POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

Ondata International SL (en adelante Ondata) depende de los sistemas de la información y los servicios para alcanzar sus objetivos. Estos sistemas y servicios deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar 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 (ENS) y la norma ISO/IEC 27001, 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.

Los diferentes departamentos deben 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 de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el ENS y la ISO/IEC 27001.

Esta política servirá a la organización como referencia permanente para la obtención del nivel de seguridad y objetivos que se pretendan alcanzar, así como el mantenimiento y el desarrollo del Sistema de Gestión de Seguridad de la Información implantado.

MISIÓN Y ALCANCE

La misión de Ondata es la de proporcionar servicios de calidad y gestión segura de la información que satisfagan las necesidades de nuestros clientes y partes interesadas, garantizando la confidencialidad, integridad y disponibilidad de la información, mediante la mejora continua de nuestros procesos y el compromiso de nuestro equipo.

Ondata International proporciona a organismos públicos y entidades privadas soluciones tecnológicas avanzadas de terceros en los ámbitos de la informática forense, la ciberinteligencia, la seguridad informática y la investigación digital, aportando los servicios profesionales asociados que permitan su correcta implantación, utilización y mantenimiento.

El SGSI tiene por **alcance** los sistemas de información que presta soporte al suministro, instalación, despliegue, mantenimiento, formación y soporte a usuarios de las soluciones software y hardware de ciberseguridad, ciberinteligencia e informática forense, según la declaración de aplicabilidad vigente, considerando las medidas de seguridad que le sean de aplicación del anexo II del RD 311/2022, junto a las disposiciones de su articulado.

Dichas actividades son llevadas a cabo:

- Desde las oficinas de Ondata ubicadas en la avenida de Bruselas 36, 1º izq 28108, de Alcobendas (Madrid).
- Por el personal de Ondata.
- Sujetas a las cuestiones internas y externas definidas en el contexto de la organización, así como al cumplimiento de los requisitos referentes a las partes interesadas definidas también en el contexto de la empresa.
- Desde la perspectiva de la seguridad física, no se marcan exclusiones.
- Desde la perspectiva de la seguridad lógica, abarca todos los activos que pudieran afectar a la seguridad de la información dentro del alcance.

De modo expreso se encuentra excluido del alcance:

- Todas aquellas actividades efectuadas por la organización y que no se encuentran expresamente descritas en el alcance.
- Todo aquel personal de Ondata que no forme parte de las actividades descritas en el alcance.
- Los activos tecnológicos que no afecten a la seguridad de la información identificada dentro del alcance.
- Los controles de seguridad definidos como no aplicables en el documento MSI-02 Declaración de Aplicabilidad.

MARCO NORMATIVO

Identificación

Los servicios prestados por Ondata se desarrollan dentro del ámbito de la informática y las telecomunicaciones, poniendo para ello a disposición de los clientes servicios TI que pueden procesar, almacenar o transmitir la información que estos depositan en nuestros sistemas, o transitan por ellos. Por este motivo, Ondata busca garantizar permanente la alineación de nuestros procedimientos y servicios con el marco normativo de aplicación en cada momento. Dicho marco normativo se encuentra referenciado en el Registro de Requisitos Legales, debidamente actualizado y revisado periódicamente.

Datos de carácter personal

En el ámbito de aplicación de la regulación en materia de datos de carácter personal, Ondata cumple con todos los requisitos reflejados en la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, habiendo adaptado su normativa interna, procedimientos, contratos y otros documentos.

ISO 27001

Ondata se encuentra certificada en el estándar internacional de Seguridad de la Información, donde muestra un compromiso elevado con la seguridad de la información, el mantenimiento del servicio, la resiliencia y la calidad.

Esquema Nacional de Seguridad

En el ámbito del Esquema Nacional de Seguridad, está política está integrada por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, de modificación del Real Decreto 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad.

Otras normativas

Cualquier otra normativa que le sea de aplicación a la empresa, será recogida en el documento de requisitos legales y de control de la documentación y registros.

ORGANIZACIÓN DE LA SEGURIDAD

De modo general, los requisitos del Sistema de Gestión de Seguridad de la Información se encuentran en el Manual de Seguridad de la Información de la organización, si bien hay ciertos aspectos que son específicos dentro del alcance y en consecuencia requieren de procedimientos al efecto.

La política de gestión aplicable a la seguridad de la información es la política de gestión global de la organización, además de la presente, puesto que las directrices de la Dirección son únicas.

A continuación se detallan algunos aspectos específicos del Sistema de Gestión de Seguridad de la Información en el contexto general de la organización:

GESTIÓN DOCUMENTAL. El procedimiento que rige la gestión de la documentación relativa al sistema de gestión se desarrolla en el documento **PG-01 Control de la Documentación y Registros**, el cual es común al sistema de gestión de la organización.

GESTIÓN DE PERSONAL. Todos los aspectos relacionados con la concienciación, formación y capacitación se rigen por el procedimiento **PG-04 RRHH**, el cual es común al sistema de gestión de la organización.

LEGISLACIÓN APLICABLE. La legislación aplicable se encuentra identificada en el listado de documentación externa de la organización, presente en el registro **Control Documentación y Registros**. De igual modo, en el documento **MSI-02 Declaración de Aplicabilidad (SoA)**, en el campo justificación para la aplicación de controles, se hace referencia a los requisitos legales y contractuales de aplicación.

RIESGOS Y CONTROLES. La sistemática seguida por la organización desde la perspectiva de análisis y gestión de riesgos se desarrolla en el procedimiento **PS-02 Análisis y Gestión de Riesgos**, así como el desarrollo de cómo se gestiona la eficacia de los controles de seguridad implantados. De modo expreso, se identifica dentro del documento **MSI-02 Declaración de Aplicabilidad (SoA)** el listado de controles implantados, así como la referencia de su implantación, ya se encuentre desarrollada en un procedimiento documentado o se base en controles implantados sin procedimientos asociados.

Prevención

Se debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, deben implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

Otros principios generales

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.

- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información de la Organización deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones) donde reside la información deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes la Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales.

Roles y responsabilidades

La estructura organizativa, roles y responsabilidades generales de Ondata están definidos en el documento MSI-01 Manual de Seguridad de la Información.

No obstante, en el marco del ENS y la ISO/IEC 27001, la gestión de la seguridad de la información implica la existencia de una estructura organizativa que defina unas responsabilidades diferenciadas en relación a requisitos de información, requisitos del servicio y requisitos de seguridad.

Ondata articula esta diferenciación en el ámbito del alcance del ENS a través de los roles (CCN-STIC 801 ANEXO B. ESTRUCTURAS POSIBLES DE IMPLANTACIÓN):

NIVEL	RESPONSABILIDAD	RESPONSABLE
Gobierno	Responsable de Información y Servicios	Dirección
Supervisión	Responsable de Seguridad	Senior Forensics Manager
Operación	Responsable del Sistema	Director Técnico de Ingeniería

Es por ello que se ha definido la siguiente tabla RACI de asignación de responsabilidades en el SGSI.

R → Persona responsable de llevar a cabo la tarea **A** → Persona que autoriza **C**→ Persona que debe ser consultada **I** → Persona que debe ser informada	**Gobierno**	**Supervisión**	**Operación**	**Responsable de RRHH**	**Responsables de Departamento**
Alcance del SGSI	**R**	C	C		
Política de Seguridad	**R**	C	C		
Revisión de los Objetivos del Sistema de Gestión de Seguridad	I	A	**R**		
Identificación de requisitos legales y contractuales	I	**R**	C		
Gestión de Competencias del personal		I	C	**R**	C
Concienciación en Seguridad		C	**R**	C	I
Análisis de Riesgos	I	C	**R**		C
Aceptación Riesgo Residual	**R**	I	C		
Implantación del Plan de Tratamiento de Riesgos	A	I	**R**		
Medición de la eficacia de los controles de seguridad	I	I	**R**		
Gestión de Incidentes de Seguridad	I	A	**R**		
Análisis de Vulnerabilidades	I	A	**R**		
Planificación del Programa de Auditorías		**R**	C		
Gestión de No Conformidades, AC y AP relativas al SGSI		A	**R**		I
Revisión por la Dirección	**R**	C	**C**		
Niveles de seguridad requeridos por la información	A	**R**	C		
Niveles de seguridad requeridos por el servicio	A	**R**	C		

Determinación de la categoría del sistema	I	**A/R**	I		
Declaración de aplicabilidad	I	**A/R**	C		
Medidas de seguridad adicionales	I	**A/R**	C		
Configuración de seguridad		**A/R**	C		
Documentación de seguridad		**A**	C		
Estado de seguridad del sistema	I	**A**	I		
Planes de mejora de la seguridad		**A**	C		
Planes de continuidad		C	**A**		
Suspensión temporal del servicio	A	C	**R**		
Seguridad en el ciclo de vida		C	**A**		

Nombramiento

El responsable de Seguridad de la Información será nombrado por la dirección. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

REVISIÓN Y APROBACIÓN

Será misión de los responsables de Información, Servicios, Seguridad y Sistema la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la dirección y difundida para que la conozcan todas las partes afectadas.

GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, se establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. Del mismo modo, se dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.

DESARROLLO DE LA POLÍTICA

La documentación relativa a la Seguridad de la Información se encuentra definida dentro del Sistema de Gestión, el cual se regula en el procedimiento PG-01 Control de la información documentada.

OBLIGACIONES DEL PERSONAL

Todos los miembros de Ondata tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, independientemente de si les afecta directa o indirectamente.

Las acciones específicas de concienciación y formación relativas al ENS y a la ISO/IEC 27001 se gestionan dentro del proceso PG-04 RRHH.

Carlos Sánchez Schaelchli

Director General

Versión 1 - 16 de junio de 2026