



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



Índice

Control de versiones	3
1. Introducción y Propósito	4
1.1. Antecedentes	4
1.2. Misión de la Organización	5
2. Principios rectores y Alcance	7
2.1. Principios rectores	7
2.2. Alcance	8
3. Marco Normativo y Legal	9
4. Principios Básicos y Requisitos Mínimos de la Seguridad de la Información	10
4.1. Principios básicos	10
4.2. Requisitos mínimos	10
5. Organización de la seguridad	16
5.1. Introducción	16
5.2 Roles: funciones y responsabilidades	17
5.3. Procedimiento para la designación y renovación de roles	21
5.4. Mecanismos de coordinación entre responsables	22
5.5. Resolución de Conflictos	22
5.6. Comité de Seguridad de la Información	23
5.6.1 Composición	23
5. 6. 2. Funciones	23
5. 6. 3. Convocatoria	24
7. Directrices para la gestión de la documentación	25
8 .Difusión y aplicación de la Política de Seguridad de la Información	26



Control de versiones

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	10/06/2026	Redacción inicial de la política.
1.0	16/07/2026	Aprobación formal de la política.



1. Introducción y Propósito

1.1. Antecedentes

Cloud y Olé S.L. depende de los sistemas de información para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que la entidad pueda cumplir con sus objetivos, desarrollar sus funciones o competencias y prestar los servicios para la cual se ha sido constituida 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 confidencialidad, integridad, disponibilidad, 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.

Cloud y Olé S.L. debe 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 donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.



1.2. Misión de la Organización

Cloud y Olé S.L. tiene como misión ofrecer servicios especializados de consultoría en ciberseguridad, ciberinteligencia, cumplimiento normativo y formación técnica. Asimismo, desarrolla, comercializa y opera la plataforma SaaS **Cloud Fortress**, diseñada para la centralización de la gestión de Tecnologías de la Información (TI) y ciberseguridad tanto para empresas finales como para otros proveedores de servicios gestionados (MSSP).

En el ejercicio de estas funciones, **Cloud y Olé S.L.** gestiona y custodia información tanto propia como de terceros (clientes, partners y proveedores). Por ello, los objetivos fundamentales en materia de seguridad que la organización pretende garantizar mediante la presente Política son:

- **Garantizar la confidencialidad, integridad, autenticidad** de la información corporativa y de los clientes, así como la **disponibilidad y continuidad** en la prestación de los servicios de consultoría y la explotación de la plataforma SaaS *Cloud Fortress*.
- **Implementar medidas de seguridad en función del riesgo**, adaptadas al dinamismo y la evolución tecnológica del entorno cloud, mediante la realización de análisis de riesgos periódicos.
- **Formar y concienciar a todos los integrantes** de la organización respecto a la seguridad de la información, reduciendo el riesgo humano y promoviendo una cultura interna alineada con la alta especialización técnica de la compañía.
- **Implementar medidas de seguridad que permitan la trazabilidad de los accesos** a las infraestructuras de desarrollo y producción, respetando estrictamente el principio de mínimo privilegio, reforzando el deber de secreto y confidencialidad del personal técnico en el desempeño de sus funciones.
- **Desplegar y controlar la seguridad física y lógica**, garantizando que los activos informáticos y de desarrollo de software se encuentren en entornos seguros y protegidos por controles de acceso estrictos, atendiendo a los riesgos específicos detectados en las instalaciones y entornos virtuales.
- **Establecer la seguridad en la gestión de comunicaciones** y entornos cloud, empleando mecanismos de cifrado y tunelización que aseguren que la información transmitida a través de redes públicas o compartidas se encuentre adecuadamente protegida.
- **Controlar la adquisición, desarrollo seguro y mantenimiento** de los sistemas de información en todas las fases del ciclo de vida (DevSecOps), garantizando la seguridad por defecto (*security by default*) tanto en los sistemas internos como en las soluciones de software y plataformas SaaS entregadas al cliente.
- **Controlar el cumplimiento de las medidas de seguridad** en la prestación de servicios externos, manteniendo un estricto control y homologación de seguridad en la adquisición de soluciones de terceros y proveedores cloud.



- **Gestionar de manera ágil los incidentes de seguridad** para su correcta detección, contención, mitigación y resolución, aplicando metodologías que permitan aprender de ellos e implementar medidas correctivas para evitar su reproducción.
- **Proteger la información de carácter personal** gestionada en los tratamientos de la empresa, adoptando las medidas técnicas y organizativas necesarias conforme al Reglamento General de Protección de Datos (RGPD) y la normativa nacional aplicable.
- **Supervisar de forma continuada el sistema de gestión de la seguridad**, promoviendo la mejora continua y la subsanación de cualquier ineficiencia detectada en los procesos de ciberdefensa y auditoría.

2. Principios rectores y Alcance

2.1. Principios rectores

- **Alcance estratégico:** la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente
- **Seguridad integral:** la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de la seguridad basada en el riesgo:** la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- **Prevención, detección, respuesta y conservación** con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, dando una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- **Existencia de líneas de defensa,** la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- **Vigilancia continua y reevaluación periódica:** la entidad implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- **Seguridad por defecto y desde el diseño:** los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- **Diferenciación de responsabilidades,** en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.



2.2. Alcance

Esta política se aplica a todos los sistemas de información de Cloud y Olé S.L. a las personas que conforman la organización y a los prestadores de servicios o proveedores de soluciones TIC de **Cloud y Olé S.L.**

3. Marco Normativo y Legal

El marco legal y regulatorio que rige las actividades y competencias de la organización en el ámbito del Esquema Nacional de Seguridad (ENS) abarca las normas jurídicas comunitarias y nacionales, estatales y autonómicas en materia de ciberseguridad y seguridad de la información en general y de protección de datos personales, así como estándares internacionales reconocidos como las norma, que refuerzan la gestión de la seguridad de la información. Asimismo, contempla la legislación específica que aplica a la empresa en su carácter de sociedad mercantil.

La empresa mantiene un registro actualizado de la legislación y normativa aplicable y tiene establecido un procedimiento de identificación de dichas normas.

Cloud y Olé S.L. aplica medidas técnicas y organizativas para dar cumplimiento a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El ENS mantendrá el respeto y cumplimiento de la legislación vigente en materia de Propiedad Intelectual, particularmente en lo que se refiere al uso del software. La empresa obtendrá las licencias correspondientes y llevará un registro y control de las mismas para su empleo adecuado en el desarrollo de las actividades.

El marco legal antes indicado estará en consonancia con el ámbito de aplicación del Esquema Nacional de Seguridad, en tanto uno de los grupos de controles de seguridad de este es el cumplimiento de la legislación aplicable.

La organización manifiesta expresamente su compromiso de cumplir con los requisitos de seguridad de la información que le son aplicables.

4. Principios Básicos y Requisitos Mínimos de la Seguridad de la Información

4.1. Principios básicos

En materia de seguridad de la información se tendrán en cuenta los principios básicos enumerados a continuación, por mandato del artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, al objeto de que la organización pueda cumplir con sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información:

1. Seguridad como proceso integral.
2. Gestión de la seguridad basada en los riesgos.
3. Prevención, detección, respuesta y conservación.
4. Existencia de líneas de defensa
5. Vigilancia continua.
6. Reevaluación periódica.
7. Diferenciación entre responsabilidades.

4.2. Requisitos mínimos

La Política de Seguridad se establecerá de acuerdo con los principios básicos indicados en el apartado anterior y se desarrollará aplicando los requisitos mínimos de conformidad con el artículo 12.6 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Para dar cumplimiento a los requisitos mínimos establecidos, la organización adopta las medidas y refuerzos de seguridad correspondientes, teniendo en cuenta:

- Los activos que constituyen los sistemas de información.
- La categoría del sistema.
- Las decisiones adoptadas para gestionar los riesgos identificados.

A continuación, se enumeran los requisitos mínimos:

a) Organización e implantación del proceso de seguridad

La empresa establece una estructura organizativa que define de forma clara las responsabilidades en materia de gestión de la seguridad.



La presente Política de Seguridad identifica a los responsables de velar por su cumplimiento y las funciones que tienen atribuidas, junto con los mecanismos de coordinación previstos y los procedimientos de resolución de los conflictos que puedan surgir entre dichos responsables durante el proceso de implantación.

Se constituye un Comité de Seguridad como órgano decisor y supervisor especializado en el sistema de gestión de la seguridad de la información dentro de la organización.

Si bien existen nombramientos formales y cargos de responsabilidad en materia de SGSI, el proceso de seguridad compromete a todos los miembros de la organización y así se hace saber al personal mediante la difusión de políticas, normas, directrices y firma de acuerdos donde se establece la responsabilidad de los usuarios y las consecuencias del incumplimiento.

La organización forma e instruye a su personal acerca de cómo alcanzar los objetivos de seguridad y promueve una cultura de la seguridad, poniendo a su disposición vías de apoyo y soporte continuas y eficaces.

b) Análisis y gestión de los riesgos

La organización realiza su propio análisis y gestión de riesgos para sus sistemas de información.

Esta gestión se realiza por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema.

A través de las medidas adoptadas para mitigar o suprimir los riesgos, se han aplicado las medidas de seguridad proporcionales al riesgo detectado, existiendo una proporcionalidad entre ellas y los riesgos evaluados.

c) Gestión de personal

Todo el personal, propio o ajeno, relacionado con la información y los sistemas es formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. La actuación del mismo es supervisada al objeto de verificar que se siguen los procedimientos establecidos y se aplican las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

Este personal ejercita y aplica los principios de seguridad en el desempeño de sus funciones.

Para corregir, o exigir responsabilidades en su caso, cada usuario que accede a la información del sistema debe estar identificado de forma única; de modo tal que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.



El acceso a la información está restringido según las necesidades de cada puesto de trabajo.

Se prevén medidas disciplinarias, además de otras responsabilidades que correspondan, en caso de incumplimiento de las políticas y normas de seguridad de la organización.

El sistema está dotado de mecanismos que permiten identificar los accesos y acciones de los usuarios al objeto de realizar correcciones y exigir responsabilidades.

El significado y alcance del uso seguro del sistema es concretado y plasmado en la Normativa de Seguridad aprobada por la Alta Dirección.

d) Profesionalidad

El personal encargado de la seguridad de la información cuenta con la formación y experiencia necesaria para desempeñar satisfactoriamente las tareas propias de su puesto.

La seguridad de los sistemas está atendida y revisada periódicamente por personal cualificado, dedicado e instruido, en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

La organización determina los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo. El personal recibe la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios sujetos al ENS. Estos conocimientos se mantienen actualizados y se impulsa el seguimiento de recomendaciones y buenas prácticas establecidas por los organismos competentes en materia de seguridad.

La empresa exige, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados

e) Autorización y control de los accesos

Los accesos a los sistemas de información están controlados y limitados a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados y exclusivamente a las funciones permitidas.

Se define qué usuarios y en qué medida tendrán acceso a los recursos de información, de manera que se disponga del acceso necesario para el desarrollo de sus funciones, sin poder acceder a equipos, sistemas, datos o funciones que excedan de aquellas y que, por tanto, no deban estar a su alcance por razones de seguridad.



La organización tiene implementados mecanismos de autenticación robustos así como mecanismos de autorización para permitir el acceso, denegarlo y revocarlo cuando sea necesario, realizando auditorías regulares para revisar los accesos.

f) Mínimo privilegio

Los sistemas de información se diseñan y configuran otorgando los mínimos privilegios necesarios para su correcto desempeño.

El sistema proporciona la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

Las funciones de operación, administración y registro de actividad son las mínimas necesarias, y se asegura que solo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados.

Mediante controles de configuración, se eliminan o desactivan las funciones que resultan innecesarias o inadecuadas al fin perseguido. El uso ordinario del sistema es sencillo y seguro, de forma tal que una utilización insegura requiera de un acto consciente por parte del usuario.

La organización cuenta con guías de configuración de la seguridad para las diferentes tecnologías utilizadas, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones innecesarias o inadecuadas.

g) Integridad y actualización del sistema

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requieren de actualización formal previa. La organización lleva a cabo actividades de evaluación y monitorización permanentes que permiten adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afectan, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

h) Protección de la información almacenada y en tránsito

La organización, a la hora de organizar e implantar sus objetivos de seguridad, tiene especial consideración por la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas.

Se aplican procedimientos que garantizan la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito del ENS.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el ENS está protegida con el mismo grado de seguridad, aplicándose las medidas necesarias conforme a la naturaleza del soporte, de acuerdo con las normativas aplicables.

i) Prevención ante otros sistemas de información interconectados

La organización lleva a cabo el análisis de los riesgos derivados de la interconexión del sistema con otros sistemas y controla su punto de unión.

Se establecen políticas, procedimientos y mecanismos de protección del perímetro del sistema de información de acuerdo al análisis de riesgos, reforzando las tareas de prevención, detección y respuesta a incidentes de seguridad.

j) Registro de la actividad y detección de código dañino

La organización registra las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, con identificación de la persona que las ha realizado.

Este registro tiene por finalidad exclusiva la de satisfacer el objeto del ENS, y se realiza con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, laboral y demás disposiciones que resulten de aplicación.

La organización, al único objeto de preservar la seguridad de los sistemas de información, y en la medida estrictamente necesaria y proporcionada, podrá analizar las comunicaciones entrantes y salientes de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación del servicio, evitar la distribución malintencionada de código dañino y otros daños a sus redes y sistemas de información, en plena y rigurosa observancia de los principios y disposiciones del Reglamento General de Protección de Datos.

k) Incidentes de seguridad

La organización dispone de procedimientos eficaces de gestión de incidentes de seguridad según normativa.



Asimismo, dispone de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de actuaciones, el cual emplea para la mejora continua de la seguridad del sistema.

I) Mejora continua del proceso de seguridad

El proceso integral de seguridad implantado se actualiza y mejora de forma continua, aplicando para ello los criterios y métodos reconocidos internacionalmente relativos a la gestión de la seguridad de las tecnologías de la información.

La organización está comprometida con la mejora continua del sistema de gestión de la seguridad de la información.



5. Organización de la seguridad

5.1. Introducción

La seguridad en nuestra empresa se considera un proceso integral que abarca todos los aspectos relacionados con el sistema de información: elementos humanos, materiales, técnicos, jurídicos y organizativos. La implementación del sistema de gestión de seguridad de la información basado en el ENS tiene este enfoque integral, evitando actuaciones puntuales o soluciones temporales.

Prestamos especial atención a la concienciación de todo el personal involucrado y de los responsables jerárquicos. Es fundamental mitigar los riesgos asociados al desconocimiento, la falta de organización, de coordinación y de instrucciones claras. Para ello, se realizan formaciones y se dan directrices continuas, asegurando que todos los miembros de la empresa comprendan y actúen conforme a las políticas de seguridad establecidas.

El análisis y la gestión de riesgos son fundamentales para nuestro proceso de seguridad siendo actividades continuas y constantemente actualizadas. Mantenemos un entorno controlado mediante la identificación y evaluación constante de riesgos, con el objetivo de reducirlos a niveles aceptables. Esto se logrará aplicando medidas de seguridad adecuadas y equilibradas, en función de la naturaleza de la información tratada, los servicios prestados y los riesgos identificados. Esta gestión proactiva permite asegurar que las medidas de seguridad son siempre pertinentes y efectivas, protegiendo así los activos y la integridad de la empresa.

La seguridad del sistema en nuestra empresa incluye acciones de prevención, detección y respuesta para minimizar vulnerabilidades y proteger la información y los servicios.

- **Prevención:** Implementamos medidas destinadas a disuadir y reducir la exposición a riesgos. Estas medidas eliminan o disminuyen el impacto de las amenazas que puedan materializarse.
- **Detección:** Establecemos mecanismos para identificar rápidamente la presencia de ciber incidentes y cualquier actividad sospechosa que pueda comprometer el sistema.
- **Respuesta:** Desarrollamos procedimientos para actuar de manera eficiente y oportuna en caso de incidentes, con el fin de restaurar la información y los servicios afectados.

Garantizamos la conservación de los datos e información en soporte electrónico y mantenemos los servicios disponibles durante todo el ciclo de vida de la información digital.

Los procedimientos del sistema asegurarán la preservación del patrimonio digital, respetando siempre los principios básicos y requisitos establecidos.

Nuestro sistema de información cuenta con una estrategia de protección basada en múltiples capas de seguridad. Esta estrategia se garantiza que, si una capa de seguridad es comprometida, se logren los siguientes objetivos:

- Reacción frente a incidentes: Se implementan mecanismos para desarrollar una respuesta adecuada a los incidentes que no pudieron evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su totalidad
- Minimización del impacto: Se toman medidas para minimizar el impacto en el sistema y limitar los efectos adversos en la información y los servicios.

Las líneas de defensa están compuestas por medidas de naturaleza organizativa, física y lógica, creando un entorno de seguridad robusto y efectivo.

La vigilancia continua es esencial para detectar actividades o comportamientos anómalos y permitir una respuesta oportuna. Además, realizamos una evaluación permanente del estado de seguridad de nuestros activos, lo que nos permitirá medir su evolución, identificar vulnerabilidades y detectar deficiencias de configuración.

Las medidas de seguridad son reevaluadas y actualizadas periódicamente para garantizar que su eficacia se ajuste a la evolución de los riesgos y los sistemas de protección. En caso necesario, se realiza un replanteamiento de la seguridad para mantener un entorno seguro y protegido.

En nuestros sistemas de información se definen claramente los roles de los responsables, que incluyen al responsable de la información, al responsable del servicio, al responsable de la seguridad y al responsable del sistema. La responsabilidad de la seguridad de los sistemas de información está claramente diferenciada de la responsabilidad sobre la explotación de los mismos.

Se especifican las atribuciones de cada uno de estos responsables, así como los mecanismos para la coordinación entre ellos y para la resolución de posibles conflictos.

5.2 Roles: funciones y responsabilidades

La Dirección de Cloud y Olé S.L. asigna responsabilidad y autoridad para los roles relevantes de la seguridad de la información. Los roles definidos para el SGSI de la empresa son los siguientes:



Responsable de Seguridad

Tipo de rol: supervisión.

Funciones:

Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisar la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportar sobre estas cuestiones.

Redactar, mantener y comunicar de forma adecuada las políticas, procesos y procedimientos de seguridad.

Dimensionar los recursos necesarios para la eficacia del SGSI.

Aportar información operativa del SGSI para reuniones del Comité de Seguridad de la Información.

Realizar análisis de riesgos del SGSI.

Apoyar el proceso de auditorías internas y de certificación del SGSI.

Planificar la implantación y mejora del SGSI.

Integrar el Comité de Seguridad de la Información.



Responsable del Sistema

Tipo de rol: operación .

Funciones:

Desarrollar la forma concreta de implementar la seguridad en el sistema y supervisar la operación diaria del mismo.

Implantar las medidas técnicas sobre las infraestructuras y sistemas de información de la empresa.

Redactar procedimientos técnicos de las medidas de seguridad adoptadas.

Monitorizar las infraestructuras y sistemas de información.

Informar periódicamente al Comité de Seguridad de la Información sobre el desempeño de las implantaciones efectuadas.

Aportar información técnica y económica para la definición de mejoras sobre la implantación.

Organizar y actualizar el Inventario de Activos.

Responsable del Servicio

Tipo de rol: gobierno.

Funciones:

Establecer los requisitos de seguridad sobre el servicio.

Definir los niveles de seguridad aplicables a la prestación del servicio abarcando el ciclo de vida establecido en la organización.

Integrar el Comité de Seguridad de la Información.

Responsable de la Información

Tipo de rol: gobierno.

Funciones:

Establecer los requisitos de seguridad sobre la información tratada.

Determinar la clasificación de la información alineada con el nivel de privacidad y la categorización del sistema.

Integrar el Comité de Seguridad de la Información.

Delegado de Protección de Datos (DPD)

Tipo de rol: asesor / consejero.

Funciones:

Proporcionar asesoramiento e información sobre Protección de Datos.

Supervisar el cumplimiento del Reglamento General de Protección de Datos y otra normativa aplicable en materia de Protección de Datos.

Ofrecer asesoramiento acerca de la Evaluación de Impacto relativa al tratamiento de datos personales.

Cooperar con la autoridad de control y actuar como punto de contacto.

En cumplimiento de la medida de seguridad del ENS correspondiente a la calificación de la Información, con respecto a la categorización de los sistemas de información, se establece lo siguiente:

- El responsable de la información y del servicio afectado por el análisis y gestión de riesgos se indicará en el Análisis de Riesgos del ENS (que son los dueños de los riesgos y miembros del Comité de Seguridad de la Información). El análisis de riesgos recogerá los criterios que determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales prescritos en el Anexo I del Real Decreto del ENS.
- El responsable de cada información y/o de cada servicio seguirá los criterios determinados, dentro del marco establecido en el artículo 40 y los criterios generales prescritos en el Anexo I del Real Decreto del ENS, para asignar a cada información el



nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.

- El responsable de la información y del servicio, en cada momento, tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido.

El Delegado de Protección de Datos ofrecerá su asesoramiento especializado al responsable del tratamiento con el fin de asegurar que los datos personales se tratan y se protegen conforme al Reglamento General de Protección de Datos y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, y trabajará en coordinación con el Responsable de Seguridad de la Información y con el Responsable del Sistema.

Todo el personal, tanto interno como externo, será responsable de cumplir con la presente Política de Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del ENS de Cloud y Olé S.L. en el ejercicio de sus actividades laborales que se vean afectadas por la seguridad de la información.

5.3. Procedimiento para la designación y renovación de roles

El procedimiento para la designación de los roles iniciará con la propuesta de designación de la Alta Dirección al candidato a ocupar un rol de seguridad de la información, que atenderá a los requisitos en cuanto a competencias, conocimientos y experiencia derivados de la identificación de los roles necesarios dentro del Sistema de Seguridad de la Información.

La aceptación de la propuesta del candidato constará documentalmente. En dicho acuerdo o contrato se especificarán las responsabilidades y duración del rol y condiciones aplicables al mismo.

La nueva designación se registrará en los sistemas internos de gestión de Recursos Humanos y de seguridad de la información. Los directorios internos y los sistemas de comunicación corporativos serán actualizados conforme al nuevo nombramiento.

Los nombramientos se revisarán por la Alta Dirección cada cuatro años y, salvo disposición contractual en contrario, se renovarán tácitamente por períodos anuales siempre que cualquiera de las partes, el nombrado o la empresa, no notifique a la otra, con al menos un mes de antelación, su voluntad de cesar en el cargo.

Los puestos que queden vacantes deberán cubrirse, en la medida de lo posible, el plazo de un mes, siguiendo el mismo procedimiento.

5.4. Mecanismos de coordinación entre responsables

En conocimiento de la crucial importancia de establecer mecanismos de coordinación entre los distintos responsables implicados en la gestión de la seguridad de la información, la empresa ha adoptado las siguientes medidas:

- Asignación de funciones y responsabilidades: cada rol tiene asignadas sus funciones y responsabilidades de forma clara para evitar duplicidades y omisiones, logrando una actuación coordinada y eficiente.
- Comité de Seguridad de la Información: se establece un Comité de Seguridad de la Información para tratar de forma coordinada los diferentes asuntos que atañen a la seguridad de la información en la organización.
- Canales de comunicación: se habilitan canales de comunicación directos entre los distintos responsables con el objetivo de facilitar la comunicación continua, ágil y eficiente.
- Documentación de actividades: las actividades relacionadas con la implementación y gestión de la seguridad son documentadas y compartidas entre los roles para garantizar la transparencia.
- Planificación conjunta de mejoras: cada área identificará posibles mejoras y coordinará con los otros roles para su implementación conjunta. Las propuestas de mejora serán presentadas al Comité de Seguridad para su evaluación y aprobación.
- Protocolo de incidentes de seguridad: en caso de incidente de seguridad, los distintos roles deberán coordinarse de forma inmediata para mitigar el impacto

5.5. Resolución de Conflictos

Se establece un procedimiento formal para la resolución de conflictos que puedan surgir entre responsables:

- Identificación del conflicto: cualquier responsable puede identificar y reportar un conflicto potencial.
- Notificación: el conflicto se notificará inmediatamente al Comité de Seguridad de la Información.
- Reunión de evaluación: se convocará una reunión extraordinaria del Comité para tratar el conflicto.
- Propuesta de solución: el Comité propondrá una solución basada en las mejores prácticas y alineada con la política de seguridad del ENS.
- Implementación: se implementará la solución acordada y se realizará un seguimiento para asegurar su eficacia.

En aquellos casos en que no se haya podido alcanzar una solución a través del procedimiento formal, el conflicto escalará a la Junta de Socios.

- El Comité de Seguridad presentará un informe detallado del conflicto, las soluciones propuestas y las razones por las cuales no se llegó a un acuerdo.
- La Junta de Socios tomará una decisión final que será vinculante para todas las partes.

5.6. Comité de Seguridad de la Información

En muestra del compromiso de la Dirección de proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora continua de un sistema de gestión de la información de acuerdo con el Esquema Nacional de Seguridad, y ejerciendo su liderazgo respecto del mismo, constituye el Comité de Seguridad de la Información (“CSI”).

El Comité de Seguridad de la Información actúa como un vínculo esencial entre la Alta Dirección, los departamentos técnicos y operativos y todos los empleados, asegurando que la seguridad de la información esté integrada en todos los aspectos de la organización.

5.6.1 Composición

El Comité de Seguridad de la Información se compone del Responsable de Seguridad, el Responsable del Sistema, el Responsable del Servicio y el Responsable de la Información.

Siempre compondrá el Comité de Seguridad un representante de la Dirección.

Asimismo, se integrarán en el Comité aquellas personas cuya participación sea necesaria, bien por su capacidad para aportar información relevante, bien porque el asunto a tratar les afecte de manera directa. La composición del Comité podrá ajustarse de acuerdo a las necesidades de cada sesión, con el fin de garantizar un enfoque integral y eficaz en la toma de decisiones relativas a la seguridad de la información.

5.6.2. Funciones

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia empresarial.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del ENS en los servicios y procesos de la compañía.
- Asegurar la disponibilidad de los recursos necesarios para el ENS.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del ENS.
- Asegurar que el ENS consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del ENS.
- Promover la mejora continua.
- Fomentar una cultura organizacional de protección de la información.

- Proporcionar canales adecuados para que los empleados reporten incidentes de seguridad y posibles vulnerabilidades.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.

El Comité de Seguridad de la Información procederá a revisar y a proponer la aprobación de la presente Política de Seguridad de la Información a la Dirección, que será la máxima responsable de la información y que también integra el Comité.

Además, el Comité de Seguridad de la Información centralizará los mecanismos de coordinación y resolución de conflictos entre los responsables que se indican a continuación, que se tratarán mediante debate durante las reuniones de los miembros de dicho comité:

- La Dirección será la encargada de aprobar esta Política y será la responsable de la autorización de sus modificaciones, así como de toda la información documentada del ENS de la entidad.
- El Responsable de Seguridad de la Información será el encargado de notificar la presente política al personal y de los cambios que en ella se produzcan, así como de determinar la categoría de seguridad del sistema y coordinar las acciones de implantación, mantenimiento y mejora del ENS de la entidad (incluyendo la Declaración de Aplicabilidad que formaliza la relación de medidas de seguridad aplicables del Real Decreto que regula el ENS y de las derivadas del Análisis y Gestión de Riesgos), y de sus auditorías, con el Responsable del Sistema, que se encargará de gestionar los requisitos técnicos de seguridad de los sistemas de información derivados de la categoría de seguridad del sistema (responsabilidad sobre la explotación de los sistemas de información), y con el Responsable del Servicio, que se encargará de gestionar los requisitos de seguridad de las actividades para la prestación de los servicios.

5.6.3. Convocatoria

El Comité de Seguridad de la Información se reunirá trimestralmente y siempre que sea necesario en atención al cumplimiento de sus competencias, funciones y responsabilidades.

El Responsable de Seguridad será el encargado de convocar al Comité, mediante comunicación a través de medios que aseguren su recepción y con antelación suficiente, fijando el orden del día.

El Responsable de Seguridad elaborará, preparará o recopilará toda la documentación o información necesaria para el buen desarrollo de las reuniones del Comité de Seguridad, dentro de sus competencias.



7. Directrices para la gestión de la documentación

El despliegue del ENS de Cloud y Olé S.L. se iniciará a partir del análisis de riesgos de seguridad de los sistemas de información (incluyendo los derivados del tratamiento de datos personales), que permitirá determinar el nivel de riesgo de seguridad de la información en que se encuentra la entidad e identificar los controles de seguridad necesarios y oportunidades de mejora para el tratamiento del riesgo y llevarlo a un nivel aceptable, tomando en cuenta el contexto de la organización.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada que deberá ser revisada y aprobada por el Comité de Seguridad de la Información, según se establece en el procedimiento de gestión documental.

En cumplimiento del artículo 12 del Real Decreto del ENS, la presente política de seguridad se desarrollará aplicando los requisitos mínimos descritos en el punto 4.2 de la presente política para incluirse en la documentación del sistema.

Además de aplicar los requisitos del propio Real Decreto 311/2022 como tal, se utilizarán las Guías CCN-STIC de Seguridad que son las normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de seguridad de las organizaciones, especialmente la Serie CCN-STIC-800 que establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS.

Se comunicará la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo), que tendrá la obligación de aplicarla en la realización de sus actividades laborales.

La información documentada será clasificada por niveles atendiendo a sus necesidades de confidencialidad, criticidad y sensibilidad, siendo manipulada de acuerdo a la clasificación establecida..

El sistema será objeto de una autoevaluación regular, al menos cada dos años, para verificar el cumplimiento del ENS de Cloud y Olé S.L. con los requisitos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, por lo que el personal afectado por el alcance de dichas auditorías deberá ser colaborativo para la eficacia de estas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo.

El responsable de cada información manejada por el sistema será el propietario del activo atendiendo al Inventario de la organización.



8 .Difusión y aplicación de la Política de Seguridad de la Información

La presente Política será difundida entre las partes interesadas tras su aprobación.

La Dirección dotará de los recursos necesarios para la aplicación efectiva de esta política, y para su buen desarrollo, tanto en las actividades de implantación como en su posterior mantenimiento y mejora de todo el ENS de la entidad.

Documento aprobado por la Dirección de Cloud y Olé S.L

Firmado por ***3855**
SALVADOR JESUS MADRID
(R: ****1459*) el día
24/07/2026 con un
certificado emitido
por AC Representación

Firmado por RUIZ VILLEN
RAFAEL - ***2691** el
día 24/07/2026 con un
certificado emitido por
AC FNMT Usuarios