POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de la **Optima Grupo**, en el marco de sus competencias para establecer las políticas y estrategias de la organización, ha aprobado la presente Política de Seguridad de la Información (en adelante, la "Política").

El objetivo de esta Política, dirigida a todos los grupos de interés, es definir y establecer los principios, criterios y objetivos de mejora que rigen las actuaciones en materia de seguridad de la información en línea con las directrices marcadas por la norma ISO27001 en lo relativo a los servicios de prestación de servicios de limpieza técnica y general, servicios de atención domiciliaria, mantenimiento e instalaciones, servicios energéticos, jardinería, servicios auxiliares y de soporte a terceros diseño y desarrollo de itinerarios de inserción laboral y atención psicosocial a personas con discapacidad.

1. Finalidad

Optima Grupo asume la seguridad de la información asociada a sus servicios como uno de los factores clave en la realización de sus actividades con objeto de garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad, protegiendo los datos personales, la privacidad de la información y los sistemas de información contra accesos indebidos y modificaciones no autorizadas.

Forma parte de la política estratégica de **Optima Grupo** la implantación y el desarrollo de un Sistema de Gestión de Seguridad de la Información basado en la identificación, protección, detección, respuesta y recuperación de los sistemas de información, aportando para ello la Dirección de la compañía, los recursos necesarios para su consecución.

Optima Grupo, consciente de la necesidad de integrar todas las herramientas y los medios necesarios para prestar sus servicios con eficiencia, calidad y en un entorno seguro de gestión de la información, incidirá en todas aquellas medidas y actuaciones que logren reducir, minimizar, transferir o evitar los riesgos y permitan aprovechar las oportunidades para su sistema de gestión.

A tal efecto, la Dirección de **Optima Grupo** se compromete a mejorar continuamente el Sistema de Gestión de Seguridad de la Información implantado, en las revisiones periódicas que mantiene anualmente y mediante el establecimiento de objetivos y acciones de mejora.

2. Principios Generales

Mediante esta Política, **Optima Grupo** asume y promueve los siguientes principios generales que deben guiar todas sus actividades relativas al Servicio de Asistencia domiciliaria:

a. Dirigir nuestros esfuerzos a la prevención de errores, así como a su corrección, control y gestión.
b. Fomentar la participación de todos para conseguir los objetivos establecidos por **Optima Grupo**, lo que redundará en el bien de nuestros empleados, clientes y otras partes interesadas.
c. Tomar la formación continua y la concienciación como uno de los principales pilares en los que se sustenta la seguridad de la información.
d. Asegurar que **Optima Grupo** cumple con todos los requisitos exigibles por parte de las distintas administraciones y organismos públicos, así como todos los requisitos legales y reglamentarios aplicables,
e. poniendo especial énfasis en aquellos establecidos por la legislación en materia de seguridad de la información.
f. Establecer los procedimientos que sean necesarios para el control, monitorización y prevención de incidentes.

g. Dotarse de herramientas y procedimientos que permitan adaptarse con agilidad a las condiciones cambiantes del entorno.
h. Garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad, así como la debida protección de los datos y los sistemas de información contra accesos indebidos, ciberataques y modificaciones no autorizadas.
i. Garantizar la continuidad del negocio, en cuanto a seguridad de la información se refiere, protegiendo los procesos críticos contra fallos o desastres significativos.
j. Realizar una adecuada evaluación, gestión y tratamiento del riesgo de seguridad de la información para alcanzar un nivel madurez elevado y minimizar el riesgo, priorizando las medidas y controles a implantar acordes con los riesgos identificados y objetivos de negocio.
k. Actuar de manera adecuada y conjunta para prevenir, detectar y responder a los ciberincidentes que pudieran afectar a la seguridad de la información.
l. Mejorar la eficiencia de los controles de seguridad implantados para adaptarse a la evolución de los riesgos y los nuevos entornos tecnológicos.
m. Mejora continua de los procesos y sistemas
n. Crear políticas de contraseñas, implementar mecanismos de autenticación robustos y realizar una adecuada gestión de los usuarios para garantizar el acceso únicamente a los usuarios autorizados.
o. Garantizar una adecuada protección del correo electrónico, servidores y endpoints mediante la implementación de medidas que aseguren la disponibilidad, confidencialidad, integridad, trazabilidad y autenticidad de la información.
p. Establecer políticas de copias de seguridad que incluyan mecanismos anti ransomware, con el objetivo de garantizar una rápida y adecuada recuperación de los datos ante incidentes de seguridad.
q. Realizar parcheos y actualizaciones periódicas de software, asegurando el uso de las versiones más actualizadas de los sistemas, y estando al día de las posibles vulnerabilidades que se descubran.
r. Promover la mejora continua del Sistema de Gestión de la Información, revisando periódicamente su eficacia, adecuación y desempeño, e implantando las acciones necesarias para reforzar de forma continua la protección de la informacion.

OPTIMA FACILITY SL
OPTIMA FACILITY SERVICES SLU
OPTIMA TECHNICAL SERVICES SAU
OPTIMA INCLUSION Y DIVERIDAD SL
PEOPLE PLUS INNOVATION SL
SERVICIOS OPERATIVOS INTERNOS SAU
L´HEURA, CENTRE ESPECIAL DE TREBALL SL
HEURA INCLUSION Y DIVERSIDAD SL
VENTURE TECH INNOVATIONS SL

Julio 2026