OZONA
Política de Seguridad de la Información

27/10/2025

	SISTEMA DE GESTIÓN INTEGRADO DE OZONA Política de Seguridad de la Información

CONTROL DE VERSIONES

Revisión	Fecha	Descripción del cambio	Redacción
1.0	11/04/2011	Versión inicial	Ozona
2.0	25/06/2012	Adaptar la política a la ISO27001	Ozona
3.0	20/06/2013	Revisión	Comité de Seguridad
4.0	20/06/2014	Revisión de la política	Comité de Seguridad
5.0	19/06/2015	Revisión de la política – capitulo 4	Comité de Seguridad
6.0	23/06/2016	Adaptar para certificación 27001	Comité de Seguridad
7.0	11/01/2017	Revisión de la política para adaptación al GDPR. Sin cambios por estar ya recogido la protección de datos.	Comité de Seguridad
8.0	11/01/2018	Revisión de la política	Comité de Seguridad
9.0	15/01/2019	Revisión de la política	Comité de Seguridad
10	18/11/2022	Adecuación de la política al ENS	Comité de Seguridad
11	12/11/2024	Revisión de la política	Comité de Seguridad
12	27.10.2025	Revisión de la política	DBX

1. Introducción

1.1 Objetivo

La Dirección de Ozona reconoce que la información es un activo fundamental que aporta gran valor al negocio y, por tanto, debe protegerse adecuadamente. Esta Política de Seguridad de la Información (PSI) establece el compromiso de Ozona con la protección de la información en todas sus formas (digital, en papel, conocimiento del personal, etc.) y a través de todos sus canales de comunicación.

La política de seguridad de la información se alinea con la estrategia corporativa y con los objetivos del negocio, garantizando que las medidas implantadas permiten el cumplimiento de los compromisos adquiridos con clientes, socios y otras partes interesadas

El presente documento tiene por objeto dirigir y dar soporte tanto al Sistema de Gestión de la Seguridad de la Información como al Sistema de Gestión de Servicios implantados en Ozona. Para ello, la Dirección establece de forma clara e inequívoca las directrices de actuación en materia de seguridad de la información, manifestando su compromiso y enfoque para su gestión eficaz en toda la organización.

El propósito del Sistema de Gestión de la Seguridad de la Información es garantizar que los riesgos relacionados con la información sean conocidos, asumidos, gestionados y minimizados de forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios en el entorno, los riesgos y la tecnología, dentro del alcance definido.

Asimismo, se busca asegurar la calidad de la información y la prestación continua de los servicios, actuando de forma preventiva, supervisando la actividad diaria para detectar cualquier incidente, y reaccionando con agilidad para recuperarse lo antes posible, conforme a lo establecido en el artículo 8 del Esquema Nacional de Seguridad (ENS): Prevención, detección, respuesta y conservación.

La Dirección de Ozona se compromete a publicar y comunicar el presente documento a todos los miembros de la organización y partes interesadas incluidas en el alcance del Sistema de Gestión de la Seguridad de la Información y del Sistema de Gestión de Servicios, así como a su mantenimiento, adecuación y actualización permanente.

1.2 Alcance

Esta política se aplica a todas las empresas del **Grupo Ozona Consulting**, abarcando todos los procesos, servicios, sistemas y personas incluidos en el alcance del Sistema de Gestión Integrado (SGI) definido en el documento Contexto del SGI.
Todos los miembros de Ozona y las terceras partes que manejen información de Ozona deben cumplir con esta política.

1.3 Principios rectores de la seguridad de la información

Todas las actividades relacionadas con la seguridad de la información en Ozona se regirán por los siguientes principios fundamentales:

- **Prevención, detección, respuesta y recuperación** ante incidentes de seguridad, conforme al artículo 8 del ENS.
- **Gestión basada en el riesgo**, mediante análisis y evaluación sistemática para aplicar controles proporcionados.
- **Responsabilidad y rendición de cuentas**: cada persona tiene responsabilidades claras sobre la seguridad de la información.
- **Mejora continua** del sistema de gestión y de los controles implantados.
- **Formación y concienciación** permanentes, como base para implicar a todo el personal en la cultura de seguridad.
- **Cumplimiento legal y normativo**, nacional e internacional, así como de los compromisos contractuales.
- **Segregación de funciones** y control del acceso, para evitar conflictos de interés o accesos indebidos.
- **Disponibilidad de la política y documentación de seguridad** para todas las partes interesadas.

2. Misión

La misión de Ozona en seguridad de la información es garantizar la continuidad del negocio y la confianza de clientes y partes interesadas, protegiendo la información frente a un amplio abanico de amenazas. Para ello, Ozona define la seguridad de la información como la preservación de cinco características fundamentales: confidencialidad (solo las personas autorizadas acceden a la información), integridad (la información es completa y exacta), disponibilidad (los usuarios autorizados acceden a la información cuando la necesitan), autenticidad (se asegura la identidad y origen de la información) y trazabilidad (las acciones sobre la información pueden ser atribuidas y auditadas).

3. Objetivo de la Dirección

La Dirección de Ozona establece como objetivos de base, punto de partida y soporte de los objetivos y principios de la seguridad de la información los siguientes:

1. El conocimiento y cumplimiento de la Política por todas las partes interesadas.
2. El cumplimiento de la legislación y demás normativa vigente en materia de seguridad, protección de datos y propiedad intelectual.
3. El aseguramiento de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información que soporta los servicios objeto de este sistema.
4. El establecimiento de un sistema de clasificación de la información a fin de proteger mejor los activos críticos de la empresa.
5. La asignación de responsabilidades de seguridad.
6. La sensibilización y formación del personal en materia de seguridad.
7. La salvaguarda de los registros de la organización.
8. La gestión de los incidentes de seguridad y el aprendizaje de estos.
9. La gestión de la continuidad del negocio.

Todas estas acciones serán seleccionadas e implantadas en base los resultados de los informes de análisis de riesgos a fin de conseguir un equilibrio entre riesgo residual resultante y el coste de las medidas seleccionadas; valor este que está decidido y aprobado por dirección en base a sus propios criterios.

4. Compromiso de la Dirección

La Dirección de Ozona mediante la elaboración e implantación del Sistema de Gestión adquiere los siguientes compromisos:

1. Promover y comunicar la política de seguridad de la información y su importancia a todas las partes interesadas y garantizar que los objetivos de gestión de seguridad de la información son establecidos.
2. Desarrollar productos y servicios conformes con los requisitos legislativos, identificando para ello las legislaciones de aplicación a las líneas de negocio desarrolladas por la organización e incluidas en el alcance del Sistema de Gestión.
3. Definir el enfoque para la gestión de riegos de seguridad de la información e sus criterios de aceptación de los riesgos. He de asegurar que las evaluaciones de riesgo de seguridad de la información son realizadas en intervalos planeados.
4. Promover y apoyar la implantación de las medidas / controles necesarios para minimizar los riesgos a los que se encuentra expuesta la información en la consecución de los objetivos estratégicos que sean definidos.

5. Prevención y detección de virus y otro software malicioso, mediante el desarrollo de políticas específicas y el establecimiento acuerdos contractuales con organizaciones especializadas.
6. Establecer y cumplir con los requisitos contractuales establecidos con las partes interesadas.
7. Definir los requisitos de formación en seguridad y proporcionar la formación necesaria en dicha materia a las partes interesadas, mediante el establecimiento de planes de formación.
8. Gestionar, tratar y analizar las incidencias de seguridad de acuerdo con los procedimientos de gestión de incidencias.
9. Analizar las peticiones de cambios identificando riesgos de seguridad de la información nuevos o modificados y el posible impacto en la política y controles de seguridad actuales.
10. Gestionar la continuidad del negocio, desarrollando planes de continuidad conformes a metodologías de reconocido prestigio internacional.
11. Asegurar la realización de auditorías de seguridad y la revisión de la eficacia de las medidas / controles implantados.
12. Promover la mejora continua, identificando oportunidades de mejora resultantes de las auditorias.
13. Establecer las consecuencias de las violaciones de la política de seguridad, las cuales serán reflejadas en los contratos firmados con las partes interesadas, proveedores y subcontratistas.
14. Actuar en todo momento dentro de la más estricta ética profesional.

Por tanto, la dirección se compromete a respaldar el desarrollo de procedimientos específicos relativos a la seguridad de la información.

5. Cumplimiento legal y regulatorio

Ozona cumple con el marco legal y regulatorio aplicable en materia de seguridad de la información, la normativa de protección de datos personales, las leyes de propiedad intelectual, así como cualquier otra legislación sectorial o estándar internacional que aplique a las actividades de la organización.

El cumplimiento de requisitos legales y otros requisitos se evalúa regularmente a través del registro de Evaluación de Cumplimiento Legal del SGSI.

La organización mantiene un enfoque sistemático para asegurar este cumplimiento, que incluye:

- la consulta periódica a fuentes oficiales como el BOE y organismos reguladores (AEPD, CCN-CERT, INCIBE);
- el mantenimiento del registro de cumplimiento por parte del responsable del SGSI;
- la participación de áreas clave (legal, seguridad, servicios) en la revisión anual o cuando existan cambios normativos relevantes.

La responsabilidad de mantener actualizado este registro recae en el responsable de seguridad de la información, quien coordina con las áreas afectadas para asegurar que los requisitos se integren adecuadamente en los procesos y controles del sistema. Este registro se revisa al menos una vez al año o cuando se produce un cambio normativo, contractual o técnico que pudiera afectar su validez.

5.1. Cumplimiento con el Esquema Nacional de Seguridad

La Política de Seguridad de la Información de Ozona se alinea con los principios básicos establecidos en el Esquema Nacional de Seguridad (ENS), según lo previsto en el Real Decreto 311/2022.

Asimismo, Ozona ha integrado en su Sistema de Gestión de Seguridad de la Información los **requisitos mínimos establecidos en el Anexo II del ENS**, tales como:

- organización e implantación del proceso de seguridad,
- gestión de riesgos,
- seguridad del personal,
- control de accesos físicos y lógicos,
- protección de la información y de los sistemas,
- gestión de incidentes,
- continuidad de la actividad, entre otros.

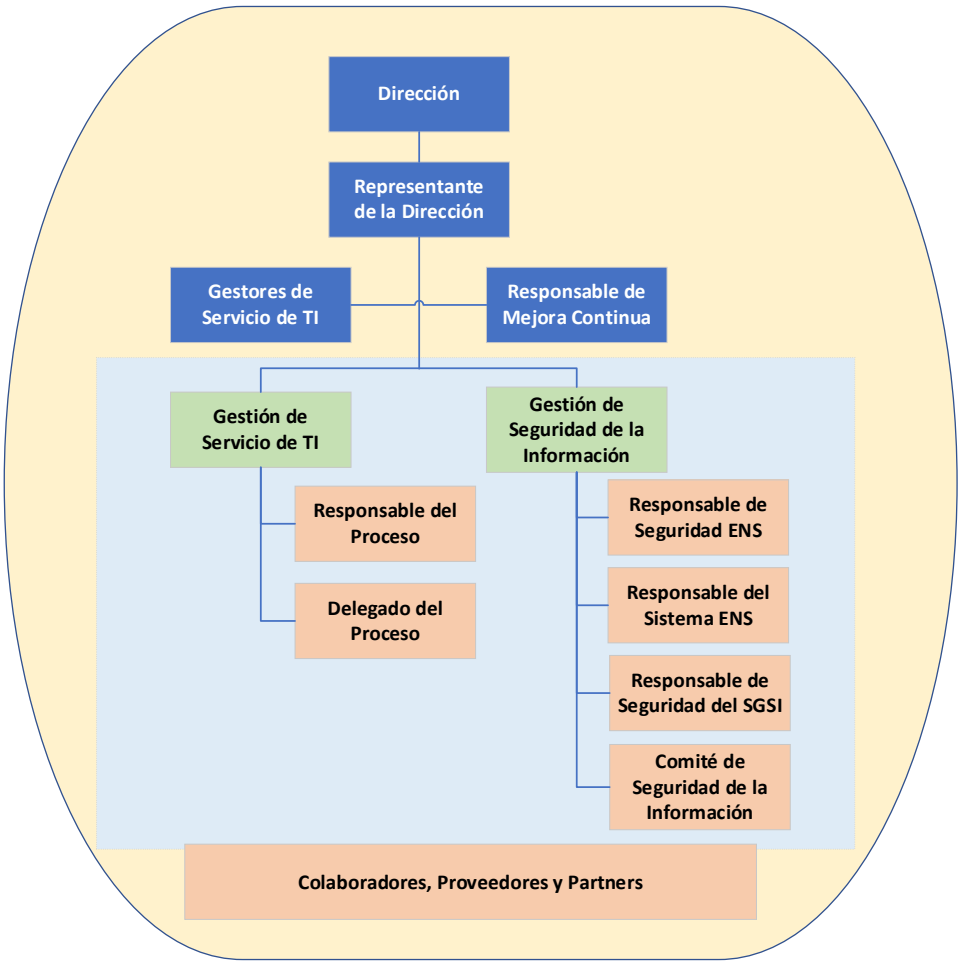
Estos aspectos están desarrollados en los documentos técnicos, normativos y procedimientos específicos que forman parte del Sistema de Gestión Integrado (SGI), disponibles en el repositorio interno para todas las partes interesadas pertinentes.

6. Estructura de la documentación de seguridad

La documentación de seguridad de Ozona está estructurada jerárquicamente para proporcionar coherencia y claridad. Ozona cuenta con un marco documental de Seguridad completo: una política corporativa (este documento), un Manual del SGI integrado, declaraciones de alcance, análisis de contexto, procedimientos técnicos y operativos, normativas específicas (ej. control de accesos, gestión de incidentes, continuidad, etc.), y registros de cumplimiento y operación. Esta documentación está integrada en el SGI para abarcar la gestión de calidad, servicios, medio ambiente y seguridad de la información de forma unificada.

7. Responsabilidades

La Dirección de Ozona mediante la aprobación del siguiente organigrama de carácter funcional y nominativo define las responsabilidades generales y específicas en materia de gestión de servicios y de gestión de seguridad de la información.



Los roles o funciones de seguridad en el marco del ENS son:

- Comité de Seguridad de la Información: órgano colegiado encargado del gobierno de la seguridad en Ozona. Su ámbito de responsabilidad incluye la aprobación de políticas de seguridad, la supervisión del desempeño del SGSI, la revisión de incidentes y auditorías, el seguimiento del cumplimiento normativo (ENS, ISO/IEC 27001) y la toma de decisiones estratégicas para la mejora continua de la seguridad.

  El Comité está formado por representantes de la Alta Dirección, así como por los principales roles de seguridad definidos en el SGSI: Responsable de Seguridad (RSEG), Responsable del Sistema (RSIS), Responsables de la Información (RINFO) y Responsables de los Servicios (RSERV), entre otros perfiles clave según el contexto o asunto tratado.

  Actúa como foro de coordinación entre las distintas áreas de la organización, facilitando la colaboración transversal entre responsables técnicos, operativos y estratégicos. Además, se relaciona directamente con el resto del sistema de gobierno corporativo y con los mecanismos de gestión de riesgos, continuidad de negocio, calidad y protección de datos, asegurando una gestión integrada.

- Responsable de la Información (RINFO): responsable de garantizar que la información bajo su dominio (normalmente asociada a una línea de negocio, servicio o proceso) se gestione de forma segura. Define los

requisitos de seguridad para la información y vela por que su tratamiento cumpla con las políticas y normativas aplicables.

- Responsable del Servicio (RSERV): responsable de la continuidad y seguridad de un servicio específico prestado por Ozona. Asegura que el servicio reúna las medidas de seguridad necesarias para cumplir los niveles de servicio acordados y la normativa, coordinando con el RINFO cuando corresponda.

- Responsable de Seguridad (RSEG): es el supervisor de la seguridad de la información en la organización (equivalente a un CISO). Es responsable de implantar y coordinar las medidas de seguridad, verificar su cumplimiento y evaluar su idoneidad respecto a los objetivos de seguridad de Ozona. Este rol de supervisión se asegura de que la seguridad esté alineada con los objetivos operativos y productivos de la empresa, reportando al Comité de Seguridad y a la Alta Dirección sobre el desempeño del SGSI.

- Responsable del Sistema (RSIS): es el encargado operativo de la seguridad en los sistemas de información. Implementa las medidas de seguridad en los activos de TI y servicios bajo su gestión, de acuerdo con las directrices del RSEG y los objetivos estratégicos de Ozona. Garantiza en el día a día que los sistemas y aplicaciones operen conforme a los controles de seguridad establecidos, y que las vulnerabilidades o incidencias técnicas se aborden adecuadamente.

Todos los perfiles, roles y responsabilidades se describen en la Matriz de Stakeholders del Sistema de Gestión Integrado.

La designación formal de los responsables anteriormente citados es competencia de la Dirección, que asegura que las personas designadas cumplen con los requisitos de cualificación y experiencia adecuados. Las asignaciones se formalizan por escrito y son documentadas y aceptadas explícitamente por cada responsable.

Las designaciones se revisan y actualizan:

- al menos con carácter periódico,
- cuando se produzcan cambios organizativos o funcionales relevantes,
- o cuando se detecte una necesidad de refuerzo, sustitución o reasignación por motivos técnicos, normativos o de continuidad operativa.

Este proceso está alineado con los principios de responsabilidad y trazabilidad definidos en el ENS.
Asimismo, estos roles garantizan la segregación de funciones en la gestión de la seguridad, ya que cada uno tiene cometidos distintos y complementarios, evitando la concentración de autoridad o posibles conflictos de interés. En caso de que surjan discrepancias entre responsables, estas serán resueltas por el Representante de la Alta Dirección (Coordinador Senior), asegurando una solución efectiva a nivel estratégico.

Asimismo, la Dirección promoverá de forma continua la concienciación en seguridad de la información entre todos los miembros de la organización, mediante acciones de comunicación, formación, recordatorios y divulgación adaptados a los diferentes perfiles. El objetivo es que todo el personal sea consciente de que la seguridad de la información es una responsabilidad compartida y fundamental para el desarrollo de la actividad de la compañía.

7.1 Obligaciones del personal

Todos los miembros de Ozona tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad de la Dirección disponer los medios necesarios para que la información llegue a los afectados.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

Todas las áreas de Ozona deben evitar, o prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad.

Para ello las áreas deben implementar las medidas mínimas de seguridad respaldados por la dirección en el apartado anterior, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, están definidos y documentados en la matriz de stakeholders.

7.2 Terceras partes

Cuando Ozona utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa.

8. Revisión, difusión y accesibilidad de la política

Esta Política de Seguridad de la Información será revisada de forma regular para asegurar su vigencia y adecuación. Como mínimo, la Dirección y el Comité de Seguridad evaluarán su contenido anualmente o siempre que ocurran cambios significativos en la organización, en la normativa aplicable o en el entorno de amenazas. Las revisiones buscan incorporar mejoras continuas y ajustar la política a nuevas exigencias o riesgos emergentes. Cualquier actualización de la política será aprobada la Dirección. La Dirección de Ozona se compromete al mantenimiento, adecuación y actualización permanente de esta política, de modo que siempre refleje los objetivos y requisitos vigentes de seguridad.

Una vez aprobada, la política se difunde y comunica a todos los miembros de la organización y a las partes interesadas aplicables. La Dirección garantiza que la política esté disponible y sea fácilmente accesible a través de la intranet corporativa.

Todos los empleados de Ozona deberán confirmar que han leído y entendido la política, y pueden plantear dudas o sugerencias a sus responsables o al Comité de Seguridad.

Asimismo, cuando proceda, esta política (o aspectos relevantes de la misma) se comunica a terceras partes que presten servicios a Ozona o que accedan a información de Ozona, a fin de que conozcan nuestras directrices y asuman los compromisos de seguridad necesarios. De esta manera, la PSI de Ozona es conocida por toda la organización y su cumplimiento es fomentado activamente por la Dirección.

9. Excepciones a la política de seguridad de la información

Cualquier exención o excepción a lo establecido en esta Política de Seguridad de la Información deberá ser formalmente solicitada, justificada y aprobada antes de su aplicación. La evaluación de dichas excepciones será responsabilidad del Comité de Seguridad de la Información, quien valorará los riesgos asociados, la justificación técnica u operativa y la temporalidad propuesta.

Una vez autorizadas, las excepciones deberán ser documentadas por escrito, registradas adecuadamente y revisadas periódicamente, para asegurar que siguen siendo válidas y no comprometen la seguridad de la información ni el

cumplimiento legal o normativo. Ninguna excepción podrá suponer un riesgo inaceptable para la organización ni violar compromisos contractuales o regulatorios asumidos por Ozona

10. Aprobación y entrada en vigor

Esta política ha sido aprobada y estará vigente hasta que sea reemplazada por una nueva versión.

35317844X DIEGO BEREA (R: B86171204)

Firmado digitalmente por 35317844X DIEGO BEREA (R: B86171204)
Fecha: 2025.11.11 10:29:20 +01'00'