POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fecha edición: 27/05/2025
Versión: 01

RESPONSABLE	REVISADO	APROBADO
Dpto. Plataforma Digital y Ciberseguridad	*Dpto. Control de Gestión y Gestión de Riesgos Dirección Tecnología y Digital*	*CEO*

CONTROL DE CAMBIOS

EDICIÓN	DESCRIPCIÓN DEL CAMBIO	ENTRADA EN VIGOR
Versión 1	Creación del documento.	27/05/2025

ÍNDICE

1. Objeto

Este documento refleja la Política de Seguridad de la Información de Ecoembes, fijando las directrices fundamentales para una gestión adecuada de la seguridad que garantice la protección de la información, los servicios y los recursos corporativos.

La necesidad de proteger estos activos responde a los siguientes factores:

- La obligación de garantizar la seguridad de la información, asegurando que el acceso, uso y custodia de los activos de información se alineen con los requisitos del negocio.
- El cumplimiento del marco legal vigente, así como de las políticas internas, normativas, procedimientos e instrucciones de seguridad, incluyendo las obligaciones derivadas del tratamiento de datos personales.
- La voluntad de reforzar el posicionamiento institucional Ecoembes, demostrando madurez en la gestión de riesgos tecnológicos y la confianza ante terceros.

Esta Política está alineada con la estrategia empresarial y la gestión de riesgos de Ecoembes y establece las bases para el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI). Se apoya en un proceso sistemático de apreciación de riesgos, que permite evaluar el impacto y la probabilidad de ocurrencia de las amenazas, facilitando decisiones coherentes sobre su tratamiento.

La Dirección de Ecoembes declara su compromiso firme con la protección de la información, asegurando que los objetivos de seguridad estén integrados en los procesos de negocio, y que los requisitos de seguridad sean identificados y aplicados de forma coherente en toda la organización.

Asimismo, la Dirección se compromete con la mejora continua del SGSI revisando su idoneidad, adecuación y eficacia, a través del análisis de:

- Oportunidades de mejora detectadas.
- Resultados del desempeño de la seguridad (no conformidades, auditorías, indicadores, cumplimiento de objetivos).
- Comentarios y expectativas de las partes interesadas.
- Cambios en el contexto interno y externo relevante para el SGSI.
- Resultados de la apreciación de riesgos y evolución del plan de tratamiento.

Para garantizar la efectividad del sistema, la Dirección dotará al SGSI de los recursos necesarios y apoyará activamente a todo el personal en la consecución de los objetivos establecidos.

2. Alcance y aplicación

El alcance de la Política de Seguridad de la Información se extiende a todo el Sistema de Gestión de Seguridad de la Información (SGSI).

Todas las áreas de la organización son responsables de promover, comunicar y facilitar el cumplimiento de esta Política, dotando de los recursos humanos, técnicos y económicos necesarios para su aplicación efectiva.

Esta Política es de obligado conocimiento y cumplimiento para todo el personal de Ecoembes, incluyendo empleados, dirección, proveedores y colaboradores externos que, directa o indirectamente, accedan, traten o gestionen información de la organización.

3. Referencias

- Cuerpo Normativo de Seguridad de la Información de Ecoembes.

4. Definiciones

Información

Datos que poseen significado, en cualquier formato o soporte. Se refiere a toda comunicación o representación de conocimiento.

Sistema de información

Se refiere a un conjunto de recursos relacionados y organizados para el tratamiento de información, según determinados procedimientos, tanto informáticos como manuales.

Seguridad de la información

Conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener las dimensiones de la misma.

5. Desarrollo

5.1. Principios

Ecoembes mantiene un compromiso firme con la seguridad de la información, entendida como un componente esencial de su actividad y de su responsabilidad corporativa. Este compromiso se manifiesta en la adopción de medidas que garanticen la protección de la información, los servicios, los procesos y los activos tecnológicos frente a todo tipo de amenazas.

En este contexto, la presente Política se sustenta en los siguientes principios:

- **Eficacia:** la información gestionada debe ser adecuada, relevante y útil para el cumplimiento de la misión de Ecoembes, contribuyendo a la toma de decisiones y a la generación de valor.
- **Eficiencia:** el procesamiento de la información debe realizarse optimizando recursos y reduciendo costes, apoyando una gestión ágil y sostenible.
- **Legalidad:** todas las actividades relacionadas con la información deben ajustarse al marco legal y normativo vigente. Ecoembes promueve el cumplimiento regulatorio, la protección de datos personales, la prevención del fraude y la integridad ética en su actuación.
- **Innovación:** se fomenta la mejora continua y la adopción de tecnologías seguras, que refuercen los controles existentes y mantengan a Ecoembes como un referente en su sector.

Los principios que deben respetarse, en base a las dimensiones básicas de la seguridad, son los siguientes:

- **Confidencialidad: l**a información solo debe estar disponible para aquellas personas debidamente autorizadas.
- **Integridad:** la información debe mantenerse completa, exacta y protegida frente a modificaciones no autorizadas.
- **Disponibilidad:** la información y los servicios deben estar accesibles cuando se necesiten, evitando interrupciones que afecten a la continuidad operativa.

5.2. Objetivos de seguridad de la información

La gestión de la seguridad de la información de Ecoembes se basa en el establecimiento, seguimiento y revisión periódica de objetivos de seguridad, en coherencia con el marco definido por el Sistema de Gestión de Seguridad de la Información (SGSI) y la estrategia general de la organización.

Los objetivos deben ser medibles, alcanzables, revisables y alineados con los requisitos aplicables, incluyendo los establecidos por la legislación vigente, las partes interesadas, las necesidades internas del negocio y los riesgos identificados en el análisis de riesgos.

De manera general, los objetivos estratégicos de seguridad de la información son:

- Contribuir desde la gestión de la seguridad al cumplimiento de la misión, visión y objetivos de Ecoembes, reforzando el posicionamiento institucional, y permitiendo ser referencia de gestión.
- Establecer las medidas de control necesarias que garanticen el cumplimiento de requisitos legales, normativos y regulatorios aplicables. En particular, toda la legislación relativa a la protección de datos de carácter personal, prestando especial atención al manejo de datos personales, la seguridad de comunicaciones y el intercambio de información.
- Minimizar el riesgo en las funciones más importantes de la entidad.
- Mejorar el servicio prestado a los clientes y terceros en términos de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información.
- Fortalecer la cultura de seguridad de la información en empleados.
- Asegurar la prestación continuada de los servicios.

5.3. Requisitos

Para garantizar una gestión eficaz de la seguridad de la información, Ecoembes establece un conjunto de requisitos mínimos que deben aplicarse en el desarrollo de sus las actividades, servicios y operaciones que impliquen el tratamiento de información o el uso de sistemas TIC:

- Establecer requerimientos de seguridad desde el diseño y por defecto.
- Prevención, detección, respuesta y conservación.
- Vigilancia continuada y reevaluación periódica.
- Diferenciación de responsabilidades.
- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión del personal.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Seguridad en la adquisición de productos y contratación de servicios.
- Mínimo privilegio.
- Integridad y actualización del sistema de información.
- Protección de la Información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.
- Seguridad en la cadena de suministro.
- Confiabilidad, seguridad y resiliencia.

La versión vigente del documento se encuentra disponible en el Área de Calidad en EcoStock; es responsabilidad del personal la comprobación de la vigencia de cualquier copia impresa antes de su uso, y la destrucción de la misma si está obsoleta.

Estos principios se aplican de forma transversal a toda la organización y son desarrollados mediante un marco normativo complementario, compuesto por normativas, procedimientos, instrucciones técnicas, guías y manuales, que permitirán alcanzar los objetivos definidos y asegurar un nivel de protección adecuado en cada ámbito.

Toda la documentación que integra el SGSI, se gestiona, estructura y conserva conforme a los procesos documentados que Ecoembes ha desarrollado teniendo en cuenta los estándares nacionales e internacionales que aplican en cada caso.

5.4. Organización de la seguridad de la información

Ecoembes establece una estructura organizativa basada en roles diferenciados y comités de seguimiento que facilita la toma de decisiones, la gestión del riesgo y los mecanismos de coordinación para garantizar una protección eficaz de los activos y el cumplimiento de los requisitos normativos y legales aplicables.

Los requisitos específicos sobre la asignación de funciones, así como la descripción de los distintos perfiles implicados en el SGSI, se desarrollan en el documento "Roles y responsabilidades".

5.5. Gestión de la Política de seguridad

La Política de Seguridad de la Información de Ecoembes, junto con su desarrollo normativo asociado, constituye el marco de referencia obligatorio que todas las áreas de la organización deben cumplir en el ámbito de sus competencias.

La gestión de esta política se rige por los siguientes principios:

- **Comunicación y accesibilidad**: La Política será comunicada a todas las personas que desempeñan funciones para Ecoembes, tanto internas como externas, y estará disponible para todas las partes interesadas pertinentes.
- **Difusión y formación**: Se establecerán mecanismos de formación, sensibilización y concienciación para asegurar la comprensión y aplicación de la Política por parte del personal.
- **Cumplimiento y seguimiento**: Se evaluará regularmente el cumplimiento de la política a través de auditorías, revisiones internas y otros mecanismos de supervisión.
- **Mejora continua**: La gestión de la política se integra en el ciclo de mejora continua, garantizando su adecuación, eficacia y alineación con los objetivos estratégicos de Ecoembes y el nivel de riesgo aceptado por la organización.
- **Aprobación y revisión**: La política será aprobada por Dirección y revisada al menos una vez al año o ante cambios relevantes en el entorno tecnológico, organizativo, normativo o en los resultados del análisis de riesgos.