POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ESTADO DE REVISIÓN/MODIFICACIÓN DEL DOCUMENTO

N.º EDICIÓN	Fecha	Naturaleza de la Revisión
00	08/06/2020	Edición inicial
01	11/05/2021	Modificación de versión del SOA
02	13/10/2022	Adecuación de las políticas al Real Decreto 311/2022, de 3 de mayo, por El que se regula el Esquema Nacional de Seguridad (ENS) en su nivel medio.
03	05/1/2024	Actualización a ISO 27001:2022
04	30/01/2025	Separación de la política de calidad y medioambiente

1. OBJETO, APROBACIÓN Y ENTRADA EN VIGOR

El objeto de este documento es integrar, establecer y revisar la POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN de ECOSISTEMAS VIRTUALES Y MODULARES, S.L. (en adelante EVM). En especial ésta última, definidas a través del SOA y del mapa de riesgos de la organización.

EVM depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad [D], autenticidad [A], integridad [I], confidencialidad [C] y trazabilidad [T] uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 y 8 del ENS.

2. POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE EVM

Para ello EVM adquiere los siguientes compromisos:

En **general**:

- Mejora continua del desempeño tanto de los sistemas de gestión como del resultado a obtener.
- Mejora de la eficacia de los sistemas.
- Actualización y cumplimiento del marco legal y de los requisitos propios y específicos que nos puedan poner tanto nuestros clientes como los proveedores y personas implicadas.
- Mantener un alto nivel de cualificación y talento para poder ser eficaces y eficientes en los procesos.
- Mantenimiento de los adecuados canales de comunicación con todas las partes interesadas, con objeto de asegurar su satisfacción con respecto al cumplimiento de sus necesidades, requisitos y expectativas
- Se adoptarán las medidas necesarias para que todo el personal de EVM sea conocedor de esta política. Difundiéndose también ésta a los proveedores y colaboradores, estando además a disposición del público a través de la página web.

En **seguridad de la información según ISO 27001:2022**:

- Política de Disminución del riesgo potencial grave. Se priorizarán las actuaciones sobre riesgos potenciales graves.
- Política de Tolerancia 0 con las incidencias. Se investigará y sancionará aquellas actuaciones dolosas o imprudentes.
- Política de impacto reputacional mínimo. La incidencia reputacional en materia de seguridad debe tender a 0.
- Controlar operacionalmente de forma eficaz las amenazas y riesgos sobre el activo y las instalaciones.
- Gestionar eficientemente las incidencias que afecten a la integridad, disponibilidad y confidencialidad de la información de la empresa.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información

- Implantar planes de continuidad del negocio que garanticen la permanencia de las actividades de la sociedad en caso de incidencias graves o contingencias.

Y como compromiso con el cumplimiento de esta política firma la Dirección a 30 de enero de 2025.