POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL USO Y PRESTACIÓN DE SERVICIOS EN LA NUBE

Versión 1.0

Madrid, 10 de septiembre, 2025

Autor/es: Responsable de Seguridad
Validado por: Comité de Seguridad y Privacidad de la Información
Aprobado por: Órgano de Administración

Proyecto: Sistema de Gestión de Seguridad de la Información (SGSI)
Clasificación: Público

Contenido

NWorld ha adoptado un sistema de gestión de la seguridad y privacidad de la información como marco para la planificación, implantación, mejora y certificación de la conformidad con los principales estándares internacionales, así como para el cumplimiento proactivo de las obligaciones legales.

El sistema de gestión de la seguridad y privacidad de la información (SGSI) de NWorld permite garantizar la confidencialidad, integridad y autenticidad de los datos de nuestros clientes, colaboradores, empleados y candidatos, así como la disponibilidad de las operaciones que desarrollamos y servicios que prestamos.

Con la presente Política ampliamos y reforzamos nuestro compromiso con la seguridad y privacidad de la información del uso y prestación de servicios en la nube

1. OBJETO

El presente documento tiene por finalidad establecer los principios básicos en materia de seguridad y privacidad de la Información para el uso y la prestación de los servicios en la nube.

2. ALCANCE

Lo dispuesto en la presente Política es de obligado cumplimiento para todo empleado o colaborador de NWorld que sea usuario y/o que preste servicios o desarrolle soluciones en la nube.
Las modalidades de prestación de los servicios en la nube incluidas en el ámbito de esta Política son:

- Software como servicio (SaaS)
- Infraestructura como Servicio (IaaS)
- Plataforma como Servicio (PaaS)

Asimismo, la presente Política es de aplicación a los proveedores de la cadena de suministro de los servicios o de soluciones en la nube de NWorld en lo aplicable.

3. MARCO NORMATIVO Y REGULATORIO

El cumplimiento proactivo de la normativa y de la regulación se considera un aspecto clave para la sostenibilidad del negocio de NWorld cuyo desarrollo y control de la normativa interna deberá garantizar la prevención de incumplimientos, la evitación de sanciones y el daño reputacional.

El marco de referencia de esta Política es el normativo de adhesión voluntaria constituido por los estándares siguientes:

- UNE-ISO/IEC 27001:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.

(ISO/IEC 27001:2022).

- UNE-EN ISO/IEC 27002:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información. (ISO/IEC 27002:2022).

- UNE-EN ISO/IEC 27018:2020 Tecnología de la Información. Técnicas de seguridad. Código de práctica para la protección de identificación personal (PII) en nubes públicas que actúan como procesadores PII (ISO/IEC 27018:2019)

- UNE-EN ISO/IEC 27017:2021. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para los servicios en nube. (ISO/IEC 27017:2015).

- UNE-EN ISO/IEC 27701:2021. Técnicas de seguridad. Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información. Requisitos y directrices. (ISO/IEC 27701:2019).

Asimismo, NWorld establece como marco de cumplimiento la legislación que le es aplicable, entre la que destaca la siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- 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.

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

- Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011.

- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento

(UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

NWorld mantiene un registro detallado de normativa y regulación de aplicación para su debida evaluación y cumplimiento que pone a disposición, bajo solicitud, de las partes interesadas.

4. REQUISITOS ESENCIALES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NWorld como proveedor de servicios en la nube especifica los requisitos esenciales de seguridad y privacidad que se aplican al ciclo de vida, desde la especificación de requisitos, diseño, implementación, puesta en operación, producción, soporte y mantenimiento, así como la reversibilidad del servicio al cliente.

La línea base de requisitos esenciales se documenta en forma de catálogo, que se adaptará para cada proveedor, cliente o proyecto para dar cumplimiento a los requisitos normativos y contractuales establecidos en cada caso.

Los requisitos esenciales para el uso y prestación de servicios en la nube se establecerán en relación con las dimensiones de confidencialidad, integridad, trazabilidad y autenticidad de la información y de disponibilidad de los servicios.

5. GESTIÓN DE RIESGOS

NWorld como usuario y proveedor de servicios en la nube promueve una cultura de gestión de riesgos que incluya la evaluación y la implantación de medidas de tratamiento de los riesgos para el uso y prestación de servicios en la nube, de acuerdo con una metodología reconocida internacionalmente que tiene en cuenta las obligaciones reglamentarias, los principales estándares internacionales y los requisitos contractuales.

La gestión de riesgos incluye los controles o medidas para identificar y prevenir cualquier vulnerabilidad de terceros y amenazas del uso y prestación de servicios en la nube, así como para detectar, responder y mitigar el impacto en caso de un incidente.

La seguridad de las redes y los sistemas de información del uso y prestación de servicios en la nube contempla, en especial, la confidencialidad e integridad de los datos almacenados, transmitidos y procesados en la nube, con el objetivo de prevenir y evitar cualquier acceso a la información que no haya sido no autorizado.

6. SEPARACIÓN Y VIRTUALIZACIÓN DE ENTORNOS CON INFORMACIÓN SENSIBLE Y/O SERVICIOS ESENCIALES O CRÍTICOS

NWorld como proveedor de servicios en la nube adopta la obligación de segregar los entornos lógicos de distintos grupos de usuarios u organizaciones si se gestiona información clasificada como sensible para garantizar el principio de confidencialidad, integridad y disponibilidad, impidiendo que el usuario de una organización pueda acceder a los datos o recursos de otra.

La forma de lograr esta segregación será mediante la creación de instancias o “tenants” separadas cuando se establezca como requisito esencial la separación clara y robusta de la información cuando se manejan datos de diferentes organizaciones para satisfacer los requisitos siguientes.

- Confidencialidad: Se deberá asegurar que el control de acceso a la información solo sea accesible para aquellos usuarios que están autorizados.

- Integridad: Se deberán implantar medidas para proteger la información de modificaciones no autorizadas.

- Disponibilidad: Se deberá separar los recursos para que un incidente que afecte a una instancia o “tenant” no comprometa la disponibilidad de los servicios de otras organizaciones que prestan servicios esenciales o críticos, limitando el alcance de los incidentes.

7. CONTROL DE ACCESO A LOS ACTIVOS DEL CLIENTE EN LA NUBE

NWorld como proveedor de servicios en la nube adopta la obligación de controlar el acceso a los activos del cliente a su personal debidamente autorizado, para las tareas de despliegue, administración y mantenimiento acordadas y/o siguiendo las instrucciones del cliente.

NWorld, bajo el principio de “necesidad de conocer”, aplicará los controles de autorización, identificación y autenticación multifactor establecidos por NWorld y/o por el cliente.

Los permisos de acceso son revisados y validados periódicamente para garantizar su actualización y vigencia.

Las conexiones remotas de las personas autorizadas por NWorld serán realizadas a través de una VPN SSL y las conexiones mediante accesos móviles asimismo serán realizadas a través de HTTPS.

El acceso a los activos del cliente, en cualquier caso, será monitorizado, registrado y revisado

periódicamente o bien cuando sea necesario para prevenir, responder o investigar un eventual incidente siguiendo los procedimientos y mecanismos establecidos por NWorld y/o por el cliente.

8. SEGURIDAD DEL CICLO DE VIDA

NWorld como proveedor de soluciones y servicios en la nube adopta la obligación de seguir las mejores prácticas de desarrollo seguro en el ciclo de vida con el propósito de eliminar o reducir el impacto de las posibles amenazas de seguridad antes de la puesta en producción y conservar el nivel de seguridad durante toda la vida útil.

En consecuencia, se establecen las fases siguientes:

- Durante el diseño y desarrollo de una solución a cliente, bajo los principios de "seguridad desde el diseño" y “seguridad por defecto”, especificando y verificando los requisitos de seguridad de acuerdo con el análisis de riesgos realizado.

- Antes de la puesta en producción ejecutando un análisis de vulnerabilidades y pruebas de intrusión mediante auditorías llevadas a cabo por un tercero cualificado.

La aplicación de la obligación de seguir las mejores prácticas de desarrollo seguro en el ciclo de vida incluye a los proveedores de NWorld de servicios contratados, implementados o gestionados de plataformas en la nube (IaaS, PaaS, SaaS), así como de provisión de componentes o equipamiento.

9. GESTIÓN Y COMUNICACIÓN DE CAMBIOS

NWorld como proveedor de servicios y soluciones en la nube adopta la obligación de comunicar al cliente, con la anticipación debida a su implantación los cambios, tales como las actualizaciones, las configuraciones, los cambios de ubicación, etc., evaluando el impacto cuando sea relevante y acordando las ventanas de oportunidad para desplegarlos sin o con la mínima incidencia en los usuarios.

La comunicación de cambios y la evaluación de impacto operativo y/o legal, se realizará siguiendo los procedimientos y canales establecidos por NWorld y/o por el cliente.

NWorld designará para cada cliente una persona de contacto (POC) responsable de canalizar, responder y coordinar toda comunicación relativa a la seguridad y privacidad de la información y la disponibilidad del servicio.

10. CONTINUIDAD DEL SERVICIO

NWorld adopta la obligación de garantizar la continuidad de las soluciones y servicios en la nube de los clientes ante eventuales incidentes de conformidad con los acuerdos de nivel de servicios (ANS o SLA) establecidos.

Para ello, se establecerán medidas para identificar y valorar los activos críticos, así como para planificar, implantar, evaluar y mejorar los planes de recuperación de los servicios.

La aplicación de la obligación incluye a los proveedores de NWorld de servicios contratados, implementados o gestionados de plataformas en la nube (IaaS, PaaS, SaaS), así como de provisión de componentes o equipamiento de conformidad con los acuerdos de nivel de servicios (ANS o SLA) establecidos.

11. NOTIFICACIÓN DE INCIDENTES

NWorld como proveedor de soluciones y servicios en la nube adopta la obligación de notificar al cliente afectado por una incidencia, incumplimientos, violación de seguridad o vulnerabilidad que pueda afectar, con un impacto crítico, muy alto, alto y medio, a la integridad, disponibilidad o confidencialidad de la información gestionada y el servicio prestado.

La notificación se deberá producir a través de los canales de comunicación establecidos y dentro de los plazos acordados o legales, de forma que se pueda evidenciar la debido confidencialidad, trazabilidad e integridad de los registros de notificación, información detallada, evaluación de impacto, acciones y responsabilidades de subsanación, análisis de causa raíz, investigación forense y notificación a las autoridades, en su caso.

La aplicación de la obligación incluye a las incidencias, incumplimientos, violación de seguridad o vulnerabilidad originadas por los proveedores de NWorld de servicios contratados, implementados o gestionados de plataformas en la nube (IaaS, PaaS, SaaS), así como de provisión de componentes o equipamiento.

La persona de contacto (POC) designada por NWorld designará para cada cliente responsable de canalizar, responder y coordinar toda comunicación y coordinación relativa a la gestión de una eventual incidencia, incumplimientos, violación de seguridad o vulnerabilidad.

12. PROTECCIÓN DE DATOS PERSONALES

NWorld como proveedor de soluciones y servicios en la nube adopta la obligación del cumplimiento proactivo de la regulación en materia de protección de datos personales de los tratamientos que lleva a cabo como responsable y encargado de los clientes.

NWorld designará un Delegado de Protección de Datos encargado de informar y asesorar, así como supervisar, al responsable y encargado de los tratamientos que lleva a cabo del cumplimiento de la regulación en materia de protección de datos personales.

El Delegado de Protección de Datos actuará como punto de contacto de NWorld con las autoridades y organismos reguladores competentes en materia de protección de datos personales.

13. ORGANIZACIÓN DE LA SEGURIDAD Y

PRIVACIDAD DE LA INFORMACIÓN.

El Comité de Seguridad y Privacidad de la Información de NWorld como órgano colegiado está integrado por los responsables siguientes:

- Director de Operaciones (como delegado del Comité de Dirección), que actuará como Presidente del Comité
- Delegado de Protección de Datos (con voz, pero sin voto) que actuará como Secretario del Comité
- Responsable del Sistema
- Responsables de la información y del servicio de las unidades organizativas
- Responsables de Seguridad de las unidades organizativas
- Administradores de Sistemas IT

El Comité de Seguridad y Privacidad de la Información de NWorld elabora y actualiza la presente Política y propone su aprobación al Órgano de Administración.

Además, el Comité desarrollará y aprobará la documentación normativa de seguridad y privacidad para el uso y la prestación de los servicios en la nube y los mecanismos de coordinación y resolución de conflictos entre los diferentes responsables que se resolverán colegiadamente mediante deliberación de los miembros del Comité moderados por la Presidencia del Comité

Los Responsables de la información y del servicio de NWorld serán responsables de valorar y firmar los niveles de seguridad de los activos esenciales de las soluciones y servicios en la nube, documentado en la Categorización, en coordinación con el Responsable del Sistema y los Responsables de Seguridad de NWorld.

Los Responsables de Seguridad de la Información de las unidades organizativas de NWorld comunicarán la presente Política al personal de sus respectivas unidades, así como de coordinarán la implantación de los requisitos de seguridad, mantenimiento y mejora de las medidas y controles de seguridad de los sistemas de información que dan soporte al uso y prestación de servicios en la nube establecidas en la Declaración de aplicabilidad, en coordinación con el Responsable del Sistema y los Administradores de Sistemas IT de NWorld.

El Responsable del Sistema implantará, mantendrá y mejorará las medidas y controles de seguridad establecidas en la Categorización de los sistemas de información que dan soporte al uso y prestación de servicios en la nube y la Declaración de Aplicabilidad vigente, en coordinación con los Responsables y Administradores de Seguridad de NWorld de cada unidad organizativa.

Por último, todo el personal y colaboradores externos serán responsables de cumplir con lo dispuesto en la presente Política, así como de seguir toda la documentación normativa de seguridad y privacidad para el uso y la prestación de los servicios en la nube de NWorld en su desempeño laboral.

14. AUDITORÍAS DE CUMPLIMIENTO

Se realizarán auditorías internas y externas regulares para verificar y acreditar el cumplimiento de los requisitos de los estándares internacionales adoptados voluntariamente, así como de la regulación aplicable.

El Responsable del Sistema, por delegación de la Dirección General de NWorld, coordinará la planificación y ejecución de auditorías internas y externas informando puntualmente a los integrantes del Comité de Seguridad y privacidad de la Información de los resultados, con especial énfasis de las No Conformidades detectadas, observaciones y oportunidades de mejora y del Plan de Acciones Correctivas para su tratamiento y cierre en plazo y forma.

15. DISPOSICIÓN FINAL

La presente Política ha sido aprobada por el Órgano de Administración de NWorld y difundida a todas las partes interesadas de NWorld.

La presente Política será evaluada en las revisiones del sistema de gestión de seguridad de la información por el Órgano de Administración, a través del Comité de Seguridad y Privacidad de la Información, siempre que se produzcan cambios significativos, un incidente de impacto alto o muy alto o crítico o, al menos, una vez al año.

El Órgano de Administración de NWorld dotará de los recursos proporcionales para la implantación efectiva de esta Política, y para su buen desarrollo, tanto en las actividades de implantación como en su mantenimiento, mejora continua y evidencia de cumplimiento.

La presente política estará accesible para todas las partes interesadas y será comunicada y formalmente reconocida por todo el personal y colaboradores de NWorld.