

Anexo 4 - Política Calidad, Medio Ambiente y Seguridad de la información

1. INTRODUCCIÓN

SETTING es consciente de que la información constituye un activo fundamental para el desarrollo de su actividad, tanto desde el punto de vista operativo como estratégico, ya que permite la correcta prestación de los servicios, el cumplimiento de los compromisos adquiridos con clientes y partes interesadas, y el respeto a los requisitos legales y contractuales aplicables.

La información es tratada, almacenada y transmitida mediante sistemas y tecnologías de la información y la comunicación (TIC), en un entorno en constante evolución que posibilita la prestación de servicios tecnológicos de calidad, pero que al mismo tiempo introduce nuevos riesgos para la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Si bien este entorno facilita el acceso a la información por parte de las personas y organizaciones con un interés legítimo, también incrementa la exposición a amenazas de diversa naturaleza, cuya frecuencia, complejidad e impacto evolucionan de forma continua. Por ello, resulta imprescindible adoptar un enfoque sistemático y preventivo en la gestión de la seguridad de la información.

En este contexto, y de acuerdo con lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), así como con los requisitos de la norma ISO/IEC 27001, SETTING establece como prioridad la implantación y mantenimiento de medidas organizativas y técnicas destinadas a proteger la información y los sistemas que soportan los servicios que presta a sus clientes, tanto de forma directa como a través de terceros.

El ENS establece un conjunto de principios básicos y requisitos mínimos orientados a generar confianza en el uso de los medios electrónicos. Para SETTING, la seguridad de la información constituye una actividad de carácter integral y permanente, que no se limita a la definición puntual de controles o a la elaboración de documentación formal, sino que implica el desarrollo de directrices claras, procesos efectivos y una cultura de seguridad compartida en toda la organización.

La presente Política de Seguridad de la Información establece las bases para la protección de la información, los sistemas y los servicios gestionados por SETTING, garantizando un nivel de seguridad adecuado desde las

perspectivas del control de acceso, la confidencialidad, la integridad, la autenticidad, la trazabilidad y la disponibilidad de la información.

Esta Política constituye el marco de referencia para la gestión de la seguridad de la información en SETTING y será desarrollada mediante normativa interna, procedimientos y controles específicos. La Política será accesible y comprensible para todo el personal y para aquellos terceros que, directa o indirectamente, participen en la prestación de servicios o tengan acceso a la información y a los sistemas de la organización, en función del nivel de seguridad requerido.

En virtud de lo expuesto, la Política de Seguridad de la Información de SETTING se rige por los siguientes principios y directrices:

Prevención

SETTING adoptará medidas preventivas orientadas a eliminar o reducir, hasta un nivel razonable, la probabilidad de que las amenazas se materialicen y causen daños a la información, a los sistemas o a los servicios.

Estas medidas incluirán mecanismos de disuasión, reducción de la exposición y aplicación de los controles de seguridad establecidos por el ENS, de acuerdo con el Real Decreto 311/2022, así como aquellos controles adicionales identificados a partir de los procesos de análisis y gestión de riesgos, debidamente documentados.

El enfoque preventivo se basará, entre otros, en los siguientes aspectos:

- La realización de análisis de riesgos previos a la puesta en servicio de sistemas o servicios relevantes.
- La monitorización y evaluación continua de las medidas de seguridad y de los cambios significativos en la configuración de los sistemas.
- La realización de auditorías y evaluaciones periódicas de adecuación al ENS y a la normativa aplicable.
- La revisión y actualización periódica de las medidas de seguridad, garantizando su adecuación a la evolución de los riesgos, de las tecnologías y del contexto operativo, conforme a lo establecido en el artículo 9 del ENS.

Detección

SETTING establecerá las medidas organizativas y técnicas necesarias para la supervisión de los sistemas y servicios, con el fin de detectar de forma temprana cualquier anomalía, debilidad o incidente de seguridad que pueda afectar a su funcionamiento normal.

A tal efecto, se dispondrá de un proceso de detección y gestión de incidentes de seguridad que permita el análisis, la respuesta y la comunicación a las partes responsables, así como el registro de las actuaciones realizadas, de acuerdo con la normativa interna aplicable.

Respuesta

SETTING dispondrá de los mecanismos necesarios para responder de forma eficaz a los incidentes de seguridad, con el objetivo de minimizar su impacto sobre la información, los sistemas y los servicios.

La respuesta ante incidentes se basará, entre otros, en los siguientes principios:

- Reducción al mínimo razonable de los tiempos de detección, comunicación y gestión.
- Contención y mitigación del impacto del incidente.
- Restauración, en la medida de lo posible, del estado de los sistemas previo al incidente.
- Análisis de causas y adopción de medidas que reduzcan la probabilidad de repetición.

Recuperación

Con el fin de garantizar la disponibilidad de la información y de los servicios que presta SETTING, la organización desarrollará y mantendrá planes de continuidad y recuperación que permitan restablecer los sistemas y la información en situaciones en las que un incidente de seguridad o una contingencia grave inhabilite los medios habituales de operación.

Estos planes formarán parte del enfoque global de continuidad del negocio y serán revisados y probados periódicamente, de acuerdo con el nivel de riesgo y la criticidad de los servicios.

2. OBJETO Y ALCANCE

La presente Política establece los principios, compromisos y directrices generales de SETTING en materia de Calidad, Medio Ambiente y Seguridad de la Información, de conformidad con los requisitos de las normas ISO 9001, ISO 14001, ISO/IEC 27001 y del Esquema Nacional de Seguridad (ENS), en categoría media.

El alcance de esta Política comprende los servicios de análisis, desarrollo, mantenimiento e implantación de software, así como los servicios de soporte, operación y consultoría que SETTING presta a

sus clientes, incluyendo los sistemas de información, activos, infraestructuras, procesos y personas que intervienen en la prestación de dichos servicios.

La presente Política es de obligado cumplimiento para todo el personal de SETTING, incluidos los órganos de dirección, empleados, colaboradores y terceros que, en el marco de una relación contractual o de prestación de servicios, tengan acceso a información, sistemas o activos de la organización.

El desarrollo y aplicación de esta Política se apoyará en la normativa interna, procedimientos y controles de seguridad que la complementan, los cuales permitirán asegurar su cumplimiento, revisión periódica y mejora continua.

3. MISIÓN Y VALORES

La misión de SETTING es atender las necesidades tecnológicas, de servicios y de asesoramiento de sus clientes, optimizando su gestión mediante soluciones personalizadas e innovadoras, en un marco de estabilidad, sostenibilidad y excelencia.

La descripción completa de la misión, visión y valores de SETTING se recoge en la documentación del Sistema de Gestión Integrado de la organización, que incluye los procedimientos aplicables en materia de Calidad, Medio Ambiente y Seguridad de la Información.

4. MARCO NORMATIVO

El marco normativo aplicable a las actividades de SETTING en el ámbito de la presente Política de Seguridad de la Información está constituido, entre otras, por las siguientes disposiciones legales y normativas, en lo que resulte de aplicación:

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento (UE) 2016/679, de 27 de abril, General de Protección de Datos (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Adicionalmente, SETTING mantiene actualizada la relación de la normativa legal y reglamentaria aplicable en el documento «*Listado de*

Documentos_Integrado_ENS», que forma parte de la documentación del Sistema de Gestión Integrado.

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El Sistema de Seguridad de la Información de SETTING se organiza conforme a los niveles definidos en el Esquema Nacional de Seguridad:

Nivel	Descripción	Órganos/Roles
Gobierno	Nivel estratégico. Define la dirección, recursos, aprobación de políticas y decisiones de alto impacto.	Comité de Dirección
Supervisión	Nivel táctico. Supervisa el funcionamiento del SGSI, ENS y medidas de seguridad.	Comité de Seguridad, Responsable de Seguridad
Operación	Nivel operativo. Ejecuta medidas técnicas y organizativas.	Responsable del Sistema, administradores, usuarios

5.1 Comité de Dirección (Nivel Gobierno)

Descripción

Es el máximo órgano estratégico en materia de seguridad. No ejecuta tareas operativas, pero sí toma decisiones que afectan a políticas, recursos y cumplimiento.

Composición

- Director General
- Dirección Comercial y Operaciones
- Dirección de Consultoría y Sistemas de Gestión
- Dirección Financiera

Responsabilidades clave

- Aprobar la Política de Seguridad y las políticas complementarias.
- Aprobar el presupuesto y recursos para el ENS y el SGSI.
- Nombrar formalmente los roles ENS: Responsable de Seguridad, Responsable de Sistemas, Responsable de Servicio/Información.
- Aprobar la revisión anual del SGSI y del ENS.

- Ser informado de incidentes graves y riesgos significativos.
- Asegurar la integración del ENS en la estrategia de la empresa.

5.2 Comité de Seguridad de la Información (Nivel Supervisión)

Descripción

El Comité de Seguridad de la Información es el órgano colegiado responsable de dirigir, coordinar y supervisar las actuaciones en materia de seguridad de la información en SETTING.

Este Comité actúa como órgano de referencia para el cumplimiento del Esquema Nacional de Seguridad y del Sistema de Gestión de Seguridad de la Información.

Composición

- Responsable de Seguridad (Presidente)
- Dirección de Operaciones
- Dirección de Consultoría y Sistemas de Gestión
- Responsable del Sistema
- Invitados según materia (IT, legal, proveedor especializado...)

Funcionamiento

El Comité se reunirá, al menos, dos veces al año y de forma extraordinaria cuando se produzcan incidentes graves o situaciones que así lo requieran.

Funciones del Comité

El Comité de Seguridad de la Información tiene, entre otras, las siguientes funciones:

- Supervisar el cumplimiento del ENS, del SGSI y de las guías CCN-STIC aplicables.
- Elaborar, revisar y proponer la Política de Seguridad de la Información y las normativas derivadas.
- Aprobar instrucciones técnicas, normas y procedimientos de seguridad.
- Validar la categorización de los sistemas y servicios conforme al ENS.
- Analizar los incidentes de seguridad y supervisar las medidas adoptadas.
- Priorizar riesgos y aprobar acciones del Plan de Tratamiento.
- Promover la mejora continua del sistema de seguridad de la información.
- Elevar al Comité de Dirección las decisiones estratégicas y los informes relevantes.
- Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC.

5.3 Roles de seguridad de la información

Responsable de Información / Responsable de Servicios

Dirige las decisiones sobre la seguridad de la información o del servicio bajo su ámbito.

La figura del o la Responsable de Información o Responsable de Servicios tendrá definidas las siguientes funciones y responsabilidades en relación con el ENS:

- Definir los requisitos de seguridad del servicio o información.
- Establecer los niveles CIDAT para cada activo: Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.
- Garantizar que los contratos con terceros incluyen cláusulas de seguridad ENS.
- Evaluar el impacto de incidentes sobre sus servicios.
- Participar en la categorización ENS.
- Colaborar en el análisis de riesgos.
- Proponer salvaguardas y medidas complementarias.

Responsable de Seguridad de la Información

Es el rol central del ENS. Coordina y supervisa todo el sistema de seguridad. La figura del o la Responsable de Seguridad de la Información tendrá definidas las siguientes funciones y responsabilidades en relación con el ENS:

- Determina los requisitos de seguridad de la información tratada.
- Efectúa la valoración de las categorías de seguridad de la información relativas al Anexo I del ENS.
- Elaborar y actualizar el Documento de Aplicabilidad ENS (DoA).
- Supervisar la operativa de todos los activos en todo su ciclo de vida.
- Realizar análisis de riesgos según determinan las normas de seguridad relativas al cumplimiento del ENS.
- Coordinar el Plan de Tratamiento de Riesgos.
- Supervisar la implantación de medidas técnicas y organizativas.
- Elaborar informes de incidentes graves.
- Promover la Política de Seguridad.
- Proponer normativa técnica, instrucciones y directrices.
- Impulsar auditorías ENS e ISO.

Este rol debe ser independiente del Responsable del Sistema.

Responsable del Sistema

La figura del o la Responsable del Sistema tendrá definidas las siguientes funciones y responsabilidades en relación con el ENS:

- Determina los requisitos de seguridad de los sistemas prestados bajo su responsabilidad.
- Efectúa los procesos de seguridad de los sistemas.
- Garantizar el funcionamiento adecuado del sistema.
- Aplicar las medidas técnicas ENS aprobadas.
- Ejecutar medidas de seguridad física y lógica.
- Colaborar en auditorías y análisis de riesgos.
- Informar al RSI de vulnerabilidades, desviaciones o incidentes.

Administradores / Técnicos TIC

La figura del o la Administrador o Técnicos TIC tendrá definidas las siguientes funciones y responsabilidades en relación con el ENS:

- Gestionar accesos y permisos (principio de mínimo privilegio).
- Aplicar hardening, parches y configuraciones seguras.
- Monitorizar eventos, logs y alertas.
- Custodiar evidencias para auditoría.
- Detectar, registrar y comunicar sin demora al Responsable de Seguridad cualquier incidente, vulnerabilidad o evento anómalo identificado en los sistemas bajo su responsabilidad.

Personal Usuario

La figura del personal usuario tendrá definidas las siguientes funciones y responsabilidades en relación con el ENS:

- Cumplir las políticas y normas de seguridad.
- Proteger la información a la que acceden.
- Notificar de forma inmediata cualquier incidente, sospecha de incidente o anomalía de seguridad.
- Usar canales seguros para intercambio de información.

Proveedores

La figura de los proveedores tendrá definidas las siguientes funciones y responsabilidades en relación con el ENS:

- Cumplir las cláusulas ENS del contrato.
- Mantener medidas de seguridad equivalentes.
- Notificar incidentes y colaborar en su tratamiento.
- Facilitar auditorías y verificaciones.

Delegado de Protección de Datos (DPO)

SETTING evaluará periódicamente la obligatoriedad de designar un Delegado de Protección de Datos (DPO), conforme a lo establecido en el artículo 37 del Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018.

Dicha evaluación quedará documentada formalmente y será revisada cuando se produzcan cambios en la naturaleza, volumen o finalidad de los tratamientos realizados.

En caso de que resulte obligatoria o se decida voluntariamente su designación:

- El DPO actuará con independencia funcional.
- Reportará directamente a la Dirección.
- No recibirá instrucciones en el ejercicio de sus funciones.
- No podrá ser destituido ni sancionado por el desempeño de sus funciones.
- Dispondrá de los recursos necesarios para el adecuado cumplimiento de sus obligaciones.

Las funciones del DPO incluirán, entre otras:

- Informar y asesorar a la organización sobre sus obligaciones en materia de protección de datos.
- Supervisar el cumplimiento del RGPD y de la normativa nacional aplicable.
- Asesorar en la realización de Evaluaciones de Impacto en Protección de Datos (EIPD).
- Actuar como punto de contacto con la autoridad de control.
- Supervisar la gestión de violaciones de seguridad que afecten a datos personales.

Cuando SETTING actúe como encargado del tratamiento, notificará sin dilación indebida al responsable del tratamiento cualquier violación de seguridad que afecte a datos personales, conforme al artículo 28 del RGPD.

5.4 Nombramiento y renovación de roles

Nombramiento

- Realizado por el Comité de Dirección.
- Documentado formalmente.
- Basado en competencias técnicas y experiencia.

Renovación

- Cada **dos años**, o
- por cambios organizativos,
- cambios en sistemas ENS,

- o por incidentes relevantes.

6. DATOS DE CARÁCTER PERSONAL

SETTING trata datos de carácter personal en el desarrollo de sus actividades y en la prestación de sus servicios, de conformidad con lo establecido en el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), y en la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales.

SETTING adopta las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta la naturaleza de los datos personales tratados y la finalidad del tratamiento, de acuerdo con la normativa vigente.

Los sistemas de información que tratan datos personales se diseñan y operan atendiendo a los principios de privacidad desde el diseño y por defecto, promoviendo:

- la incorporación de medidas de protección de datos desde las fases iniciales de planificación o desarrollo de los sistemas de información o aplicaciones, y
- la configuración, por defecto, de los niveles más altos posibles de protección de la privacidad.

El desarrollo, formalización y mantenimiento de la documentación específica en materia de protección de datos personales se realizará de forma progresiva dentro del Sistema de Gestión Integrado, de acuerdo con la evolución de los servicios y los requisitos legales aplicables.

7. GESTIÓN DE RIESGOS

SETTING realiza el análisis y tratamiento de los riesgos de seguridad de la información para todos los sistemas sujetos a la presente Política, evaluando las amenazas y riesgos a los que se encuentren expuestos, de acuerdo con una metodología formalmente establecida.

El análisis de riesgos se revisará periódicamente, al menos cada dos años, y adicionalmente cuando se produzcan cambios significativos en la información tratada, en los sistemas de información o en los servicios prestados, así como en caso de incidentes graves de seguridad o de identificación de vulnerabilidades relevantes.

La metodología de análisis y tratamiento de riesgos, así como los criterios de aceptación del riesgo, se encuentran definidos en el procedimiento *PRO-SI-*

01 Metodología de análisis de riesgos, que forma parte de la documentación del Sistema de Gestión de Seguridad de la Información de SETTING.

El Comité de Seguridad de la Información supervisará la correcta aplicación de dicha metodología, asegurando la coherencia de los análisis de riesgos y promoviendo la asignación de los recursos necesarios para la implantación de las medidas de seguridad que resulten adecuadas.

8. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información complementa las políticas y procedimientos de SETTING en materia de seguridad de la información, en particular en los ámbitos de:

- la protección de datos de carácter personal;
- la gestión de riesgos de la información;
- y otras materias compatibles con el cumplimiento normativo aplicable.

La Política de Seguridad de la Información se desarrollará mediante normativas y documentos de seguridad que abordarán aspectos específicos, los cuales estarán a disposición de los miembros de la organización que deban conocerlos, especialmente de aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

SETTING estructura el desarrollo y despliegue de la Política de Seguridad de la Información en los siguientes niveles documentales:

- 1) Primer nivel: La Política de Seguridad de la Información y las normativas generales de seguridad.
- 2) Segundo nivel: Las instrucciones y directrices de seguridad de la información, que establecen cómo actuar ante situaciones no contempladas de forma explícita en los procedimientos.
- 3) Tercer nivel: Los procedimientos de seguridad de la información, que describen de forma detallada y paso a paso cómo llevar a cabo determinadas actividades.
- 4) Cuarto nivel: Documentación de apoyo, como buenas prácticas, recomendaciones, guías, materiales formativos y otros recursos relacionados con la seguridad de la información.

La Política de Seguridad de la Información y las normativas generales serán aprobadas por el Comité de Dirección, a propuesta del Comité de Seguridad de la Información.

Las instrucciones, directrices y procedimientos de seguridad correspondientes a los niveles segundo, tercero y cuarto serán aprobados por el Comité de Seguridad de la Información, a propuesta del Responsable de Seguridad, en

colaboración con los responsables de los servicios y de los sistemas de información.

El incumplimiento de las instrucciones y normativas de seguridad de la información aprobadas podrá dar lugar a la adopción de las medidas disciplinarias que resulten de aplicación, de acuerdo con la normativa interna y la legislación vigente.

9. OBLIGACIONES DEL PERSONAL

Todos los miembros de SETTING tienen la obligación de conocer y cumplir la presente Política de Seguridad de la Información y las Normativas de Seguridad que la desarrollan.

Corresponde al Comité de Seguridad de la Información disponer los medios necesarios para garantizar que dicha información sea comunicada y accesible a las personas interesadas.

SETTING, consciente de la importancia del factor humano en el cumplimiento de los principios básicos y requisitos mínimos del Esquema Nacional de Seguridad, promoverá la concienciación y formación de su personal en materia de seguridad de la información y en la correcta utilización de los sistemas de información.

Todos los miembros de SETTING recibirán formación periódica en materia de seguridad de las tecnologías de la información y las comunicaciones. Esta formación no se limitará exclusivamente al personal con responsabilidades directas en el uso, operación o administración de los sistemas de información, sino que se extenderá a todo el personal que requiera el uso de dichos sistemas para el desempeño de sus funciones. Se establecerá un programa de concienciación continua, especialmente orientado al personal de nueva incorporación y a aquellos casos en los que se produzcan cambios relevantes en el puesto de trabajo o en las responsabilidades asignadas.

Los órganos de dirección y gestión de SETTING deberán promover y dar ejemplo en el cumplimiento de la Política de Seguridad de la Información y de los principios del ENS, facilitando los medios, recursos y niveles adecuados de concienciación, con el objetivo de evitar que la falta de conocimiento, organización, coordinación o instrucciones inadecuadas constituya una fuente de riesgo para la seguridad de la información.

10. TERCERAS PARTES

Cuando SETTING preste servicios a terceros, utilice servicios de terceros o intercambie información con otras entidades, se garantizará que dichas relaciones se gestionen de acuerdo con la presente Política de Seguridad de la Información y con la normativa de seguridad que la desarrolla.

SETTING establecerá los mecanismos necesarios de coordinación y comunicación con las terceras partes, con el objetivo de asegurar una adecuada gestión de la seguridad de la información y una correcta reacción ante incidentes de seguridad que puedan afectar a la información, los servicios o los sistemas implicados.

Cuando SETTING utilice servicios de terceros o facilite acceso a información o sistemas a proveedores, estos quedarán sujetos a las obligaciones de seguridad que resulten de aplicación, las cuales se formalizarán mediante cláusulas contractuales, anexos específicos de seguridad o documentos equivalentes, en función del tipo de servicio prestado y del nivel de acceso concedido.

Las terceras partes deberán cumplir, al menos, un nivel de seguridad equivalente al establecido en la presente Política, pudiendo desarrollar sus propios procedimientos internos siempre que garanticen dicho cumplimiento.

SETTING garantizará que el personal de terceros con acceso a información o sistemas esté debidamente concienciado y comprometido con la seguridad de la información, requiriéndose, con carácter previo al acceso, la aceptación expresa de los compromisos de seguridad y confidencialidad que correspondan.

Se establecerán procedimientos específicos para la comunicación, gestión y resolución de incidentes de seguridad que involucren a terceras partes, así como para la gestión de incumplimientos, pudiendo adoptarse medidas correctivas, restrictivas o contractuales en función de la gravedad del incidente.

En aquellos casos en los que una tercera parte no pueda cumplir plenamente algún aspecto de la presente Política, se deberá realizar un análisis específico de riesgos que identifique los riesgos asumidos y las medidas de tratamiento correspondientes. Dicho análisis deberá ser informado por el Responsable de Seguridad de la Información y aprobado por los responsables de la información y de los servicios afectados con carácter previo a la continuidad de la relación.

11. APROBACIÓN Y DESIGNACIÓN DE ROLES DE SEGURIDAD

Los roles de seguridad definidos en la presente Política han sido formalmente designados por el Comité de Dirección de SETTING, quedando constancia de dichos nombramientos en el acta correspondiente del Comité.

Las actas de nombramiento se conservan como registros del Sistema de Gestión Integrado, de conformidad con el procedimiento de control de registros vigente.

12. COMPROMISOS EN CALIDAD

SETTING se compromete a proporcionar servicios de calidad, respetuosos con el medio ambiente y seguros desde el punto de vista de la información, integrando estos principios en su estrategia, procesos y toma de decisiones.

En este marco, SETTING asume el compromiso de proteger la información y los sistemas de información que utiliza en el desarrollo de su actividad, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, así como la mejora continua de sus procesos y el cumplimiento de los requisitos legales y normativos aplicables.

La Dirección lidera y respalda la implantación, mantenimiento y mejora continua del sistema de gestión integrado, proporcionando los recursos necesarios y fomentando una cultura de responsabilidad y concienciación en toda la organización.

SETTING se compromete a:

Satisfacción del cliente

- Comprender sus necesidades y expectativas.
- Entregar productos y servicios que cumplan con los requisitos acordados, sean fiables, trazables y de calidad.

Mejora continua

- Establecer objetivos de calidad medibles y revisados anualmente.
- Analizar no conformidades, acciones correctivas y oportunidades de mejora.
- Mantener un sistema de revisión periódica por la Dirección.

Gestión por procesos

- Estandarizar y documentar los procesos clave.
- Medir y controlar su desempeño mediante indicadores accesibles y actualizados.
- Asegurar la coordinación entre los distintos departamentos y roles implicados.

Competencia y formación

- Proporcionar formación continua al personal, asegurando que dispone de los conocimientos necesarios para el desempeño de su función con calidad.
- Fomentar la implicación, la responsabilidad y el compromiso con la mejora continua.

12.1 Compromisos en Medio Ambiente

En coherencia con ISO 14001, SETTING se compromete a:

Protección del entorno

- Prevenir la contaminación y minimizar el impacto ambiental de las actividades de la empresa.
- Promover el uso responsable de los recursos naturales (papel, energía, agua).

Gestión de residuos y ciclo de vida

- Gestionar adecuadamente los residuos generados, especialmente los electrónicos.
- Tener en cuenta aspectos ambientales en el diseño de productos y servicios cuando aplique.

Cumplimiento de requisitos legales y otros compromisos

- Cumplir con la legislación ambiental vigente y otros requisitos aplicables.
- Mantener actualizada la evaluación de aspectos e impactos ambientales.

Sensibilización ambiental

- Fomentar una cultura de sostenibilidad a través de campañas, buenas prácticas internas y formación ambiental.
- Involucrar a proveedores y colaboradores en prácticas sostenibles.

12.2 Compromisos en Seguridad de la Información y Esquema Nacional de Seguridad (ENS)

SETTING adopta los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, y se compromete a:

Cumplimiento del ENS nivel medio

- Cumplir con las medidas de seguridad establecidas en el ENS para sistemas de categoría media.
- Designar formalmente al Responsable de Seguridad, Responsable del Sistema y Responsable del SGSI, asignándoles funciones claras.
- Integrar las medidas ENS con el SGSI de ISO 27001.

Seguridad desde el diseño y por defecto

- Incorporar la seguridad en todas las fases del ciclo de vida de los sistemas y servicios.
- Aplicar configuraciones seguras por defecto y principios de mínimo privilegio.

Análisis y gestión de riesgos

- Mantener un proceso continuo de identificación, evaluación y tratamiento de riesgos.
- Revisar regularmente los riesgos derivados de tecnologías, amenazas y proveedores.

Protección de datos y cumplimiento legal

- Garantizar la alineación con RGPD y LOPDGDD.
- Aplicar controles reforzados cuando se traten datos sensibles o especialmente protegidos.

Control de accesos, monitorización y continuidad

- Implementar controles de acceso robustos.
- Mantener registros de actividad, auditoría y monitorización de eventos.
- Realizar copias de seguridad periódicas y verificadas.
- Mantener un Plan de Continuidad del Servicio y un Plan de Recuperación ante Desastres.

Gestión de incidentes

- Aplicar un proceso estructurado de detección, análisis, respuesta y notificación.
- Registrar todos los incidentes y mejorar los procesos a partir de ellos.

Seguridad en proveedores

- Incluir cláusulas de seguridad en contratos.
- Evaluar periódicamente a proveedores críticos y servicios en la nube.

12.3 Igualdad de oportunidades

SETTING promueve:

- La igualdad efectiva entre mujeres y hombres.
- La no discriminación.
- La igualdad en el acceso al empleo, formación y promoción interna.

12.4 Comunicación, formación y concienciación

- Esta política se comunicará a todo el personal y estará disponible para las partes interesadas.
- SETTING proporcionará formación periódica en Calidad, Medio Ambiente, Seguridad de la Información y ENS.
- Se fomentará una cultura de responsabilidad individual y colectiva.

12.5 Revisión y mejora continua del sistema integrado

La Dirección revisará la Política al menos una vez al año o cuando existan cambios significativos en la organización, en el ENS, en las normas ISO o en los servicios prestados.

12.6 Declaración de la Dirección

La Dirección se compromete a dotar de los recursos necesarios para:

- Cumplir los requisitos del ENS nivel medio.

- Mantener y mejorar los sistemas de gestión ISO 9001, 14001 y 27001.
- Asegurar la calidad de los servicios, la protección ambiental y la seguridad de la información.

En Barcelona, a 2 de enero de 2026

Dirección