Wolters Kluwer

03/2026

Política de Seguridad de la Información y Continuidad de Negocio

USO PÚBLICO

Control del documento

Detalles del documento	
Título	Política de Seguridad de la Información y Continuidad de Negocio
Estado del documento	Activo
Owner	Comité de Seguridad de la Información

Histórico de cambios

Versión	Última revisión	Owner	Aprobado por	Comentarios
1.0	2024	Comité de Seguridad de la Información	Comité de Dirección de Wolters Kluwer Tax and Accounting	Creación y aprobación de la Política
1.1.	2025	Comité de Seguridad de la Información	Comité de Dirección de Wolters Kluwer Tax and Accounting	Revisión de la Política
1.2.	2026	Comité de Seguridad de la Información	Comité de Dirección de Wolters Kluwer Tax and Accounting	Actualización normativa y de la denominación social de la entidad

Aprobación y entrada en vigor

Texto aprobado en julio de 2024 y revisado en el año 2026 por la Dirección de ***Wolters Kluwer Tax and Accounting España, S.L.U***. Esta Política de Seguridad de la Información y Continuidad de Negocio es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Contenido

1 Introducción

Este documento expone la Política de Seguridad de la Información y Continuidad de Negocio de ***Wolters Kluwer Tax and Accounting España, S.L.U.*** en adelante referenciada como la" Organización". Este sistema debe ser administrado con diligencia para proteger la información durante todo su ciclo de vida, desde su creación hasta su eventual borrado o destrucción, frente a daños accidentales o deliberados que puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información tratada o de los servicios prestados.

2 Objetivo de la política

La política se basa en los principios de las normas ISO/IEC 27001, ISO/IEC 22301 y del Esquema Nacional de Seguridad (ENS), y marca las directrices y el compromiso de la Alta Dirección, dentro del ámbito de alcance y del Contexto de la Organización, alineada con la Estrategia de la Organización y cumpliendo la legislación y normativas de aplicación vigentes, aplicando la gestión y compromiso en la mejora continua.

2.1 Prevención

Para evitar que la información o los servicios se vean perjudicados por incidentes de seguridad, la Organización implementará las medidas mínimas de seguridad determinadas por el ENS, 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.

- **Autorización de sistemas**: Los sistemas deben ser autorizados antes de entrar en operación.
- **Evaluaciones regulares**: La seguridad debe evaluarse regularmente, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- **Revisión por terceros**: Se hará una revisión periódica por parte de terceros para una evaluación independiente.
- **Mejora continua**: Se velará por el mantenimiento y mejora constante de la gestión de la seguridad y la calidad, aportando los recursos necesarios. Para asegurar su eficacia y adecuación continua, esta Política será revisada y actualizada al menos una vez al año, o si se dan cambios significativos en la Organización o el entorno normativo.

2.2 Detección

La Organización establecerá medidas de detección en sus sistemas de información para descubrir la presencia de ciberincidentes y anomalías en la prestación de los servicios, actuando según establece el ENS en los Artículos 8 y 9.

- **Monitorización continua**: Los servicios se monitorizarán continuamente para detectar anomalías.

- **Reevaluación periódica**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
- **Líneas de defensa**: Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros preestablecidos.

2.3 Respuesta

La Organización establecerá mecanismos para responder eficazmente a los incidentes de seguridad, designando puntos de contacto y estableciendo protocolos para el intercambio de información relacionada con los incidentes.

- **Mecanismos de respuesta**: Se establecerán mecanismos para responder eficazmente a incidentes de seguridad.
- **Puntos de contacto**: Se designarán puntos de contacto para las comunicaciones con respecto a incidentes detectados en diferentes áreas de la Organización o en otros organismos.
- **Protocolos de intercambio de información**: Se establecerán protocolos para el intercambio de información relacionada con los incidentes.

2.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, la Organización dispondrá de un Plan de Continuidad de Negocio (PCN) y un Plan de Recuperación ante Desastres (DRP), valorando los posibles escenarios de desastre y estrategias de recuperación, y estableciendo planes de emergencia que se revisan periódicamente.

- **Conservación de datos**: El sistema de información garantizará la conservación de los datos e información en soporte electrónico.
- **Disponibilidad de servicios**: Se dispondrá de los medios, técnicas y procedimientos necesarios para garantizar la recuperación de los servicios más críticos.

3 Misión y Visión

La Organización está firmemente comprometida con el éxito de nuestros clientes, por ello nuestros productos y servicios reflejan la orientación que tenemos hacía sus necesidades, por lo que asegurar la disponibilidad de nuestros procesos de negocio es un objetivo primordial para la Organización.

Así mismo, la información que diariamente tratamos es considerada como un activo de especial importancia y criticidad. Su carácter confidencial y de especial protección, establecido en la Ley de Protección de Datos Personales y Garantías Digitales (LOPD-GDD), se contrapone a la creciente necesidad de acceso para llevar a cabo una adecuada gestión los procesos de negocio, cobrando especial importancia aquellos relacionados con nuestros clientes. Esta situación, en estrecha convivencia con las tecnologías de la información y las comunicaciones, constituye un escenario

en el que deben adoptarse las máximas precauciones para de reducir los riesgos, garantizar la continuidad de negocio y mantener una adecuada seguridad de la información.

Por tanto, y en esta línea, siendo conscientes desde siempre de la importancia y sensibilidad de la información inherente a nuestra actividad, la Organización considera clave el establecimiento de un Sistema de Gestión Integrado (en adelante, *SGI*), el cual está compuesto por un Sistema de Gestión de la Seguridad de la Información (en adelante, *SGSI*) de acuerdo con los requisitos de la norma UNE ISO/IEC 27001 y con los requisitos del Esquema Nacional de Seguridad (en adelante, *ENS*) en sus versiones vigentes, y por un Sistema de Gestión de Continuidad de Negocio (en adelante, *SGCN*) en línea con los requisitos de la norma UNE ISO/IEC 22301 en su versión actual.

Wolters Kluwer Tax and Accounting España, S.L.U. vincula su estrategia de negocio a largo plazo al compromiso de todos los profesionales que forman parte de la Organización en conseguir que nuestros clientes tengan éxito en sus respectivos negocios, en mejorar continuamente nuestros procesos y en cumplir los ambiciosos objetivos que nos marcamos cada año. La Organización aporta a sus proyectos de tecnologías de la información y telecomunicaciones el valor añadido del conocimiento adquirido a lo largo de más de 30 años de desarrollo e innovación de procesos en su campo específico de acción. La Organización trabaja por diferenciarse de la competencia apostando por la calidad de sus productos y servicios, expresando al mismo tiempo un sólido compromiso con la protección del medioambiente, ello está directamente relacionado con el cumplimiento riguroso de las normas de Calidad (ISO 9001) y Medioambiente (ISO 14001) certificadas por AENOR.

4 Alcance

4.1 Alcance subjetivo

Esta política se aplica a todo el ámbito de actuación del alcance establecido para el Sistema de Gestión Integrado por *SGSI*/*ENS* y *SGCN*, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la *Política de Seguridad de la Información y Continuidad de Negocio* y el conjunto de normas de seguridad de la Organización.

Lo establecido en esta política es de obligado cumplimiento para todo el personal de la Organización, así como para todas las entidades y servicios, internos y externos, que manejen información o presten servicios TIC a la Organización. Se establecerán procedimientos específicos para garantizar la seguridad de la información manejada por terceros.

4.2 Alcance objetivo

La división de **Wolters Kluwer Tax and Accounting España, S.L.U.** delimita el alcance de su SGI a soluciones laborales, de recursos humanos, fiscales, contables, de facturación, gestión documental y gestión de identidades en modalidad online, en sus procesos de desarrollo de software, gestión de infraestructura y soporte postventa.

Todos los miembros de la Organización que estén bajo alcance tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad correspondiente, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

5 Principios Básicos, Requisitos mínimos y Compromisos con la seguridad de la información

La presente política se sustenta en los siguientes **compromisos y principios** fundamentales.

5.1 Principios

- **La seguridad como un proceso integral.**
    - La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. por ello, la Organización estructura la seguridad de la información mediante su sistema de gestión de seguridad de la información y continuidad del negocio, aunando procesos, procedimientos y medidas de seguridad con carácter integral y una visión global de la seguridad.
    - Se presta la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de Organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad. Por ello, la Organización realiza acciones de concienciación continuas y formaciones periódicas en ciclos de planificación anual.
- **Gestión de la seguridad basada en los riesgos.**
    - El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad y constituye una actividad continua y permanentemente actualizada. Por ello, la Organización analiza los riesgos de seguridad de la información al menos con carácter anual mediante la realización de un análisis de riesgo formal.
    - La gestión de los riesgos permite el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. Para ello, la Organización realiza los planes de tratamiento de riesgos y aplica las medidas de seguridad necesarias para la reducción del riesgo a umbrales aceptables.
- **Prevención, detección, respuesta y conservación.**
    - La seguridad del sistema contempla las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios

que presta. Por ello, se realiza un seguimiento continuo de la actualización de los sistemas de trabajo para prevenir las vulnerabilidades; y se realizan análisis de vulnerabilidades periódicos.

- Las medidas de prevención incorporan componentes orientados a la disuasión o a la reducción de la superficie de exposición, tales como la protección perimetral de los distintos entornos y el control de accesos y privilegios, para eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.
- En materia de medidas de detección, dirigidas a descubrir la presencia de un ciberincidente, la Organización cuenta con herramientas de monitorización continua de los sistemas de información y alertas de seguridad preprogramadas para la detección de eventos significativos en los sistemas de información.
- Las medidas de respuesta, orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad, cuentan con un equipo de profesionales en materia de seguridad de la información tanto a nivel español como internacional para la gestión de incidentes.
- Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantiza la conservación de los datos e información en soporte electrónico mediante la gestión de copias de seguridad de los sistemas e información críticos para la continuidad de los servicios y los planes de continuidad existentes.
- De igual modo, el sistema mantiene disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que son la base para la preservación del patrimonio digital.

- **Existencia de Líneas de defensa.**
  - El sistema de información ha dispone de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas es comprometida, permite:
    - Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.
    - Minimizar el impacto final sobre el mismo.
  - Las líneas de defensa se encuentran constituidas por medidas de naturaleza organizativa, física y lógica, mediante los procedimientos organizativos para la seguridad de la información, la protección física de los sistemas críticos en zonas de seguridad habilitadas y acondicionadas para ello y hasta la protección perimetral y medidas de monitorización, gestión de accesos, mantenimiento y operación de los diferentes entornos informáticos.

- **Vigilancia continua y Reevaluación periódica.**
  - La vigilancia continua permite la detección de actividades o comportamientos anómalos y su oportuna respuesta mediante la monitorización continua de los sistemas de información y herramientas de seguridad y la configuración de alertas de seguridad.

- La evaluación permanente del estado de la seguridad de los activos permite medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. Por ello, la Organización cuenta con un complejo sistema de métricas e indicadores de seguridad y cuadros de mandos dinámicos para su gestión.
- Las medidas de seguridad se reevalúan y actualizan periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario. A partir del análisis de las métricas e indicadores de seguridad y la gestión de riesgos.

- **Diferenciación de responsabilidades.**
  - En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema entre otros, tal y como refleja la presente política que detalla, en su correspondiente apartado, las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos. Estando la responsabilidad de la seguridad de los sistemas de información diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.
- **Principio de seguridad y protección de todo el personal** como primera premisa y objetivo prioritario tanto situaciones de normalidad como de contingencia.
- **Principio de la Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad** de la información, asegurando:
  - Su Disponibilidad, asegurando y garantizando que los usuarios autorizados tienen acceso a la información cuando lo requieren.
  - Su Integridad, garantizando su exactitud y evitando que sea alterada.
  - Su Confidencialidad, velando que sólo quienes estén autorizados puedan acceder a la información y no se produzcan fugas de esta.
  - Su Autenticidad para garantizar que quien accede, de quien la recibimos y a quien la entregamos son quien dicen ser.
  - Su Trazabilidad de los accesos y tratamientos realizados sobre la información y garantizando poder tener conocimiento en todo momento de Cuando, Donde, Quien y Qué ocurre con la información.
- **Principio de cumplimiento normativo**: Ajustando nuestros sistemas de información a la normativa legal vigente que afecte a la seguridad de la información y continuidad de negocio, en especial aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, comunicaciones y servicios electrónicos.

  Prestando especial atención a aquellos relacionados con los Datos Personales:
  - Principio de *"Licitud, transparencia y lealtad"*, que consiste en que los datos son tratados de manera lícita, leal y transparente para el interesado.
  - Principio de *"limitación de la finalidad"* que implica una finalidad legitima al recoger y tratar los datos.

  - Principio de *"minimización de datos"*, es decir, que los datos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
  - Los datos, según el *"principio de exactitud"*, deben ser exactos y cuando sea necesario, actualizados.
  - El principio de *"limitación del plazo de conservación"* tratado los datos adecuados, pertinentes y necesarios para una finalidad, y limitando su conservación en el tiempo a lo estrictamente necesario.
  - Principio de *"integridad y confidencialidad"* aplicando las medidas técnicas y organizativas apropiadas y de forma proactiva, con el objetivo de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad.

- **Compromiso en el ejercicio de los derechos sobre Datos Personales de los usuarios** estableciendo procedimientos para garantizarlos y facilitarlos: Transparencia e Información, Rectificación, Cancelación, Oposición, Supresión (Olvido), Limitación de los tratamientos y Portabilidad de los datos
- **Principio de proporcionalidad:** La implantación de controles que mitiguen los riesgos debe hacerse buscando el equilibrio entre las medidas de seguridad y continuidad, la naturaleza de la información y las amenazas a las que están sujetos.
- **Principio de responsabilidad:** Todos los empleados de la Organización son responsables de la seguridad de la información y esta es extensiva a terceros que estén incluidos en su alcance. Así mismo nos comprometemos a que todos los empleados, dispongan de la formación necesaria para el cumplimiento de sus funciones y la adecuada concienciación en seguridad de la información, continuidad de negocio y protección de datos para cumplir eficazmente con sus compromisos en seguridad.
- **Principio de mejora continua:** Implantando un modelo dinámico de mejora y actualización del *SGI*. Entendemos la gestión de la seguridad de la información y continuidad de negocio como un proceso de mejora continua y constante adaptación a los cambios operativos y tecnológicos que se producen en la Organización y su entorno.
- **Principio de permanente disposición y colaboración** con las autoridades y organismos regulatorios en caso de desastre o necesidad, como parte de la vocación de servicio de *Wolters Kluwer* y de la responsabilidad para con la sociedad en la que desarrolla su actividad.
- **Principio de continuidad de negocio:** se implantarán los mecanismos necesarios para gestionar la recuperación tras una interrupción del servicio y restaurar los procesos básicos.
- **Principio de gestión del riesgo:** Con una metodología clara, periódicamente se realizarán análisis de impactos en el negocio y análisis de riesgos, se evaluarán y definirán planes de tratamiento de los riesgos detectados
- Si la opción seleccionada es tratar los riesgos, estos deberán ser minimizados hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.
- Todos los sistemas deben realizar análisis de riesgos regularmente, al menos una vez al año, o cuando haya cambios significativos en la información manejada, los servicios prestados, o incidentes graves de seguridad.

5.2 Requisitos mínimos

La gestión de la seguridad de la información de la Organización se desarrolla aplicando los siguientes requisitos mínimos:

1. Organización e implantación del proceso de seguridad: por medio de su sistema de gestión de seguridad de la información y continuidad del negocio que analiza y establece los procesos de seguridad necesarios para la Organización
2. Análisis y gestión de los riesgos: mediante el análisis de riesgos periódico, al menos con carácter anual, se identifican los riesgos y se generan planes de acción para llevar los riesgos a umbrales aceptables.
3. Gestión de personal mediante la formación y la concienciación continua y la aplicación de la seguridad en el personal desde los procesos de selección.
4. Profesionalidad: mediante la capacitación continua del personal y el seguimiento y adaptación continua a los cambios tecnológicos y las novedades del sector.
5. Autorización y control de los accesos: mediante mecanismos para la gestión y control de accesos y las herramientas de seguridad implementadas.
6. Protección de las instalaciones, haciendo gran hincapié en la seguridad física y la identificación, adecuación y protección específica de las áreas de seguridad.
7. Adquisición de productos de seguridad y contratación de servicios de seguridad, mediante la evaluación y análisis de cada producto, servicio y proveedor con carácter previo a su adquisición.
8. Mínimo privilegio, gestionando los accesos y permisos en base al principio de necesidad de conocer.
9. Integridad y actualización del sistema, mediante la monitorización continua del estado de los sistemas y los mecanismos automatizados de actualización de sistemas periódicos existentes en la Organización.
10. Protección de la información almacenada y en tránsito, mediante las herramientas de seguridad implementadas y la clasificación de la información.
11. Prevención ante otros sistemas de información interconectados, mediante el análisis específico de cada entorno y sus interconexiones para la implementación de medidas perimetrales y la aplicación de configuraciones seguras.
12. Registro de la actividad y detección de código dañino mediante la monitorización continua y las herramientas específicas de protección frente a malware con aplicación de alertas de seguridad.
13. Incidentes de seguridad: mediante un grupo de profesionales dedicados a la gestión de los incidentes de la Organización tanto a nivel local como internacional.
14. Continuidad de la actividad, mediante su sistema de gestión de la continuidad, asegurando esta mediante los planes de continuidad del servicio y los planes de recuperación.
15. Mejora continua del proceso de seguridad, analizando y evaluando continuamente los procesos para identificar posibles mejoras y generar los planes de acción correspondiente.

5.3 Compromisos

- Lograr un liderazgo y Organización efectiva del *SGI*, dotándolo de recursos económicos y humanos y asegurando que la política y los objetivos que se establezcan sean compatibles con la estrategia de la Organización.
- Definir e implantar, en el ámbito organizativo, operativo, técnico y/o humano, las correspondientes políticas, instrucciones, medidas, controles, etc. de seguridad de la información y continuidad de negocio.
- Apostar por la mejora continua del *SGI* para la mejora del desempeño, y la implementación de medidas de seguridad eficaces y eficientes en base al entorno actual y previsto de amenazas.
- Establecer anualmente objetivos para ámbitos específicos alineados con las normas de referencia del *SGI*.
- Cumplir con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales del *SGI*.
- Establecer medidas de emergencia que protejan la integridad física de nuestros empleados en caso de que se presente una contingencia en las instalaciones de la Organización.
- Disponer de una gestión del riesgo con una metodología clara, en base a la que periódicamente se realicen análisis de impactos en el negocio y análisis de riesgos, los evalué y defina planes de tratamiento de dicho riesgo.
- Gestionar de forma eficaz la respuesta frente a incidentes de seguridad o situaciones de emergencia con objeto de asegurar la continuidad de los procesos de negocio esenciales y los sistemas de información críticos.
- Disponer de un marco de referencia y actuación para la protección de los procesos de negocio y activos de los sistemas de información frente a amenazas, internas o externas, deliberadas o involuntarias, con la finalidad de garantizar la continuidad de negocio, la seguridad de la información y su confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.
- Identificar e inventariar los activos de información y tratamientos de esta, con objeto de dotar a la Organización de un sistema de clasificación, permitiendo establecer y definir distintos escenarios de control en función de los criterios que se establezcan (formato, volumen, contenido, grado de actualización, etc.).
- Obtener la rápida recuperación de los servicios críticos ante una situación de desastre y conseguir la vuelta al estado de normalidad, en los tiempos establecidos en el análisis de impacto de negocio.
- Controlar los procesos de intercambio/comunicación de información con terceras partes (proveedores, organismos oficiales, empresas colaboradoras, etc.).
- Alineación de la política corporativa de seguridad de la información y continuidad de negocio con estándares, "best practices" y criterios internacionales de reconocido prestigio.
- Transmitir a terceras partes, relacionadas con la Organización, una imagen de seriedad, compromiso y responsabilidad focalizada en el respeto a los aspectos relativos a la seguridad de la información y continuidad de negocio.
- Fomentar una cultura corporativa de seguridad de la información y continuidad de negocio a través de la concienciación y formación del personal, tanto interno como externo, mediante la realización de acciones formativas, campañas de divulgación, etc. en dichas materias.

6 Objetivos de seguridad de la información

La Organización persigue los siguientes objetivos:

- Lograr una gestión y mantenimiento efectivo del SGI, compuesto por un Sistema de Gestión de la Seguridad de la Información para gestionar la información de manera adecuada implantando los controles necesarios y evaluando y analizando los riesgos, y por un Sistema de Continuidad de negocio para garantizar la disponibilidad y correcto funcionamiento de los sistemas y servicios implantando las medidas oportunas.
- Implementar políticas, medidas y controles de seguridad de la información y continuidad de negocio.
- Garantizar la Confidencialidad, Integridad, Disponibilidad, Trazabilidad y Autenticidad de la información.
- Garantizar el cumplimiento normativo.
- Proteger la integridad física de los empleados y asegurar la continuidad de los procesos de negocio esenciales.
- Gestionar eficazmente la respuesta frente a incidentes de seguridad.
- Garantizar la rápida recuperación de servicios críticos ante desastres.
- Controlar los procesos de intercambio de información con terceras partes.

7 Marco Normativo

Uno de los principios de la Organización es el de cumplimiento normativo, existiendo una política específica dentro de la Organización para asegurar este punto. Su objetivo es garantizar la identificación y cumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales que pudieran afectar a la Organización.

Por ello, esta política se alinea con el marco normativo, que incluye:

- Reglamento General de Protección de Datos (RGPD), reglamento de la UE 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 en su versión vigente.
- Directiva (UE) del Consejo, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego en su versión vigente
- Reglamento (UE) del Parlamento Europeo y del Consejo, por el que se establece el Mecanismo de Recuperación y Resiliencia en su versión vigente.
- Directiva europea para la protección de las personas que informen sobre infracciones del Derecho de la Unión en su versión vigente.

- LOPD-GDD - Ley Orgánica de Protección de Datos Personales y Garantía de los derechos digitales. en su versión vigente.
- LSSI-CE - de Servicios de la Sociedad de la Información y del Comercio Electrónico en su versión vigente.
- LPI - en su versión vigente.
- LEY DE PREVENCIÓN DE RIESGOS LABORALES en su versión vigente.
- Ley de trabajo a distancia en su versión vigente
- Ley del Estatuto de los trabajadores en su versión vigente
- Ley de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego.
- Ley de creación y crecimiento de empresas en su versión vigente.
- Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción en su versión vigente.
- El Esquema Nacional de Seguridad en su versión vigente.
- Las normas ISO/IEC 27001 e ISO/IEC 22301 en su versión vigente.
- Real Decreto 1007/2023, de 5 de diciembre, por el que se aprueba el Reglamento que establece los requisitos que deben adoptar los sistemas y programas informáticos o electrónicos que soporten los procesos de facturación de empresarios y profesionales, y la estandarización de formatos de los registros de facturación y su normativa de desarrollo.
- Reglamento de IA - 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.
- Reglamento DORA - Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero.
- Directiva NIS2 - 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.

8 Organización de la seguridad

8.1 Comité de Seguridad de la Información

La Organización cuenta con un *Comité de Seguridad de la Información*, como organismo responsable para la coordinación, implantación, gestión, supervisión, revisión y mantenimiento (enfocado en la mejora continua) del *SGI*.

Este comité, por medio de la presente política, declara su firme compromiso y apoyo, al establecimiento de dichos sistemas de gestión y a garantizar el cumplimiento de sus requisitos.

8.1.1 Objetivos del Comité:

Los objetivos del Comité son:

- Disponer de un órgano único, centralizado y multidisciplinar para la gestión de la *Seguridad de la Información* y *Continuidad del Negocio* en las soluciones, servicios y productos establecidos en el alcance.
- Facilitar la comunicación y coordinación entre las distintas partes implicadas (la seguridad de la información y continuidad del negocio es transversal a toda la Organización).
- Poner a disposición de todo el ámbito de la Organización un único punto de referencia para tratar aspectos relacionados con la seguridad de la información y continuidad del negocio.
- Garantizar un enfoque de mejora continua en todos los ámbitos del SGSI y SGCN

8.1.2 Funciones

- Aprobar las diferentes asignaciones de roles específicos y los responsables del SGSI/ENS
- Atender a las modificaciones legislativas, así como a las instrucciones, recomendaciones, resoluciones, etc. emitidas por los organismos reguladores (ej. la Agencia Española de Protección de Datos - AEPD)
- Garantizar los flujos de comunicación entre todas las partes internas implicadas ante las obligaciones de la Organización o el ejercicio de los derechos por parte de los usuarios que establece la LOPD-GDD, o en su defecto actuar proactivamente para su resolución.
- Garantizar el establecimiento de un Comité de Crisis y Continuidad de Negocio, y sus responsabilidades de coordinación y de apoyo necesarias para la gestión eficaz de escenarios de crisis.
- Aprobar las diferentes asignaciones de roles específicos y los responsables del SGCN y Comité de Crisis y Continuidad del Negocio.
- Realizar, mantener, revisar y aprobar periódicamente el análisis de Impacto en el Negocio (Business Impact Analysis) y, sobre esa base, establecer tiempos de recuperación en el PCN e identificar y abordar acciones que los minimicen.
- Establecer, desarrollar y aprobar las estrategias de Continuidad del Negocio y planes de respuesta.
- Identificar y establecer las medidas, procedimientos y controles en todos los ámbitos: organizativos, operativos, legales y/o técnicos, necesarios y adecuados para disponer de planes de respuesta eficaces a incidentes disruptivos.
- Establecer, planificar, desarrollar y aprobar planes de pruebas y ejercicios de simulacros de Continuidad del Negocio
- Garantizar las evaluaciones del PCN mediante pruebas y ejercicios de simulacros periódicos bajo un enfoque de mejor continua.
- Garantizar que los responsables de los planes de acción del PCN, sus colaboradores inmediatos y los afectados conocen dichos planes y realizan los oportunos simulacros.

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

8.1.3 Composición

La composición permanente del Comité de Seguridad de la Información es:

- Comité de Dirección WK Tax & Accounting
- Representante del Comité de Ética, Cumplimiento Normativo y Auditoría (CECNA)
- Equipo de Managers de la Unidad SDO /CAM
    - Área de Desarrollo Online/Onpremise
    - Área Cloud Application Management

- Products Managers o Product Owners
- Secretario General / Responsable de Asesoría Jurídica de la Organización.
- CISO, que actúa en calidad de Coordinador del Comité

El Comité de Seguridad de la Información podrá convocar a otras personas en función de las necesidades. Dependiendo de los temas a tratar en sus reuniones, la composición de los miembros del Comité Seguridad de la Información podrá variar; ampliando la composición con personal clave de otras direcciones o reduciéndose en el caso de no existir afectación en los departamentos que son representados por los miembros no convocados.
Los miembros del Comité Seguridad de la Información, en caso de no poder asistir a una convocatoria, podrá delegar su representación en otro miembro de su equipo, que tendrá poder de decisión.
Del mismo modo, la asistencia a las reuniones ordinarias del Comité está abierta a cualquier dirección, área o departamento de WK que requiera tratar algún tema específico de su ámbito funcional (contactar previamente con el Comité Seguridad de la Información).

8.1.4 Reuniones y convocatorias

El Comité se reunirá de forma ordinaria con una periodicidad mínima anual. Si por cualquier motivo se requiriese tratar algún tema de carácter excepcional, el Comité podrá ser convocado por cualquiera de sus miembros.
Se levantará acta documentada de todas las reuniones del Comité. Éstas serán conservadas y protegido su acceso debidamente en un repositorio de la empresa, cuyo contenido estará a disposición del *Comité Seguridad de la Información, del* Comité de Ética, Cumplimiento Normativo y Auditoría (CECNA)*y de* la *Alta dirección*.

8.1.5 Aprobación formal

Las aprobaciones y decisiones del *Comité Seguridad de la Información* podrán ser formalizadas alternativamente de dos formas:

A) A través *la Alta Dirección* (*Managing Director WK TAA*) mediante la validación a través de su firma en representación del *Comité SGSI* y la *Organización*.
B) Mediante la firma del responsable del Comité de Ética, Cumplimiento Normativo y Auditoría (CECNA), previa autorización del Consejo de Administración.
C) Mediante la firma del acta de reunión del *Comité Seguridad de la Información*, por todos los miembros permanentes.

8.1.6 Delegación de funciones

El *Comité Seguridad de la Información* podrá delegar las funciones que consideré pertinentes en el *Responsable de Seguridad – CISO* exceptuando la aprobación formal cuando sea requerida, que es potestad del *Comité Seguridad de la Información*, la *Alta Dirección* (*Managing Director WK TAA*), o del Comité de Ética, Cumplimiento Normativo y Auditoría (CECNA).

8.2 Roles y responsabilidades

La dirección asignará, renovará y comunicará las responsabilidades y roles en seguridad de la información, asegurando que todos los empleados conozcan y asuman sus responsabilidades. Los roles y responsabilidades de seguridad del personal en materia de seguridad de la información son los que se determinan a continuación:

8.2.1 Responsable de la Información

- El responsable de cada información y/o del servicio afectado por el análisis y gestión de riesgos se indicará en el Mapa de Riesgos del SGSI/ENS de la Organización que recogerá los criterios que determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales prescritos en el Anexo I del Real Decreto del ENS.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Establecer los requisitos de la información en materia de seguridad.
- Es el propietario de los riesgos sobre la información. El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.

8.2.2 Responsable del Servicio

- Cuya figura recae en los directores de las áreas de la entidad, que se encargará de gestionar los requisitos de seguridad de las actividades de su área para la prestación de los servicios.
- Establecer los requisitos del servicio en materia de seguridad del servicio.
- Determinar los niveles de seguridad de los servicios
- Es el propietario de los riesgos sobre los servicios. El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario

8.2.3 Responsable de Seguridad y Seguridad de la Información

- Será el encargado de notificar la presente política al personal de la entidad y de los cambios que en ella se produzcan, así como de coordinar las acciones de implantación, mantenimiento y mejora del SIG/ENS de la entidad (incluyendo la firma de la Declaración de Aplicabilidad que formaliza la relación de medidas de seguridad aplicables derivadas del Análisis de Riesgos), y de sus auditorías.
- Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la Organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Elaborar y proponer para aprobación por la Organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la Organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la Organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del
- cumplimiento de las obligaciones que se derivan del RD-l 12/2018 y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las
- deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

8.2.4 Responsable del Sistema

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la tipología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad

- El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad

8.2.5 Responsable de Seguridad Física

- Adoptará las medidas de seguridad que le competan, 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
- Clasificar las medidas de protección de las instalaciones físicas (obstáculos físicos, técnicas de vigilancia, sistemas de inteligencia, vigilantes y personal de seguridad.
- Desarrollar un marco conjunto capaz de dar respuesta a exigencias físicas y lógicas.

8.2.6 Administrador de Seguridad

- Se encargará de gestionar los requisitos técnicos de seguridad de los sistemas de información
- 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.
- La aplicación de los Procedimientos Operativos de Seguridad (POS).
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

8.2.7 Responsable de Continuidad de Negocio

El Responsable de Continuidad del Negocio es responsable de:

- identificar y evaluar los riesgos, desarrollar planes de contingencia y recuperación.
- Implementar medidas de seguridad adecuadas, coordinar y reportar a la dirección, y evaluar regularmente los planes de contingencia y recuperación para mejorar la eficacia de las medidas de seguridad implementadas.
- Garantizar la continuidad de los servicios y sistemas críticos en caso de una interrupción o desastre.
- Garantizar que el Sistema de continuidad de negocio es acorde a los requerimientos de las normas bajo alcance.

8.2.8 Responsable de Protección de Datos

- Será el encargado de garantizar que los datos personales se tratan y se protegen conforme al Reglamento General de Protección de Datos (RGPD UE 2016/679), por lo que trabajará en coordinación con el responsable de Seguridad de la Información y con el responsable de Sistemas.

8.3 Designación, Renovación de roles y resolución de conflictos

Los roles previamente mencionados son fundamentales para garantizar la correcta implementación del Sistema Integrado y el cumplimiento de las políticas y procedimientos establecidos.

A continuación, se detallan los principios y procesos para la designación y renovación de roles:

- Designación de Roles:
  - Los roles se asignarán a individuos en base a sus habilidades, conocimientos y experiencia pertinentes.
  - La designación de roles será realizada por la dirección mediante actas.
  - La designación de roles se llevará a cabo de manera clara y documentada, estableciendo las responsabilidades y autoridades correspondientes.

- Renovación de Roles:
  - La renovación de roles se realizará según las necesidades de la Organización y serán aprobados por la dirección mediante actas.
  - La renovación de roles puede implicar la reasignación de responsabilidades, la designación de nuevos roles o la actualización de las tareas y funciones existentes.

- Resolución de conflictos:
  - La resolución de conflictos se llevará a cabo en el Comité de Seguridad de la Información y de Continuidad de Negocio, el cual será el encargado de tratarlos y gestionarlos llegando a acuerdos para la resolución de los mismos.

Al seguir estos principios y procesos de designación y renovación de roles, la Organización garantiza un enfoque sistemático y efectivo en la gestión de roles y sus responsabilidades. Esto contribuye a mantener un enfoque sólido y efectivo en la gestión del Sistema Integrado en nuestra Organización.

8.4 Canales de comunicación

El *Comité Seguridad de la Información* puede ser contactado, a través de la dirección de correo electrónico del área de seguridad:

Es-dl-Itsecurity_TAA@wolterskluwer.com

se podrán plantear todas aquellas consultas, dudas, observaciones, etc. en materia de seguridad de la información.

9 Concienciación y Formación

La Organización tiene como objetivo lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la Organización y a todas las actividades, de acuerdo al principio de Seguridad Integral recogido

en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

10 Gestión de riesgos

Todos los sistemas deben realizar análisis de riesgos regularmente, al menos una vez al año, o cuando haya cambios significativos en la información manejada, los servicios prestados, o incidentes graves de seguridad.

Se presta especial atención a los riesgos derivados del tratamiento de datos personales, y se garantizará la implantación de las salvaguardias adecuadas para proteger la privacidad y confidencialidad de la información personal.

11 Responsabilidad del personal y medidas disciplinarias

- **Derechos del Personal:** El personal tiene derecho a recibir formación y orientación en seguridad de la información, a reportar incidentes y vulnerabilidades sin temor a represalias, y a acceder a la información necesaria para proteger los activos de información de manera segura.
- **Deberes del Personal:** Todo el personal es responsable de cumplir con las políticas y procedimientos del SIG y con controles de seguridad, protegiendo la información confidencial y reportando cualquier incidente de seguridad de manera inmediata. Aparte, todos los empleados deben recibir formación en seguridad de la información y continuidad de negocio al menos una vez al año. Se implementará un programa de concienciación continua para asegurar el cumplimiento de esta política.
- **Medidas Disciplinarias:** El incumplimiento de las normativas, políticas y procedimientos del sistema, puede resultar en medidas disciplinarias que se aplicarán de manera justa y proporcional, incluyendo advertencias, suspensiones, sanciones económicas o, en casos graves, la terminación del contrato laboral.

12 Estructura, Gestión y acceso a la documentación

En la Organización se establecen directrices para la estructuración, gestión y acceso de la documentación de seguridad del sistema. Estas directrices aseguran que la documentación se organice adecuadamente, permitiendo su fácil consulta y comprensión por parte de los responsables de seguridad y personal autorizado.

13 Aprobación y Revisión

La presente Política cuenta con el total compromiso de la Organización y su Alta Dirección, siendo revisada periódicamente para su continua adecuación con el Marco Normativo vigente y el cumplimiento de las leyes y regulaciones aplicables, así como para mantener su efectividad, efectuando modificaciones si existieran cambios que así lo justifiquen, en los procesos de negocio, personas, infraestructura física o tecnológica, información, suministros o partes interesadas de la Organización.

La aprobación de la presente Política se desarrollará acorde con lo establecido por la compañía, ajustando así tanto la responsabilidad sobre la modificación de los contenidos como la frecuencia, en que éstos deberán ser revisados.

14 Comunicación

La presente política será publicada en la web corporativa, comunicada a las partes interesadas que deban estar en conocimiento y puesta a su disposición para ser consultada.

En Barcelona, a 24 de Marzo de 2026

Tomàs Font Zapater
Vice President & General manager
TAA Europe Region South•TAA | Spain

Carles Cabré Boixados
IT Security Manager
DXG | TAA Spain

Wolters Kluwer

Wolters Kluwer Tax & Accounting

Wolters Kluwer Tax & Accounting España, S.L.U.
Paseo de la Castellana 93 Edificio Cadagua
28046 - Madrid

wolterskluwer.com