



ORBE
TELECOMUNICACIONES

ENS

POLITICA SEGURIDAD INFORMACION

Zaragoza, 9 octubre de 2024

ORBE TELECOMUNICACIONES, S.L.

Avda. Manuel Rodríguez Ayuso, 114 - Ctro. Empresarial Miralbueno, SS 2

50012 ZARAGOZA

Tels. 976 300000 – Fax 976336300

E-mail: orbe@orbe.es

USO PÚBLICO

ÍNDICE

1	Objeto	2
2	Objetivos y misión de ORBE TELECOMUNICACIONES	5
3	Objetivos de la Política de Seguridad	5
4	Revisión de la Política DE SEGURIDAD	6
5	Marco Normativo	9
6	Ámbito de aplicación	10
7	Principios BÁSICOS	11
7.1	Principios básicos del ENS	11
7.2	Requisitos Mínimos de Seguridad.....	11
8	Organización de la seguridad.....	14
8.1	Responsabilidad general	14
8.2	Comité de Seguridad.....	14
8.3	Responsable de Seguridad	15
8.4	Oficina de Seguridad	15
8.5	Otros Responsables	15
9	Desarrollo de la Política de Seguridad	17
9.1	Instrumentos del desarrollo	17
9.2	Aprobación de las normativas	17
9.3	Sanciones previstas por incumplimiento	17
10	Concienciación y Formación	18
11	Análisis y Gestión de Riesgos	19
12	Seguridad de la información.....	20
13	Datos de Carácter Personal	21
14	Obligaciones del personal	22
15	Terceras partes	23



VERSIÓN	ELABORA	APRUEBA	FECHA DE REVISIÓN
01	Técnico de sistemas y comunicaciones 1	Responsable del SGSI	8/10/2021
02	Responsable de sistemas de seguridad	Responsable del SGSI	9/10/2024



1 Objeto

Con el objeto de dirigir y dar soporte a la gestión de la información y de sus servicios, se establece en la presente Política de Seguridad de la Información de ORBE TELECOMUNICACIONES, en adelante ORBE TELECOMUNICACIONES, para garantizar la calidad de la información y la prestación continuada de los servicios con el objeto de actuar preventivamente ante posibles incidencias y reaccionando con rapidez ante la materialización de las mismas.

Esta Política de Seguridad de la Información, en adelante Política de Seguridad, va alineada con los requisitos establecidos dentro de los correspondientes artículos del Esquema Nacional de Seguridad, en adelante ENS.

ORBE TELECOMUNICACIONES S.L., en adelante ORBE TELECOMUNICACIONES, sustenta su actividad de servicios integrales de telecomunicaciones mediante los Sistemas de Información, siendo éste un soporte básico de la operativa interna tanto a funciones comerciales como a las funciones de gestión. Los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc. que tratan información de sus clientes, constituyen el activo principal de ORBE TELECOMUNICACIONES S.L., de tal manera que el daño o pérdida de los mismos inciden en la realización de sus operaciones y pueden poner en peligro la continuidad de la organización.

La Política de Seguridad de la Información proporciona las bases para definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran para garantizar la seguridad de la información, cumpliendo el marco legal de aplicación y las directivas, políticas específicas y procedimientos definidos.

Estas actuaciones son seleccionadas e implantadas en base al análisis de riesgos y el equilibrio entre riesgo aceptable y coste de las medidas.

El Comité de Seguridad de la Información, en adelante CSI, junto con los responsables de los activos de información son quienes deben definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada, de modo que los procesos más importantes y/o sensibles recibirán mayor protección.

Es responsabilidad de la Dirección de ORBE TELECOMUNICACIONES y del CSI, promover y apoyar la implantación de las medidas técnicas y organizativas necesarias para minimizar los riesgos potenciales a los que se encuentra expuesta la información en la consecución de los objetivos estratégicos del negocio.

El objeto de esta Política es alcanzar una protección adecuada de la información de ORBE TELECOMUNICACIONES, dentro del alcance definido para el Sistema de Gestión de Seguridad de la Información, preservando los siguientes principios de la seguridad:

- **Confidencialidad:** garantizar que la información sea accesible sólo para quien esté autorizado a tener acceso a la misma.



- **Integridad:** garantizar la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad:** garantizar que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Estos principios básicos se deben preservar y asegurar en cualquiera de las formas que adopte la información, ya sea en formato electrónico, impreso, visual o hablado, e independientemente de que sea tratada en las dependencias de ORBE TELECOMUNICACIONES o fuera de ellas.

Así mismo, estos principios se deberán contemplar en las siguientes áreas de seguridad:

- **Física:** Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información.
- **Lógica:** Incluyendo los aspectos de protección de aplicaciones, redes y prototipos de comunicación electrónica y sistemas informáticos.
- **Político-corporativa:** Formada por los aspectos de seguridad relativos a la propia Compañía, a las normas internas, regulaciones y normativa legal.



2 Objetivos y misión de ORBE TELECOMUNICACIONES

La misión de ORBE es llevar a cabo su actividad de venta, instalación y mantenimiento de equipos de comunicaciones y de sistemas de protección activa contra incendios mejorando continuamente su calidad, situándose un paso por delante de las expectativas de los clientes.

El futuro de nuestra organización estará asegurado a través del compromiso de calidad y medioambiente con los servicios prestados en el campo de las telecomunicaciones y de los sistemas de protección contra incendios, el enfoque de servicio a nuestros clientes, así como por la cualificación e implicación de nuestros empleados, y la mejora del comportamiento ambiental

Compromisos y valores estratégicos:

- El empeño por satisfacer al cliente y los requisitos legales aplicables será el punto de mira de todo lo que hagamos.
- El futuro de nuestra organización estará determinado por la calidad de nuestra respuesta a las necesidades del cliente.
- El mantenimiento y preservación del medioambiente y del entorno natural
- La base fundamental de la fuerza de nuestra organización reside en sus empleados, a los que procuraremos en todo momento un entorno de trabajo seguro, que facilite su motivación, competencia y orgullo por su contribución al trabajo realizado.
- El asegurar la rentabilidad económica en un entorno de alta competitividad.



3 Objetivos de la Política de Seguridad

ORBE TELECOMUNICACIONES S.L. para el correcto desempeño de sus funciones de negocio se basa y ayuda del tratamiento de diferentes tipos de datos e información, sustentados por los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyendo estos uno de los activos principales de ORBE TELECOMUNICACIONES S.L., de tal manera que el daño o pérdida de los mismos inciden en la realización de sus servicios y pueden poner en peligro la continuidad de la organización.

Para que esto no suceda se ha diseñado una Política de Seguridad de la Información cuyos fines principales son:

- **Proteger**, mediante controles/medidas, **los activos** frente a amenazas que puedan derivar en incidentes de seguridad.
- **Paliar** los efectos de **los incidentes** de seguridad.
- **Establecer** un sistema de **clasificación de la información** y los datos con el fin de proteger los activos críticos de información.
- **Definir las responsabilidades** en materia de seguridad de la información generando la estructura organizativa correspondiente.
- **Elaborar** un conjunto de **reglas, estándares y procedimientos** aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- **Especificar** los efectos que conlleva el **incumplimiento** de la Política de Seguridad en el ámbito laboral.
- **Evaluar los riesgos** que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- **Verificar** el funcionamiento de **las medidas/controles de seguridad** mediante auditorías de seguridad internas realizadas por auditores independientes.
- **Formar a los usuarios en la gestión de la seguridad** y en tecnologías de la información y las comunicaciones.
- **Controlar el tráfico de información y de datos** a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- **Observar y cumplir la legislación** en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los activos de ORBE TELECOMUNICACIONES S.L.
- **Proteger el capital intelectual de la organización** para que no se divulgue ni se utilice ilícitamente.



- **Reducir** las posibilidades de **indisponibilidad** a través del uso adecuado de los activos de la organización.
- **Defender los activos** ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- **Controlar el funcionamiento de las medidas de seguridad** averiguando el número de incidencias, su naturaleza y efectos.
- **Garantizar** a los usuarios que los datos alojados en ORBE TELECOMUNICACIONES serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad.
- **Aumentar** el nivel de concienciación en materia de seguridad allí donde es de aplicación esta Política de Seguridad, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.
- **Establecer** las bases de un modelo integral de gestión de la seguridad en ORBE TELECOMUNICACIONES, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.
- **Hacer patente el compromiso** de ORBE TELECOMUNICACIONES con la seguridad de la información mediante su apoyo al Comité de Seguridad dotándole de los medios y facultades necesarias para la realización de sus funciones.
- **Definir, desarrollar y poner en funcionamiento** los controles metodológicos técnicos, organizativos y de gestión, necesarios para garantizar de un modo efectivo y medible la preservación de los niveles de confidencialidad, disponibilidad e integridad de la información aprobados por ORBE TELECOMUNICACIONES.
- **Garantizar la continuidad de los servicios** ofrecidos por ORBE TELECOMUNICACIONES a los usuarios.
- **Crear y promover** de manera continua una “cultura de seguridad” tanto internamente, a todo el personal, como externamente a los clientes y proveedores que permita asegurar la eficiencia y eficacia de los controles implantados y aumente la confianza de nuestros clientes.



4 Revisión de la Política DE SEGURIDAD

Esta Política de Seguridad será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización, con el fin de asegurar que ésta se adecua a la estrategia y necesidades de la misma.

La Política de Seguridad será propuesta y revisada por el Comité de Seguridad y aprobada y difundida por ORBE TELECOMUNICACIONES para que la conozcan todas las partes afectadas.

En caso de conflictos o diferentes interpretaciones se recurrirá al Comité de Seguridad para resolución de estos, previo informe propuesta de la Oficina de Seguridad.



5 Marco Normativo

A los efectos previstos en esta Política de Seguridad, el marco normativo de referencia es el que estipula la legislación vigente en materia de seguridad.

Debido al carácter personal y reservado de la información manejada y a los servicios puestos a disposición de los usuarios, ORBE TELECOMUNICACIONES desarrolla sus actividades de acuerdo a la normativa vigente en dichas materias, de entre las que actualmente cabe destacar por su especial relevancia:

- a) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- b) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- c) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- d) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- e) 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).
- f) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- g) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- h) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- i) Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- j) Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).
- k) Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- l) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- m) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.



6 **Ámbito de aplicación**

Esta Política de Seguridad, será de aplicación y de obligado cumplimiento para todos los usuarios de ORBE TELECOMUNICACIONES; a sus recursos y a los procesos afectados por el ENS y el RGPD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.



7 Principios BÁSICOS

7.1 Principios básicos del ENS

La Política de Seguridad de ORBE TELECOMUNICACIONES se desarrollará, con carácter general, de acuerdo a los siguientes principios:

- Seguridad como proceso integral: la seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. Se prestará atención a la concienciación de las personas para evitar que la ignorancia, la falta de organización y de coordinación, constituyan fuentes de riesgo.
- Gestión de la seguridad basada en los riesgos: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC.
- Prevención, detección, respuesta y conservación: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad. De igual manera, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.
- Vigilancia continua y reevaluación periódica: la vigilancia continua detectará actividades anómalas a las que dará respuesta. Los controles de seguridad implantados se reevaluarán al objeto de adecuar su eficacia a la constante evolución de los riesgos, de los sistemas de protección y del entorno tecnológico.
- Diferenciación de responsabilidades: la responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad de seguridad, así como de la responsabilidad de la información y la responsabilidad del servicio. Los roles y responsabilidades de cada una de estas funciones deberán quedar debidamente acotadas y reflejadas documentalmente.

7.2 Requisitos Mínimos de Seguridad

Esta Política de Seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación de un Sistema de Gestión de seguridad: la seguridad de los sistemas de información compromete a todos los miembros de ORBE TELECOMUNICACIONES. Así mismo, la estructura organizativa establecida en ORBE TELECOMUNICACIONES, cumplirá el principio de Diferenciación de Responsabilidades.
- Análisis y gestión de los riesgos: el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.
- Gestión del personal: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus



- responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
- d) **Profesionalidad:** la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. El personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables. Se exigirá, de manera objetiva y no discriminatoria, que los prestadores de 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:** se limitará el acceso a los activos de información por parte de usuarios, procesos, dispositivos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
 - f) **Protección de las instalaciones:** los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
 - g) **Adquisición de productos de seguridad y contratación de servicios de seguridad:** en la adquisición de productos de seguridad será exigible la certificación de la funcionalidad de seguridad relacionada con el objeto de dicha adquisición, según la categoría del sistema y el criterio del responsable de seguridad. Para la contratación de servicios de seguridad se estará obligado a lo dispuesto en el principio de profesionalidad.
 - h) **Mínimo privilegio:** los sistemas de información se diseñarán y configurarán otorgando los mínimos privilegios necesarios para su correcto desempeño.
 - i) **Integridad y actualización del sistema:** la inclusión de elementos físicos o lógicos requerirán autorización formal previa a su instalación en el sistema. También para cualquier modificación de la configuración de hardware y software.
 - j) **Protección de la información almacenada y en tránsito:** se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros, como los equipos portátiles, dispositivos portátiles, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. También forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por ORBE TELECOMUNICACIONES. Así como la información en soporte no electrónico que haya sido causa o consecuencia de ellos.
 - k) **Prevención ante otros sistemas de información interconectados:** se protegerá el perímetro del sistema de información. También se analizará los riesgos derivados de la interconexión de sistemas y se controlará el punto de unión.
 - l) **Registro de actividad y detección de código dañino:** Se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.
 - m) **Incidentes de seguridad:** se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad. Esta gestión de los incidentes se empleará para la mejora continua de la seguridad del sistema.



- n) Continuidad de la actividad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.
- o) Mejora continua del Sistema de Gestión de seguridad: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.



8 Organización de la seguridad

8.1 Responsabilidad general

La preservación de la seguridad será considerada objetivo común de todas las personas al servicio de ORBE TELECOMUNICACIONES, siendo estas responsables del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

En caso de incumplimiento de las directrices y normativas de seguridad indicadas en la presente Política de Seguridad y las obligaciones derivadas de ellas, ORBE TELECOMUNICACIONES se reserva el derecho de aplicar el régimen disciplinario establecido en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

Por su importancia dentro de la implementación de la seguridad, quedan desarrolladas en la presente política algunas de las funciones de los órganos que ORBE TELECOMUNICACIONES estima necesarios para la correcta gestión de la seguridad.

La estructura organizativa de ORBE TELECOMUNICACIONES en materia de seguridad se revisa cada dos años. Una vez revisada, ORBE TELECOMUNICACIONES celebra un Comité de Seguridad Extraordinario donde se ratifica la nueva organización de la seguridad (Presidente, vocales, secretario, responsable de seguridad, ...).

8.2 Comité de Seguridad

1. Se crea el Comité de Seguridad de ORBE TELECOMUNICACIONES, como órgano colegiado de carácter transversal para la coordinación y gobierno en materia de seguridad.
2. El Comité estará formado por un presidente, un secretario y una serie de vocales que representan las unidades de ORBE TELECOMUNICACIONES.
3. Serán funciones propias del Comité:
 - a) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en seguridad.
 - b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.
 - c) Elevación de propuestas de revisión del marco normativo de seguridad al órgano competente para su reglamentaria tramitación.
 - d) Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad.
 - e) Supervisión y aprobación del nivel de riesgo y de la toma de decisiones en la respuesta a incidentes de seguridad que afecten a los activos TIC.
 - f) Definición y aprobación del modelo de relación con los Comités de Seguridad de las entidades/empresas incluidas en el ámbito de aplicación de la Política de Seguridad.
4. El Comité se reunirá al menos una vez por semestre y se regirá por esta Política de Seguridad.
5. El Comité nombrará entre sus miembros un grupo de respuesta a incidentes, llamado "Comité de Crisis", cuya función será la toma urgente de decisiones en caso de



contingencia grave que afecte a la seguridad de sistemas de información críticos de ORBE TELECOMUNICACIONES.

6. Las labores de soporte y asesoramiento al Comité serán realizadas por el Responsable de Seguridad y la Oficina de Seguridad.

8.3 Responsable de Seguridad

1. El nombramiento del Responsable de Seguridad será potestad del Comité de Seguridad de ORBE TELECOMUNICACIONES.
2. La persona Responsable de Seguridad tendrá las siguientes funciones, dentro de su Departamento:
 - a) Definición y seguimiento de las actuaciones relacionadas con la seguridad de los activos de información de la entidad y la gestión del riesgo.
 - b) Asesoramiento y soporte sobre temas de Seguridad.
 - c) Coordinación en materias de seguridad de la información.
 - d) Propuesta y seguimiento de programas de formación y concienciación.
 - e) Reporte al Comité de Seguridad de un informe periódico sobre el estado de la Seguridad TI y las actividades relacionadas.
 - f) Asunción de las funciones incluidas en el Reglamento (UE) 2016/679 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 (Reglamento general de protección de datos).

8.4 Oficina de Seguridad

1. La Oficina de Seguridad estará compuesta por técnicos de las diferentes unidades de ORBE TELECOMUNICACIONES, si bien se puede convocar a aquellas personas que la Oficina estime necesarias para el desarrollo de los trabajos encomendados.
2. En esta Oficina de Seguridad estará también el Responsable de Seguridad de ORBE TELECOMUNICACIONES que tendrá funciones sobre la revisión y elaboración de propuestas para ser presentadas y debatidas en el Comité de Seguridad.
3. La Oficina de Seguridad tendrá las siguientes atribuciones:
 - a) Asesoramiento en la definición del planteamiento técnico y operativo de los objetivos, iniciativas y planes estratégicos en seguridad, de acuerdo con las directrices del Comité de Seguridad.
 - b) Asesoramiento en la elaboración de propuestas relativas a la revisión del marco normativo de seguridad.
 - c) Elaboración de informes y propuestas de cumplimiento legal y normativo.
 - d) Elaboración de informes sobre el nivel de seguridad de los activos.
 - e) Reporte al Comité Seguridad de informes periódicos sobre el estado de la seguridad.
4. La Oficina de Seguridad se regirá por esta Política de Seguridad.

8.5 Otros Responsables

El **Responsable de la Información** determina los requisitos de seguridad clasificando la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las



dimensiones de seguridad conocidas y aplicables (Disponibilidad, Autenticidad, Trazabilidad, Confidencialidad e Integridad), dentro del marco establecido en el Anexo I del ENS, respecto a la información tratada en ORBE TELECOMUNICACIONES.

El **Responsable del Servicio** determina la infraestructura hardware y software del sistema de información, los criterios de uso, los servicios ofrecidos, los formatos y cualquier otro aspecto del funcionamiento del sistema de información de ORBE TELECOMUNICACIONES.

El **Responsable de Seguridad** determina cómo satisfacer los requisitos de seguridad, tanto de la información como de los servicios ofrecidos, incluyendo la definición de procedimientos de seguridad y, en su caso, la adopción de medidas de urgencia ante posibles deficiencias o amenazas en ORBE TELECOMUNICACIONES.

El **administrador del sistema** desarrolla, opera y mantiene el sistema de información de ORBE TELECOMUNICACIONES.

Las discrepancias en materia de seguridad serán resueltas atendiendo al criterio de mayor jerarquía.



9 Desarrollo de la Política de Seguridad

9.1 Instrumentos del desarrollo

La Política de Seguridad se desarrollará por medio de instrucciones de servicio y circulares que afronten aspectos específicos. Dichas instrucciones y circulares podrán adoptar alguna de las siguientes modalidades, o mediante los siguientes instrumentos:

- **Normas de seguridad:** Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.
- **Procedimientos:** Concretan flujos de trabajo para la realización de tareas, indicando lo que hay que hacer, paso a paso, pero sin entrar en detalles (de proveedores, marcas comerciales o comandos técnicos). Son útiles en tareas repetitivas.
- **Instrucciones técnicas (IT):** Desarrollan los Procedimientos llegando al máximo nivel de detalle, (indicando proveedores, marcas comerciales y comandos técnicos empleados para la realización de las tareas).

La normativa de seguridad estará disponible en la intranet a disposición de todos los miembros de la organización que necesiten conocerla.

9.2 Aprobación de las normativas

En toda la organización, la aprobación de las normas de seguridad se hará de acuerdo a lo dispuesto en la presente Política de Seguridad y las normativas específicas que para ello desarrollará ORBE TELECOMUNICACIONES.

9.3 Sanciones previstas por incumplimiento

Del incumplimiento de la Política de Seguridad y normas que la desarrollan, podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en la Ley del Estatuto de los Trabajadores sobre régimen disciplinario de los empleados.



10 Concienciación y Formación

Con la concienciación y formación se busca alcanzar varios objetivos. Por una parte y fundamental la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de ORBE TELECOMUNICACIONES y a todas las actividades y servicios que lo componen.

Por otra parte, y siguiendo el principio de seguridad integral, la articulación de los medios necesarios para que todas las personas que intervienen en el día a día de ORBE TELECOMUNICACIONES y sus responsables jerárquicos tengan la sensibilidad adecuada hacia la responsabilidad que conlleva al gestionar información de sus clientes.



11 Análisis y Gestión de Riesgos

Todos los sistemas sujetos a esta Política de Seguridad deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando ocurra un incidente grave de seguridad.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica.



12 Seguridad de la información

Se desarrollará una Clasificación de la Información de ORBE TELECOMUNICACIONES de forma que se identifiquen los distintos tipos de información, en base a su sensibilidad, se establezca cómo etiquetar los soportes que la contengan y se determine qué se puede y no se debe hacer con cada nivel de clasificación.



13 Datos de Carácter Personal

Será de aplicación lo contemplado en el RGPD y lo dispuesto en la legislación nacional a tales efectos.

Cada departamento se encargará de gestionar y mantener la seguridad referente a los datos de carácter personal incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad.

Todos los sistemas de información de ORBE TELECOMUNICACIONES se ajustarán a los niveles de seguridad requeridos por esta normativa.



14 Obligaciones del personal

Todos los miembros de la organización y las empresas y personas terceras que realicen servicios de cualquier clase contratados por ORBE TELECOMUNICACIONES o que de alguna manera se presten bajo el control y/o la dirección de ORBE TELECOMUNICACIONES tienen la obligación de conocer y cumplir esta Política de Seguridad y el Cuerpo Normativo de Seguridad. ORBE TELECOMUNICACIONES es responsable de comunicar la política y las normas, así como de disponer de los medios necesarios para que todo el personal las conozca de forma efectiva, en especial, las que puedan afectar a sus funciones.

Se establecerá un programa de concienciación continua dirigido a todos los miembros de ORBE TELECOMUNICACIONES, en particular a los de nueva incorporación.

El personal deberá usar los procedimientos de notificación de incidentes de seguridad habilitados a tal efecto, en caso de detectar un posible incidente.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas.



15 Terceras partes

Cuando ORBE TELECOMUNICACIONES preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad, se establecerán canales para el reporte y coordinación de los respectivos Delegados de Protección de Datos y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando ORBE TELECOMUNICACIONES 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 atañe a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de la Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados, así como del responsable del tratamiento previsto en el RGPD, antes de seguir adelante.

