POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Tipo de documento:	POLITICA
Código:	SIP-REG-001-PSI
Versión:	2.0
Fecha:	10/04/2024
Autor:	Oriol Rosa
Proceso asociado:	SIP - Seguridad de la Información y Protección de Datos

OXIGEN

DATA CENTER

Control de cambios

Versión	Cambios	Tipo (Revisión, Validación, Aprobación	Autor	Aprobado por	Fecha
1.00	Redacción inicial	Aprobación	Oriol Rosa	Benjamin Rovira	01/04/2023
2.00	Actualización a ISo27001:2022 y corrección de errores menores	Revisión	Oriol Rosa	Benjamin Rovira	10/04/2024

Índice de contenido

1. Objeto

La presente es un complemento al contenido de la Política del Sistema de Gestión Integrado.
En su contenido, esta política establece:

- Las directrices y líneas de actuación en materia de Seguridad de la Información que regirán el modo en que OXIGEN gestionará y protegerá su información y sus servicios.
- Los criterios de comunicación a los grupos de interés.
- La forma de implementación de la seguridad en todas las áreas funcionales de la organización.

2. Alcance

El alcance definido en la presente política es:

"El Sistema de Seguridad de la Información de OXIGEN da soporte a los procesos de comercialización, prestación y explotación de los servicios de: Consulting (Audit, Consultancy, Planning, Business Strategy, Engineering, Design, Due Dilligence, Industrial Digitalisation, Datacenter Consultancy), Managed Services (24x7 Maintenance, 24x7 Operation, System Administration, Service Management, Provisioning, Monitoring), Infraestructures Facilities (Project Management, Construction, Start up, Commissioning, Housing), Cloud Computing (IaaS, PaaS, Storage, DataBase, Public Cloud), Cloud Data (Data arquitecture, Data government, Dashboards, PowerBI), Cloud Security (MultiCloud, SIEM, DR & BRS, Backup, Continuity Strategy).

Los servicios se prestan desde el Centro de Proceso de Datos de Sant Cugat del Vallés (Barcelona) para todos sus clientes. De acuerdo con la declaración de aplicabilidad (SIP-REG-006-SOA-V_2.0-Declaración de Aplicabilidad_con_RD 311_2022_Esquema Nacional de Seguridad de fecha 10/05/2024)."

---

3. Objeto, normas, marco legal y regulatorio

Esta política tiene por objeto establecer las directrices que deben seguirse para gestionar la información de la organización y sus servicios a través de la implantación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) que, plenamente Integrado en el Sistema Integrado de Gestión (SGI) de OXIGEN permita:

- Que el Sistema de Información mencionado en el apartado de alcance de esta política satisfaga lo contenido en Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica.
- El SGSI cubra los requisitos de la norma ISO/IEC 27001:2022

OXIGEN, dispone un procedimiento para la identificación, análisis y cumplimiento de la legislación vigente donde se identifica entre otra, el siguiente marco normativo relevante en materia de seguridad de la información:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el Ámbito de la Administración Electrónica.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley de Propiedad Industrial.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Ley 1/2019, de 20 de febrero, de secretos empresariales.
- REGLAMENTO (UE) 2022/2065 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

Todo el personal de OXIGEN será responsable de cumplir con la presente política, así como de aplicar toda la información documentada perteneciente al SGSI de la organización en sus actividades laborales que afecta al desempeño de la seguridad de la información.

4. Definiciones

No obstante, y a los efectos de una correcta interpretación de la presente política, se incluyen las siguientes definiciones:

- **Información**: datos que poseen significado, en cualquier formato o soporte. Se refiere a toda comunicación o representación de conocimiento.
- **Sistema de Gestión de la Seguridad de la Información (SGSI)**: conjunto de elementos interrelacionados (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **ENS**: son las siglas del Esquema Nacional de Seguridad, regulado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, siendo su aplicación en el ámbito de la administración electrónica del sector público. Su objeto es establecer la política de seguridad y crear las condiciones necesarias para la confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

5. Objetivos y principios de seguridad de la información

Con el objetivo de proteger de la información manejada por la empresa de las diferentes partes interesadas, así como de los sistemas de información que dan soporte a los productos y servicios prestados a los clientes, OXIGEN ha establecido los siguientes principios de seguridad como marco de referencia para el establecimiento de objetivos específicos:

1. Se entenderá la seguridad como un proceso integral, asociado a cualquier proceso de negocio dentro de la empresa, y a la protección de la información en cualquier soporte, físico o electrónico.

2. La gestión de la seguridad estará fundamentada en la protección de la información teniendo en cuenta las siguientes dimensiones de la seguridad:
    - Disponibilidad. La información debe estar disponible cuando se necesite
    - Integridad. La información debe ser exacta, veraz, y permanecer inalterada
    - Confidencialidad. El acceso a la información debe realizarse únicamente por personal autorizado
    - Autenticidad. La información debe mantenerse auténtica en origen y en destino
    - Trazabilidad. Debe poder conocerse quién y cuándo ha accedido a la información, y las operaciones realizadas sobre las misma.
3. La gestión de la seguridad estará basada en el análisis y gestión de los riesgos asociados a los activos de información. La dirección de OXIGEN establecerá el nivel de riesgo asumible, y los riesgos deberán estar por debajo de dicho valor. Los riesgos que se deben considerar pueden tener su origen en:
    - El propio análisis de riesgos asociado al cumplimiento normativo de seguridad de la información (ISO 27001 y ENS).
    - Las auditorías de seguridad asociadas al SGSI según ENS y norma ISO 27001.
    - El resto de las auditorías técnicas de seguridad y test de penetración que pudieran realizarse.
    - Los riesgos identificados por las herramientas de escaneo de vulnerabilidades utilizadas, sondas de monitorización implantadas, herramientas de detección de ataques, herramientas antimalware, y demás mecanismos de seguridad que pudieran utilizarse.
4. Se realizará una reevaluación periódica de los riesgos, y se revisará de forma continua el SGSI.
5. El conjunto de medidas de protección aplicables para la mitigación de los riesgos se documentará en las correspondientes Declaraciones de Aplicabilidad.
6. Los objetivos de seguridad estarán alineados con los principios y serán los indicados en el documento ECO-REG-002-SYM- Seguimiento y medición de Objetivos del SGI.

El Responsable de la Información conjuntamente con Responsable de Seguridad son los responsables de definir los objetivos de seguridad de la información para OXIGEN. Éstos son específicos y consecuentes con la Política de Seguridad de la Información y otros principios aplicables.

OXIGEN aplica los principios de privacidad y seguridad por defecto y como resultado, la seguridad (física y lógica) es una parte indisoluble del ciclo de vida de los servicios incluidos en el alcance. De este modo, el contenido de la presente política y todas aquellas que la complementan serán los garantes de que se aplican los correspondientes requisitos de seguridad en:

- La adquisición de bienes y servicios.
- La definición e implementación de servicios que componen el portfolio de OXIGEN.
- La gestión de la prestación del servicio.
- La prevención, detección y gestión de los incidentes de seguridad de acuerdo con los Artículos 25 y 33 del ENS.

5.1. Prevención

OXIGEN 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 se deben implementar las medidas mínimas de seguridad determinadas por el ENS de acuerdo con el nivel de seguridad requerido, 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. Para garantizar el cumplimiento de la política, OXIGEN debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

5.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 8 del ENS. La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 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.

5.3. Respuesta

OXIGEN se compromete a:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con OXIGEN.
- 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) reconocidos a nivel nacional: Iris-CERT, CCN-CERT,…
- Establecer los mecanismos para la notificación de brechas de datos personales a la Autoridad de Control y a los afectados de acuerdo con las condiciones determinadas en la legislación vigente.

5.4. Recuperación

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

6. Organización de la seguridad

OXIGEN, en materia de seguridad de la Información, tiene estructurada las responsabilidades, roles y autoridades en Comités y en roles específicos descritos en el documento "OPE-PRC-022-GPI-V_1·0-2022-12-10 Roles".
En los siguientes apartados se especifican los más relevantes en materia de Seguridad y sus funciones atribuidas:

6.1. Comité de Seguridad:

Sus funciones incluyen:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.

6.2. Responsable del Sistema de Información

Sus funciones incluyen:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Seleccionar y establecer las funciones y obligaciones a los técnicos encargados de personificar una gestión de la seguridad de los activos de OXIGEN, conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en OXIGEN.

6.3. Responsable de la Información

Sus funciones incluyen:

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.
- Determina los niveles de seguridad de la información.

6.4. Responsable del Sistema de Gestión de Seguridad (Resp. Seguridad)

Sus funciones incluyen:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de OXIGEN.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
- La estrategia de seguridad de la información definida por el Comité de Seguridad.
- Las normas y procedimientos contenidos en la Política de Seguridad de la Información de OXIGEN y normativa de desarrollo.
- Supervisar los incidentes de seguridad producidos en OXIGEN.
- Difundir en OXIGEN las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, así como las funciones y obligaciones en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables en materia de protección de datos personales y de seguridad de la información.

6.5. Responsable de seguridad física

Sus funciones incluyen:

- Adoptará y mantendrá las medidas de seguridad que le competan (protección de las instalaciones físicas), dentro de las determinadas por el Responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

6.6. CEO.

Sus funciones incluyen:

- Adoptará y mantendrá las medidas de seguridad en relación a la gestión de recursos humanos dentro de las determinadas por el Responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

6.7. Administrador de seguridad

Sus funciones incluyen:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución

6.8. Delegado de protección de datos

Las funciones del Delegado de Protección de Datos se encuentran especificadas en el artículo 39 del RGPD, siendo las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones del RPGD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.
- Cooperar con la autoridad de control. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

6.9. Designación nominal de roles

La designación nominal de los Comités y roles específicos están descritos en “LID-REG-002-ARO-Asignacion_roles_y_responsabilidades-V01_00-2023_03_26”.

7. Gestión del riesgo

El despliegue del SGSI de OXIGEN se inicia a partir del análisis de Riesgos, que permite determinar el nivel de riesgo de seguridad de la información en que se encuentra la entidad e identificar los controles de seguridad necesarios para el tratamiento del riesgo y llevarlo a un nivel aceptable, así como las oportunidades de mejora, considerando las cuestiones internas y externas y los requisitos de las partes interesadas. Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada, mediante procedimientos, normativas, instrucciones técnicas, manuales que son revisados y aprobados por los roles descritos en el punto 6.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (empleados y proveedores), que tendrá la obligación

de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del SGSI.
La gestión de la Seguridad de la Información en OXIGEN está basada en el riesgo, de conformidad con la Norma internacional ISO/IEC 27001:2022 y el ENS.
De acuerdo con lo indicado en el Artículo 12 del Real Decreto del ENS, la gestión del riesgo se extiende a los riesgos derivados del tratamiento de los datos personales.

8. Desarrollo de la política de Seguridad de la información.

Como complemento a la presente política y sirviendo ésta como base, OXIGEN ha desarrollado un Compendio de políticas y normativas de seguridad de la información.

En cumplimiento del artículo 12 del Real Decreto del ENS, la presente Política de Seguridad se desarrollará aplicando los siguientes requisitos mínimos sobre organización e implantación de los diferentes procesos de seguridad:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de la actividad y detección de código dañino.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

9. Formación y concienciación

Todos los miembros tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y el Compendio de Políticas y Normativas de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.
Todos los miembros atenderán a sesiones de concienciación en materia de seguridad. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación. Las personas con responsabilidad en el uso, operación o administración de sistemas recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.
La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo

10. Desarrollo y Control documental

La presente Política y toda la documentación establecida en OXIGEN dentro del alcance definido en el punto 2, siguen las directrices del procedimiento de control de la documentación "APY-PRC-003-IND-Informacion documentada". En este procedimiento se incluyen las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

11. Auditorías

El Comité de Seguridad de OXIGEN garantiza y verifica, mediante auditorías internas y externas, el grado de cumplimiento de los requisitos de la Norma ISO/IEC 27001:2018 y

ENS (Real Decreto 311/202) dentro del marco regulatorio legal aplicable en materia de seguridad de la información y que éstas son operadas e implementadas correctamente, responsabilizándose del cumplimiento de las medidas correctivas que hayan podido determinarse con el fin de mantener la mejora continua.

12. Terceras partes

Cuando OXIGEN preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la OXIGEN utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, 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. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad 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 antes de seguir adelante.

13.Validez y actualización

Esta política es revisada y validada por el Comité de la Seguridad mediante firma y distribuida a las partes interesadas. Desde el momento de su publicación, será revisada siempre que se produzcan cambios significativos, y como mínimo una vez al año.

El objetivo de las revisiones periódicas es adecuarla a los cambios en el contexto de la organización, con atención a las cuestiones externas e internas, analizándose las incidencias acaecidas de seguridad de la información y las No Conformidades encontradas en el SGSI. Todo ello armonizado con los resultados de los diferentes procesos de apreciación del riesgo.

Al revisar la Política también se revisará todas las Normas y demás documentos que la desarrollan, siguiendo un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la empresa y cambios organizacionales, cambio en la infraestructura, desarrollo de nuevos servicios, entre otros.

Como consecuencia se elaborará una lista de objetivos y acciones a emprender y ejecutar durante el año siguiente para garantizar la Seguridad de la Información y el buen uso de los recursos que la soportan y tratan en OXIGEN.

14. Sanciones

El incumplimiento de la Política de Seguridad de la Información tendrá como consecuencia la aplicación de sanciones, conforme a la magnitud y características del aspecto no cumplido, de acuerdo con la legislación laboral vigente y con los acuerdos específicos entre OXIGEN y su personal.

Sant Cugat, 10 de Abril de 2024

CEO de OXIGEN

Benjamin Rovira Guasch

39730083K
BENJAMIN ROVIRA
(R: B67849315)

Firmado digitalmente por 39730083K BENJAMIN ROVIRA (R: B67849315)
Fecha: 2024.05.23 14:43:05 +02'00'

Comité de Seguridad OXIGEN

Gustau Serra
Oriol Rosa
Juan Lorente
Benjamín Rovira