POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES Y SEGURIDAD DE LA INFORMACIÓN

Versión 4.0

Madrid, 14 de septiembre, 2023

Autor/es: Beatriz Junquera, Margarita Gluszek
Validado por: Comité de Gestión Integrado
Aprobado por: Órgano de Administración

Proyecto: Sistema de Gestión Integrado (SGI)
Clasificación: Público

NWorld es consciente de la importancia de la seguridad de la información y de la protección de los datos personales, como factores clave para alcanzar la excelencia organizativa, la competitividad en el mercado, la sostenibilidad del negocio y el cumplimiento normativo.

En consecuencia, con lo anterior, el grupo ha establecido en la organización procesos de planificación e implantación de controles, así como de supervisión y mejora, con el fin de garantizar la confidencialidad, la integridad, la autenticidad, la trazabilidad y la disponibilidad de la información y de los servicios.

El Órgano de Administración de **NWorld**, en colaboración con el Comité de Gestión Integrado, tiene la responsabilidad de implantar, actualizar, mejorar, acreditar y mantener el Sistema de Gestión de Seguridad de la Información, de conformidad con las buenas prácticas y los estándares internacionales, en concreto de acuerdo con la norma "UNE-*EN ISO/IEC 27001:2022. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos*".

Se han establecido los siguientes objetivos:

- Establecer un comité de seguridad de la información, con autoridad y competencia para garantizar la confidencialidad, autenticidad, integridad disponibilidad y trazabilidad de la información.

- Implantar la organización de la seguridad, designando a los responsables de la seguridad, de los servicios, de la información, de la protección de datos personales y de los sistemas de información.

- Analizar los riesgos y las amenazas a la seguridad de la información manejada e implantar las medidas, organizativas, operativas y técnicas, necesarias para su debido tratamiento.

- Asegurar la continuidad del negocio ante sucesos que pudieran afectar a los activos críticos.

- Planificar los recursos humanos y tecnológicos, para prestar los servicios a los clientes de acuerdo con los requisitos de seguridad de la información y de conformidad con la legislación vigente.

- Concienciar y formar a todo el personal y colaboradores, en los riesgos y amenazas de la información, la normativa para su prevención y mitigación y la notificación de las incidencias.

- Medir y analizar los objetivos e indicadores de gestión de la seguridad de la información, que permita el seguimiento de los riesgos e incidencias de seguridad y la gestión y mejora de la eficacia de las medidas y controles.

- Implantar los procesos de revisión, auditoría y mejora continua, que garantice el mantenimiento de los controles y medidas de seguridad establecidos.

- Cumplir y demostrar los requisitos legales, normativos y reglamentarios aplicables, con especial énfasis en los que garantizan los derechos digitales y la protección de datos personales.

NWorld y todos sus miembros se comprometen a desarrollar su actividad conforme a la legislación vigente a nivel nacional e internacional en materia de protección de datos, prestando especial atención a los postulados del 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 esos datos (en adelante, RGPD); y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (en adelante, LOPD).

NWorld cuenta con un Delegado de Protección de Datos (DPO) encargado de supervisar el cumplimiento en materia de protección de datos.

Las actuaciones del grupo y de todos sus empleados a la hora de llevar a cabo el tratamiento de los datos personales están alineadas con los principios básicos recogidos en el artículo 5 del RGPD:

a) Principio de licitud, transparencia y lealtad.

b) Principio de limitación de la finalidad. Implica que los datos deben ser tratados con fines determinados, explícitos y legítimos, y prohíbe que los datos recogidos sean tratados posteriormente de una manera incompatible con esos fines.

c) Principio de minimización de datos. Se deben aplicar medidas técnicas y organizativas para garantizar que solo se tratan los datos estrictamente necesarios ("adecuados, pertinentes y limitados") para cada uno de los fines.

d) Principio de exactitud. Los datos deben de estar actualizados y se deben de suprimir o rectificar cuando sean inexactos.

e) Principio de limitación del plazo de conservación. Una vez logrados los fines del tratamiento, los datos deben ser borrados, bloqueados o anonimizados.

f) Principio de integridad y confidencialidad. El tratamiento debe garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales.

El responsable del tratamiento será el encargado de garantizar la actuación conforme a los principios anteriores y demostrar su cumplimiento, de acuerdo con el principio de responsabilidad proactiva.

El Órgano de Administración de **NWorld**, en consecuencia, con lo anterior, está comprometido con la asignación de los recursos humanos y materiales, razonables y proporcionales, para la consecución de los objetivos anteriores.

La responsabilidad del buen funcionamiento del Sistema de Gestión de Seguridad de la Información recae, pues, en el Órgano de Administración, delegando en el Comité de Gestión Integrado y en el Responsable de Seguridad de la Información la autoridad y las competencias necesarias para su implantación efectiva, su acreditación, su mantenimiento y mejora, contando, para ello, con el respaldo del equipo directivo y del personal y colaboradores de **NWorld**