POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INFORMACIÓN DE USO PÚBLICO

Cuadro de Control

Título:	Política de Seguridad de la Información
Tipo de documento:	Normativa
Nombre del Fichero:	PO-Política de Seguridad
Clasificación:	Uso Público
Estado:	Aprobado
Autor:	Consultor Externo

Lista de distribución	
Corporativa	Todos los colaboradores de la empresa, clientes y proveedores

Control de Cambios

Versión	Fecha	Autor	Descripción del Cambio

ÍNDICE

OBJETO 4

ALCANCE 4

DEFINICIONES Y SIGLAS 4

ESPECIFICACIONES 5

- Objetivos de la Política de Seguridad de la Información 5
- Gestión del riesgo 6
- Roles, responsabilidades y autoridades 6
- Marco para la fijación de objetivos de seguridad de la información 6
- Objetivos del SGSI 7
- Organización y responsabilidades 8
- Aplicación de la política 8
- Formación y concienciación 8
- Auditoría 9
- Validez y actualización 9

Referencias 9

Sanciones 9

Ratificación 10

1 OBJETO

Esta política tiene por objeto facilitar las directivas o directrices que deben seguirse para proteger la información de la Organización de una amplia gama de amenazas, a fin de:

- Garantizar la seguridad de las operaciones realizadas, mediante los Sistemas de Información.
- Minimizar los riesgos de daño.
- Asegurar el cumplimiento de los objetivos de la Organización.

Optimia tiene la voluntad de conseguir que los principios de la Política de Seguridad de la Información formen parte de la cultura de la Organización, para lo cual ha implementado un Sistema de Gestión de la Seguridad de la Información en base a un estándar reconocido internacionalmente.

Todo el personal de Optimia, incluyendo colaboradores, proveedores y la dirección, debe conocer y cumplir esta política.

Esta Política se desarrollará mediante normativa, procedimientos, instrucciones operativas, guías, manuales y todos aquellos instrumentos organizativos considerados útiles para alcanzar sus objetivos.

2 ALCANCE

El alcance de la Política de Seguridad de la Información coincide con el alcance del SGSI que se establece en el documento "**IN-Contexto de la organización**".

Con este documento se desarrollan los requisitos exigidos por la Norma ISO/IEC 27001:2013 en su apartado: 5.2 "Política".

3 DEFINICIONES Y SIGLAS

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 Información:** Se refiere a un conjunto de recursos relacionados y organizados para el tratamiento de información, según determinados procedimientos, tanto informáticos como manuales.

4 ESPECIFICACIONES

4.1 Objetivos de la Política de Seguridad de la Información

El objetivo principal de la creación de esta Política de Seguridad de la Información, por parte del Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información (SGSI) y de la Dirección de Optimia, es garantizar a los clientes y usuarios de los servicios el acceso a la información con la calidad y el nivel de servicio que se requieren para el desempeño acordado, así como evitar serias pérdidas o alteración de la información y accesos no autorizados a la misma.

Se establece un marco para la consecución de los objetivos de seguridad de la información para la Organización. Dichos objetivos se alcanzarán a través de una serie de medidas organizativas y de normas concretas y claramente definidas.

Esta Política de Seguridad será mantenida, actualizada y adecuada a los fines de la organización.

Los principios que deben respetarse, en base a las dimensiones básicas de la seguridad, son los siguientes:

- **Confidencialidad**: Propiedad por la cual únicamente puede acceder a la información gestionada por Optimia quién esté autorizado para ello, previa identificación, en el momento y por los medios habilitados.

- **Integridad:** propiedad que garantiza la validez, exactitud y completitud de la información gestionada por Optimia, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación y permitiendo que sea modificada únicamente por quién esté autorizado para ello.

- **Disponibilidad:** propiedad de ser accesible y utilizable en los intervalos acordados. La información gestionada por Optimia es accesible y utilizable por los clientes y usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.

Adicionalmente, dado que cualquier Sistema de Gestión de la Seguridad de la Información debe cumplir con la legislación vigente, se atenderá al siguiente principio:

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta Optimia, especialmente en materia de protección de datos personales.

4.2 Gestión del riesgo

La gestión de la Seguridad de la Información en Optimia está basada en el riesgo, de conformidad con la Norma internacional ISO/IEC 27001:2013.

Se articula mediante un proceso general de apreciación y tratamiento del riesgo, que potencialmente pueden afectar a la seguridad de la información de los servicios prestados, consistente en:

- **Identificar las amenazas**, que aprovecharán vulnerabilidades de los Sistemas de Información que soportan, o de los que depende, la seguridad de la información.
- **Analizar el riesgo**, en base a la consecuencia de materializarse la amenaza y de la probabilidad de ocurrencia.
- **Evaluar el riesgo,** según un nivel previamente establecido y aprobado de riesgo ampliamente aceptable, tolerable e inaceptable.
- **Tratar el riesgo** inaceptable, mediante los controles o salvaguardas adecuadas.

Dicho proceso es cíclico y debe llevarse a cabo de forma periódica, como mínimo una vez al año. Para cada riesgo identificado se asignará un propietario, pudiendo recaer múltiples responsabilidades en una misma persona o comité.

4.3 Roles, responsabilidades y autoridades

La organización de la seguridad de la información se organiza en torno a un Sistema de Gestión de Seguridad de la Información (SGSI) y a una serie de comités y roles involucrados en el ámbito del mismo, descritos en el documento "**IN-Roles responsabilidades y autoridades**".

4.4 Marco para la fijación de objetivos de seguridad de la información

La fijación de objetivos de seguridad de la información se realiza teniendo en cuenta las siguientes entradas:

- Informes del Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información, aprobados por la Dirección de Optimia.

- Oportunidades de mejora encontradas durante la operación del SGSI.

En la fijación de objetivos, se debe tener en cuenta que los mismos deben ser medibles y alcanzables, de ahí que la planificación para su consecución deba incluir:

- Lo que se va a hacer
- Los recursos necesarios
- Quién será el responsable
- El plazo para su consecución
- Cómo se evaluarán los resultados.
- Si procede, el indicador asociado a dicho objetivo.

La Dirección, junto con el Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información, se responsabilizará de definir los objetivos de seguridad de la información para Optimia. Éstos deben ser específicos y consecuentes con su Política de Seguridad de la Información, misión, visión y valores.

4.5 Objetivos del SGSI

El SGSI de Optimia debe garantizar:

- Que se desarrollen políticas, normativas, procedimientos y guías operativas para apoyar la política de seguridad de la información.
- Que se identifique la información que deba ser protegida.
- Que se establezca y mantenga la gestión del riesgo alineada con los requerimientos de la política del SGSI y la estrategia de Optimia.
- Que se establezca una metodología para la apreciación y tratamiento del riesgo.
- Que se establezcan criterios con los que medir el nivel de cumplimiento del SGSI.
- Que se revise el nivel de cumplimiento del SGSI.
- Que se corrijan las no conformidades mediante la implementación de acciones correctivas.
- Que el personal reciba formación y concienciación sobre la seguridad de la información.
- Que todo el personal sea informado sobre la obligación de cumplimiento de la política de seguridad de la información.
- La asignación de los recursos necesarios para gestionar el SGSI.

- La identificación y cumplimiento de todos los requerimientos legales, regulatorios y contractuales.
- Que se identifiquen y analicen las implicaciones de seguridad de la información respecto a los requerimientos de negocio.
- Que se mida el grado de madurez del propio sistema de gestión de la seguridad de la información.
- Que se realice la mejora continua sobre el SGSI.

4.6 Organización y responsabilidades

- La Dirección General de Optimia es la responsable de aprobar la presente política.
- El Comité de Gestión de la Seguridad de la Información es responsable de revisar la presente política.
- El Responsable de seguridad del SGSI es el responsable de mantener la presente política.

Esta política debe ser revisada regularmente junto al resto de las Políticas Corporativas en base al esquema de revisión acordado, y siempre que se realicen cambios relevantes, con el fin de asegurar que esté alineada con la estrategia de la compañía.

4.7 Aplicación de la política

Optimia ha desarrollado el presente documento que contiene la Política General para la Seguridad de la Información y que ha sido aprobada por la Dirección General y dada a conocer a todo el personal de la empresa.

4.8 Formación y concienciación

El Responsable de Seguridad del Sistema de Gestión de Seguridad de la Información debe garantizar que todo el personal involucrado en el SGSI conoce esta política, sus objetivos y procesos, a través de su divulgación, acciones formativas y acciones de concienciación.

También debe garantizar la distribución de los documentos que aplican a cada nivel, de acuerdo a los diferentes roles definidos en la compañía.

4.9 Auditoría

La Dirección General de Optimia debe garantizar y verificar, mediante auditorías internas y externas, el grado de cumplimiento de las directrices de esta Política 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.

4.10 Validez y actualización

Esta política es efectiva desde el momento de su publicación y se revisa 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 revisarán todas las Normas y demás documentos que la desarrollan, siguiendo un proceso de actualización periódica sujeto a los cambios relevantes que pudieran acontecer: crecimiento de la empresa y cambios organizacionales, cambios 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 Optimia.

5 Referencias

- IN-Contexto de la organización
- IN-Roles responsabilidades y autoridades

6 Sanciones

El incumplimiento de la Política de Seguridad de la Información y demás normativas y procedimientos que la desarrollen, tendrá como consecuencia la aplicación de sanciones, conforme a la magnitud y características del aspecto no cumplido, de acuerdo con la legislación laboral vigente.

7 RATIFICACIÓN

Todos los abajo firmantes asumen y aceptan plenamente el contenido de esta Política y se comprometen a aplicarla en sus respectivas áreas para conseguir el correcto funcionamiento del Sistema de Gestión de la Seguridad de la Información.

Tarragona,1 de Julio de 2021

Manel Urquizar

La Dirección General

Abigail Floresta

El responsable del SGSI