la dirección empresarial estratégica de Insights;
- garantizar la integración de los requisitos del SGSI en los procesos de Insights;

- garantizar la disponibilidad de los recursos necesarios para el SGSI;
- comunicar la importancia de una gestión eficaz de la seguridad de la información y de ajustarse a los requisitos del SGSI;
- garantizar que el SGSI logre los resultados previstos;
- dirigir y apoyar a las personas para que contribuyan a la eficacia del SGSI;
- Promover la mejora continua y ayudar a otros directivos a demostrar su liderazgo en sus ámbitos de responsabilidad.

4.3 Objetivos de seguridad de la información

Los objetivos de seguridad de la información se han establecido y son compatibles con la dirección estratégica de Insights, el objetivo clave es trabajar en línea con las secciones de la norma de buenas prácticas ISO 27001:2022 que se detallan a continuación.
Además, los objetivos de seguridad serán fijados por el Foro de Seguridad de la Información como tarea permanente y en las reuniones de revisión de la gestión del SGSI.

4.4 Mejora continua del marco del SGSI

Insights tratará de mejorar continuamente el sistema de gestión de la seguridad de la información de acuerdo con un enfoque PLANIFICAR-HACER-VERIFICAR-ACTUAR para mejorar los procesos integrados en su SGSI.

La importancia que se concede a la seguridad de la información queda demostrada por la existencia del Foro de Seguridad de la Información

- revisar y avanzar en cuestiones de seguridad estratégica;
- establecer relaciones fuera de Insights con otros asesores de seguridad;
- evaluar el impacto de los nuevos requisitos legales o reglamentarios que se nos impongan;
- supervisar la eficacia del SGSI, por ejemplo, a partir de los resultados de los informes de auditoría interna y de los informes sobre incidentes de seguridad;
- recomendar/aprobar cambios en el SGSI.

El Foro de Seguridad de la Información se reúne periódicamente para abordar las actividades anteriores con el fin de garantizar la eficacia continua del SGSI de Insights. El proceso de revisión se define en la "Política de revisión de la gestión del Foro de Seguridad de la Información".

Esta Política Corporativa de Seguridad de la Información confirma el compromiso de Insights con la mejora continua y destaca las áreas clave (denominadas "temas") para asegurar eficazmente su información, a saber:

- Controles organizativos
- Controles de personas
- Controles físicos
- Controles tecnológicos

4.5 Controles organizativos

Los controles organizativos son responsabilidad del Foro de Seguridad de la Información y abordan las siguientes áreas:

- Políticas estratégicas de seguridad de la información - que abarca la presente política, la política de objetivos de seguridad y la política de comunicaciones.
- Funciones y responsabilidades: el Director de Seguridad de la Empresa preside el Foro de Seguridad de la Información.
- Gestión de identidades y accesos: el director de seguridad de la empresa y los jefes de equipo son responsables de establecer y mantener sólidos controles lógicos de acceso. Existe una política adecuada que debe cumplir todo el personal y las partes externas.
- Gestión de activos - La información de Insights debe clasificarse en función de su sensibilidad y se le debe asignar un propietario de la información. Enterprise Security Manager mantendrá un inventario de activos de información que se actualizará periódicamente, en función de su perfil de riesgo, y se protegerá en consecuencia.
- Relaciones - Los requisitos de seguridad de la información para mitigar el riesgo asociado con el acceso del proveedor a los activos Insights deben acordarse con el proveedor y documentarse.
- Los acuerdos con los proveedores de la nube deben establecerse, documentarse y someterse a

una revisión continua.

- Gestión de incidentes - Los registros de gestión de incidentes de seguridad deben mantenerse, actualizarse y supervisarse de forma centralizada y continua. Todos los empleados deben ser conscientes de lo que constituye un incidente de seguridad real o potencial, cómo notificar el incidente y a quién notificar el incidente. La responsabilidad de la supervisión de todos los incidentes de seguridad recae en el Director de Seguridad de la Empresa.
- Gestión de la continuidad del negocio - Los insights deben garantizar un enfoque coherente y eficaz de la gestión de los principales incidentes de seguridad de la información, incluida la comunicación sobre los sucesos y deficiencias de seguridad y las implicaciones para la gestión de la continuidad del negocio.

- Cumplimiento - Insights debe evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad. Insights debe tomar medidas técnicas y organizativas para proteger los datos personales contra la destrucción accidental o ilegal, o la pérdida o alteración accidental, y la divulgación o el acceso no autorizados. En particular, Insights debe tomar medidas destinadas a garantizar que:

    - Toda persona que gestione y maneje datos personales entiende que es responsable contractualmente de seguir unas buenas prácticas de protección de datos.
    - Todas las personas que gestionan y tratan datos personales han recibido la formación adecuada para hacerlo.
    - Todas las personas que gestionan y tratan datos personales están debidamente supervisadas.

4.6. Controles de personas

Los Controles de Personas son responsabilidad del Equipo de Recursos Humanos y abordan las siguientes áreas:

- Todos los empleados deben suscribir el Manual del Empleado, que les obliga a trabajar de acuerdo con todas las políticas y procedimientos, incluidos los requisitos específicos de seguridad de la información.
- Una política de seguridad de la información personal garantiza que los empleados sean conscientes de que están obligados a seguir las mejores prácticas en materia de seguridad de la información.
- También existe un procedimiento para que todos los empleados que abandonan Insights (incluidos los empleados temporales y contratados) desactiven su cuenta de red y recuperen todos los objetos de su propiedad.
- Todos los nuevos empleados (permanentes, temporales y contratistas) deben recibir formación sobre los procedimientos en las áreas descritas anteriormente como parte de su programa de iniciación. La formación continua se impartirá en forma de un programa de actualizaciones periódicas y sesiones de formación a cargo del Foro de Seguridad de la Información.

4.7 Controles físicos

Los controles físicos son responsabilidad del Equipo de Instalaciones y abordan las siguientes áreas:

- El personal debe conocer y seguir el conjunto detallado de medidas, controles y procedimientos que existen para garantizar un control adecuado de la seguridad física. Entre ellos figuran:

    - sistemas de alarma y circuito cerrado de televisión en edificios
    - acceso restringido al edificio y acceso aún más restringido dentro del mismo
    - taquillas, cajones, cajas fuertes y almacenes seguros, almacenamiento ignífugo
    - copias de seguridad externas y archivado seguros
    - escritorio despejado y pantallas despejadas
    - procedimientos para la emisión de cualquier medio de comunicación
    - la necesidad de un control permanente de todas las medidas de seguridad física

4.8. Controles tecnológicos

Los controles tecnológicos son responsabilidad del Equipo de Tecnología y Seguridad de la Empresa y abordan las siguientes áreas:

- Todos los dispositivos de punto final deben estar adecuadamente protegidos y cifrados cuando proceda.
- Gestión de identidades y accesos: los administradores de sistemas informáticos (usuarios privilegiados) se aseguran de que los controles y procedimientos de acceso acordados se gestionan conforme a la política establecida.
- Criptografía - Cuando los Insights emplean controles criptográficos, se ha desarrollado e implantado una política sobre el uso de controles criptográficos para la protección de la información.
- Seguridad de las operaciones de TI - Insights garantizará el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información. El Equipo de Tecnología y Seguridad de la Empresa realiza un seguimiento continuo de todas las actividades operativas de TI.
- Seguridad de las comunicaciones informáticas: el personal debe ser consciente de que el uso de la tecnología y las comunicaciones está establecido, controlado y gestionado por el Responsable de Seguridad de la Empresa. Él es el responsable de garantizar que se aplican las medidas y procesos de seguridad adecuados. Insights garantizará que la seguridad en torno a la red, los terminales y el trabajo a distancia estén adecuadamente protegidos.
- Seguridad en el desarrollo de sistemas informáticos: el responsable de seguridad de la empresa vela por que se incluyan en todos los proyectos los procesos de seguridad de la información adecuados de . Se aplica un enfoque de desarrollo seguro que incluye la política, los procedimientos, el entorno y las pruebas.

4.9. Período de revisión de la política

El Foro sobre Seguridad de la Información revisará esta Política al menos una vez al año.

5. Cumplimiento de la política

Medición del cumplimiento: El Equipo de Seguridad y/o el Foro de Seguridad de la Información verificarán el cumplimiento de esta política a través de diversos métodos, incluidos, entre otros, visitas periódicas, vigilancia por vídeo, informes de herramientas de negocio, auditorías internas y externas, e información al propietario de la póliza.

Excepciones: Cualquier excepción a esta política debe ser aprobada a través del Custodio y Aprobador de la política. En ausencia, como las vacaciones anuales, recaerá en la responsabilidad de un miembro del Cuerpo de Custodia y/o Responsables jerárquicos o Foro de Seguridad de la Información

Incumplimiento: Un empleado que haya infringido esta política, que afecte a la reputación de Insights Aprendizaje y Desarrollo o el Grupo Insights en general podrán ser objeto de medidas disciplinarias, que podrán llegar hasta incluido el despido.

6. Normas, políticas y procesos relacionados

Artículo	Int o Ext	Título del documento
1	Interno	Sistema de gestión de documentos SGSI
2		
3		
4		
5		
6		

7. 7. Definiciones y términos

No aplicable

8. Historial de revisiones

Revisión	Fecha	Modificado por	Descripción

2.0	09/01/2020	Graham Watson	Política aprobada por el Director General
2.1	24/09/2021	Kevin McAuley	Cambios menores basados en cambios de funciones y estructura
3.0	30/11/2021	Kevin McAuley	Política aprobada por el Comité Ejecutivo
3.1	13/02/2023	Dave McClure	Actualización de políticas añadiendo nuevas políticas
3.2	06/03/2023	Dave McClure	Funciones y responsabilidades trasladadas a la nueva política
3.3	05/04/2023	Ian Gowen	Añadida tabla de referencias internas
3.4	28/04/2023	Ian Gowen	Cambiado el orden de las Referencias Internas
3.5	05/12/2024	Andy Moore	Revisión anual y aprobación del Director General

Firmado: 

Fecha: 5th Diciembre 2024

Fiona Logan
Consejero Delegado