Política General de Seguridad de la Información

Este documento contiene información clasificada de acuerdo con lo indicado en "Clasificación" y es de propiedad de ISecurity.

De utilizar el documento, verifique que corresponda a la versión actualizada. Cualquier otra versión no es válida. Respete las restricciones asociadas a la clasificación y no reproduzca partes o el total del documento a menos que obtenga una autorización formal de ISecurity.

CONTROL DE VERSIONES				
Versión	**Fecha Publicación**	**Autor**	**Aprobador**	**Cambios efectuados**
1.0	07-06-2023	Oficial de Seguridad de la Información	Comité de Seguridad de la Información	Versión Inicial para SGSI
2.0	01-09-2023	Oficial de Seguridad de la Información	Comité de Seguridad de la Información	Incorporación de nuevos capítulos
3.0	20-10-2023	Oficial de Seguridad de la Información	Comité de Seguridad de la Información	Se mejora la redacción
4.0	14-05-2025	AYM Advisory	Comité de Seguridad de la Información	Cambio de formato y actualización del documento
5.0	09-05-2025	AYM Advisory	Comité de Seguridad de la Información	Versión aprobada en Comité de Seguridad de la Información, se publica en Intranet
6.0	28-01-2026	Oficial de Seguridad de la Información	Comité de Seguridad de la Información	Se incorpora una cláusula que establece el rol de ISecurity como OIV y la responsabilidad vinculada a su nombramiento.
7.0	26-05-2026	Oficial de Seguridad de la Información	Comité de Seguridad de la Información	Se explicitan objetivos, se quita el apartado “Declaraciones iniciales”, se incorporan nuevas directrices, se incorpora ISO42001

Directrices

1. La Información es un bien valioso y los Sistemas de Información son activos críticos para ISecurity.
2. Se define la Seguridad de la Información como toda acción que busque proteger la integridad, disponibilidad, confidencialidad de la información y la privacidad de los datos personales.
3. Se reconoce la Seguridad de la Información como un atributo indispensable en los servicios brindados por ISecurity.
4. La Información debe ser protegida de una manera adecuada, de acuerdo con su sensibilidad y criticidad.
5. De esta directriz se desprende un conjunto de Políticas de Seguridad de materias específicas y sus respectivas herramientas de implantación.
6. La Seguridad de la Información y los recursos asociados, son responsabilidad de todos los colaboradores internos y externos a la organización.
7. Todo colaborador de ISecurity, debe acceder exclusivamente a la Información que le sea estrictamente necesaria y debidamente autorizada, para cumplir sus funciones.
8. Todo colaborador de ISecurity tiene la obligación de notificar cualquier actividad o situación que afecte o pueda afectar la Seguridad de los activos de Información.
9. La organización establece el compromiso de informar a la Agencia Nacional de Ciberseguridad, los incidentes de seguridad de la información y ciberseguridad, en los términos y plazos que establece el Reglamento de Reporte de Incidentes de Ciberseguridad estableciendo mecanismos para su detección, reporte y gestión.
10. Establecer y mantener un proceso sistemático de gestión de riesgos de seguridad de la información.
11. Gestionar los accesos a la información bajo el principio de mínimo privilegio, asegurando que los usuarios cuenten únicamente con los permisos necesarios para el desempeño de sus funciones.
12. Los proveedores y terceros que accedan a la información deberán cumplir con los requisitos de seguridad establecidos por la organización.
13. Toda la información deberá ser clasificada de acuerdo con su nivel de sensibilidad y criticidad.
14. La organización reconoce que la sensibilización, capacitación y entrenamiento adecuados a sus colaboradores en las materias de seguridad de la información son tareas prioritarias.
15. La organización adhiere a la norma ISO/IEC 27001 para la implantación de un Sistema de Gestión de Seguridad de la Información, destinado a reducir de manera efectiva y permanente el riesgo para la Información. Así mismo Isecurity se adhiere a ISO/IEC 42001 adoptando las mejores prácticas en materia de Inteligencia Artificial
16. La organización se compromete a mejorar continuamente el Sistema de Gestión de Seguridad de la Información, proporcionar los recursos y formación que sean necesarios para la implementación y mantenimiento de este sistema.
17. El incumplimiento de la presente política y, sobre todo, la ejecución de alguna de las conductas prohibidas en las políticas específicas de seguridad de la información puede derivar en sanciones, según lo indicado en el Reglamento de Orden, Higiene y Seguridad.
18. La presente política será revisada al menos una vez al año y cada vez que se produzcan cambios significativos en el SGSI. Toda actualización deberá ser evaluada y aprobada por la Alta Dirección.