Revisión	Fecha	Notas de la versión
A	**07/10/2022**	Revisión inicial

Documento aprobado por todas las funciones relevantes.

Guía de referencia rápida

¿Necesito leer esta Política?
Esta política define los principios de alto nivel de Ecenarro para gestionar los riesgos de seguridad de la información en la compañía.

Esta política debe ser cumplida por todos los empleados, terceros, proveedores, contratistas, subcontratistas y clientes de Ecenarro, si corresponde.

El cumplimiento de esta política es un requisito obligatorio, y garantizará que toda la información se trate de forma segura, y se gestione correctamente según su clasificación, y ante cualquier requisito legal y contractual.

¿Qué es la seguridad de la información y por qué es importante para Ecenarro?
La seguridad de la información es la práctica de proteger la información, los sistemas y los activos, mitigando los riesgos para la seguridad de la información.

Consiste en prevenir o reducir la probabilidad de acceso no autorizado o inadecuado, uso ilícito, divulgación, alteración, supresión, corrupción, modificación, inspección, registro o devaluación de la información, de los sistemas y de los activos.

La seguridad de la información se centra en proteger la confidencialidad, integridad y disponibilidad de la información, los sistemas y los activos.

No proteger adecuadamente a Ecenarro de los riesgos para la seguridad de la información que gestiona, podría afectar negativamente a la organización por:

- Pérdidas económicas por robos, fraudes y chantajes.
- Pérdida de producción o imposibilidad de operar/suministrar debido a la falta de disponibilidad de datos y sistemas informáticos.
- Imposibilidad de cumplir los requisitos contractuales de seguridad de la información del cliente.
- Incumplimiento de contrato u otra vulneración jurídica por deficiencias, carencias o pérdida de datos, incluida la propiedad intelectual.
- Daños a la reputación.
- Posibles incidentes de seguridad.

¿Dónde puedo encontrar más información sobre las normativas de seguridad de la información de Ecenarro?

Si necesita información adicional sobre la gestión de la seguridad de la información de Ecenarro, podrá consultar la intranet (BPM Quality Pro), donde encontrará toda la normativa de seguridad de la información de Ecenarro.

¿Qué hago si necesito más ayuda?

Si necesita más ayuda, póngase en contacto con el Responsable de Seguridad de la Información en motaegi@ecenarro.com o en xlesmes@ecenarro.com

1.0 Propósito

Ecenarro confía en la confidencialidad, integridad y disponibilidad de su información para alcanzar sus objetivos empresariales.

Cualquier deterioro de la confidencialidad, integridad o disponibilidad de la información, de los sistemas de TI o de los activos (de información) podría interrumpir las operaciones corporativas de Ecenarro, o exponer a Ecenarro a riesgos comerciales, contractuales o jurídicos.

Por lo tanto, Ecenarro debe aplicar normativas y procesos para identificar, evaluar y gestionar los riesgos de seguridad de la información a los que está expuesta, y mitigar estos riesgos a un nivel aceptable.

El propósito de esta política es establecer los siguientes objetivos de alto nivel para la seguridad de la información dentro de Ecenarro, los cuales se adaptan a los objetivos de la organización:

- Protección de la organización, de forma legal y conforme a la legislación y normativa vigente.
- Evaluación y gestión de las amenazas, vulnerabilidades y riesgos de seguridad de la información.
- Mantenimiento del compromiso de confianza de la compañía, con sus clientes y socios.

2.0 Alcance

Esta política se aplicará a:

- Todos los empleados, terceros, proveedores, contratistas, subcontratistas y clientes de Ecenarro, si corresponde.
- Todos los activos de Ecenarro, incluida la información, bases de datos, sistemas de TI, redes, aplicaciones y material, así como a todas las funciones empresariales, en todas las plantas.

3.0 Política

3.1 Objetivos de seguridad de la información

Esta Política de seguridad de la información define los requisitos para proteger la información, los sistemas y los activos de Ecenarro estableciendo un Sistema de Gestión de la Seguridad de la Información (SGSI).

El SGSI se basa en los requisitos del Trusted Information Security Assessment Exchange (TISAX), y en la norma internacional de seguridad de la información ISO 27001 para definir, controlar, supervisar, mantener y mejorar continuamente la seguridad de la información.

El SGSI garantiza:

- La Confidencialidad: garantizando que la información se revela únicamente a partes autorizadas;
- La Integridad: garantizando que solo las partes y sistemas autorizados puedan realizar cambios en la información, sistemas o activos;
- La Disponibilidad: garantizando que las partes autorizadas tengan acceso a la información, sistemas y activos; y
- Que se cumplan los requisitos legales, normativos y contractuales relativos a la seguridad de la información.

3.2 Estrategia de seguridad de la información

Ecenarro deberá garantizar la protección adecuada de toda la información, sistemas, activos, ubicaciones físicas y personas.

La estrategia con respecto a la seguridad de la información está basada en el negocio, orientada a evitar el riesgo, y se gestiona de acuerdo con las buenas prácticas establecidas en el mercado, alineándose directamente con los objetivos empresariales de Ecenarro.

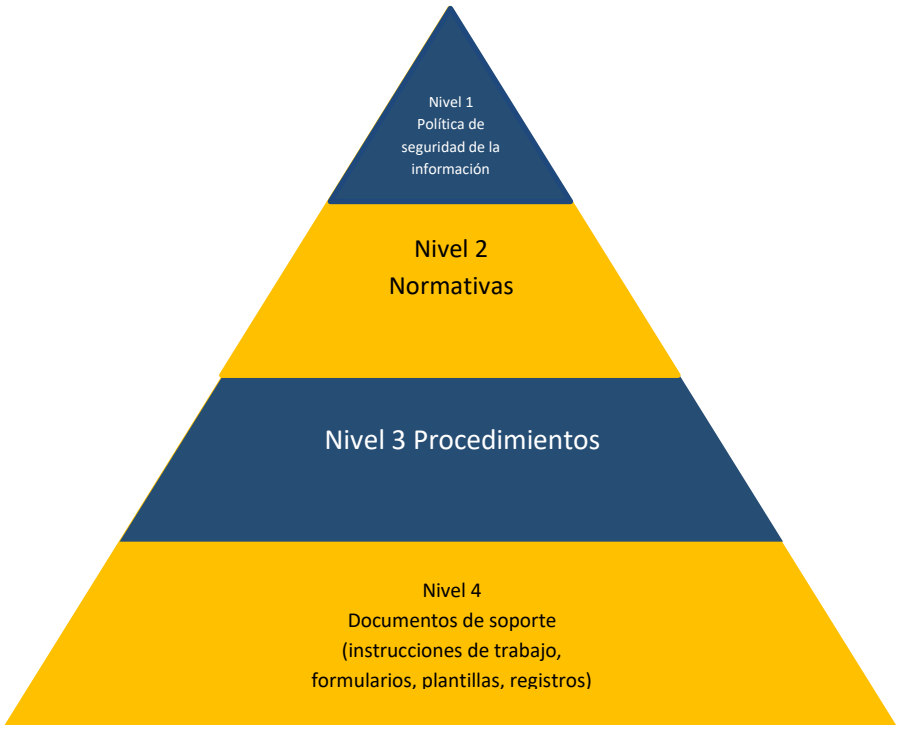
La estrategia general de seguridad de la información de Ecenarro ha sido desarrollada por el Responsable de Seguridad de la Información (CISO) y ha sido aprobada por el Consejo Rector, a propuesta del Consejo de Dirección, para demostrar el compromiso de la compañía con la protección de su información, sistemas y activos.

3.3 Normativa de seguridad de la información

Para respaldar esta Política general de seguridad de la información, debe mantenerse un conjunto de normativas, procedimientos y documentos de apoyo de seguridad de la información de nivel inferior, para garantizar que se sigan cumpliendo los objetivos de seguridad.

El CISO administrará el conjunto de la documentación complementaria, y la comunicará a los empleados de Ecenarro y (cuando sea apropiado) a las partes externas, clientes, proveedores y otros, que traten información de Ecenarro.

El SGSI de Ecenarro está basado en una estructura de información que documenta la administración y los controles de seguridad.



Esta estructura es jerárquica, con normativas y procesos de alto nivel cerca de la cima de la jerarquía, y procedimientos y registros detallados subordinados más abajo.

3.3.1 Normativa del SGSI

La normativa que respalda la Política de seguridad de la información es:

- Control de acceso, y gestión de contraseñas y usuarios.
- Copia de seguridad y recuperación.
- Gestión de la continuidad de la actividad.
- Gestión de la configuración.
- Criptografía.
- Gestión de incidentes de seguridad de la información.
- Clasificación, etiquetado y manipulación de la información.
- Gestión de activos de seguridad de la información.
- Gestión de cambios de seguridad de la información.
- Cumplimiento, garantía y auditoría de seguridad de la información.
- Gestión de riesgos de seguridad de la información.
- Formación y concienciación sobre seguridad de la información.
- Seguridad de la red.
- Seguridad física.
- Gestión de dispositivos portátiles y móviles.
- Gestión de registros.
- Auditorías técnicas de seguridad.
- Gestión de relaciones con terceros y proveedores.
- Gestión de vulnerabilidades y parches.

3.4 Organización y responsabilidades en materia de seguridad de la información

Ecenarro ha definido y aplicado responsabilidades de seguridad, para controlar la implementación y el funcionamiento de la seguridad de la información dentro de la compañía.

3.4.1 Director General

El Director General es el ejecutivo de más alto rango de Ecenarro, cuyas principales responsabilidades incluyen tomar decisiones corporativas, gestionar las operaciones generales y los recursos de Ecenarro, y ser la cara pública de la compañía.

3.4.2 Responsable de Seguridad de la Información global (CISO)

El Responsable de Seguridad de la Información global (CISO) establece la estrategia de seguridad de la información para la compañía, y determina la dirección para implementar y controlar la seguridad de la información.

El CISO proporciona orientación en materia de seguridad de la información al Director General y al equipo ejecutivo, recomendando inversiones y prácticas de seguridad de la información adecuadas.

El CISO es responsable de gestionar los riesgos relacionados con la seguridad de la información, que afectan a los activos de información, la planificación de la continuidad de la actividad, la gestión de crisis, la privacidad y el cumplimiento.

3.4.3 Responsable de Seguridad de la Información Local (LCISO)

El LCISO aplica la estrategia de seguridad de la información de la compañía, a nivel local.

El LCISO está en contacto con el CISO para aprobar las prácticas de seguridad de la información apropiadas, para la planta designada.

El LCISO es responsable de la gestión de los riesgos relacionados con la seguridad de la información, la seguridad física, la planificación de la continuidad de la actividad, la gestión de crisis, la privacidad y el cumplimiento de la normativa en la planta designada.

3.4.4 Auditor interno

El auditor interno es responsable de revisar el buen funcionamiento del SGSI a través de su conocimiento experto, y de comunicar los resultados de sus informes de auditoría a la dirección.

3.4.5 Consultor externo

En aquellas áreas del SGSI en las que se considere oportuno, Ecenarro puede contar con consultores externos que le asesoren sobre la forma más adecuada de implantar o mejorar aspectos del sistema de gestión.

3.4.6 Directores

Los directores de Ecenarro son los encargados de que sus respectivos equipos apliquen los requisitos de esta política.

3.4.7 Empleados

Todos los empleados tienen un papel crítico en el esfuerzo por proteger y mantener los activos de información de Ecenarro contra la pérdida de confidencialidad, integridad y disponibilidad; y reportar cualquier pérdida o sospecha de violación de la información, o de los activos de información.

Para asegurar esto, todos los empleados deben ser conscientes de su responsabilidad, y necesitan ser formados y concienciados.

3.5 Cumplimiento

El diseño, funcionamiento, uso y gestión de los sistemas de información deben cumplir todos los requisitos de seguridad legales, normativos y contractuales.

Esta política y el material complementario se revisarán anualmente por el CISO de Ecenarro, cuando se identifiquen riesgos significativos, o cuando haya cambios en las obligaciones legales o normativas.

Los documentos complementarios deberán ajustarse a cualquier cambio futuro de esta política y, en su caso, volver a presentarse para que los acepten las partes interesadas.

El CISO deberá informar regularmente al Consejo de Dirección de Ecenarro sobre el estado de la seguridad de la información y su eficacia a través de informes de gestión adecuados.

Cualquier incumplimiento de esta política será evaluado por el Consejo de Dirección de Ecenarro.

3.6 Mejora continua

El Consejo de Dirección de Ecenarro mejorará y revisará continuamente la idoneidad, adecuación y efectividad del SGSI.

4.0 Definiciones

SGSI	Sistema de Gestión de la Seguridad de la Información
CISO	Chief Information Security Officer
LCISO	Local Chief Information Security Officer
Confidencialidad	divulgación controlada de la información
Integridad	modificación controlada de la información
Disponibilidad	posibilidad de acceso a la información