
URÍA MENÉNDEZ

Política de Seguridad de la Información de
Uría Menéndez

Política de Seguridad de la Información de Uría Menéndez

Uría Menéndez Abogados, S.L.P. (incluyendo sus sucursales y filiales, en adelante “**UM**”) considera que la información, en especial la relativa a sus clientes, y los distintos sistemas de información utilizados para su tratamiento son activos críticos que deben ser protegidos adecuadamente, cualquiera que sea su forma y medios de almacenamiento, para asegurar el correcto funcionamiento de UM, salvaguardando la operativa de su negocio y el correcto servicio a sus clientes.

La política de seguridad (en adelante, la “**Política**”) persigue garantizar una correcta gestión de los elementos y sistemas de información en base a tres pilares básicos, que resultan claves:

- Su confidencialidad, garantizando su accesibilidad de forma única y controlada a las personas, procesos o sistemas autorizados, previniendo que se lleve a cabo una divulgación no autorizada de la misma.
- Su integridad, impidiendo que sea manipulada por terceros no autorizados de forma malintencionada;
- Su disponibilidad, mediante autorización y su recuperación en caso de incidentes de seguridad que provoquen su pérdida o corrupción.

Para la consecución de los objetivos establecidos en materia de Seguridad de la Información, la Política establece una serie de procedimientos y actuaciones, dando cumplimiento a las diferentes normas y requisitos aplicables vigentes en cada momento y manteniendo un equilibrio entre los niveles de riesgo y el uso eficiente de los recursos mediante criterios de proporcionalidad.

La política es de aplicación a todos los miembros de UM, en España y Portugal, siendo igualmente de aplicación obligatoria a sus sucursales y, eventualmente, a sus filiales. Esta Política se hará extensible a terceras partes involucradas directa o indirectamente con la correcta operatividad de los servicios involucrados en UM, estableciendo criterios de seguridad y confidencialidad que deberán ser cumplidos contractualmente y supervisados periódicamente. Los principios fundamentales para desarrollar el compromiso expreso de UM en la **mejora continua** del sistema de gestión de la seguridad de la información son los siguientes:

- Garantizar que los Sistemas de Información de UM posean el adecuado nivel de seguridad y resiliencia que proponga el Comité de Seguridad de la Información de UM.

- Establecer una política de mínimos privilegios, asignando a los usuarios los niveles o permisos de acceso mínimos necesarios, de forma que se limite el contenido y el número de personas con acceso a la información.
- Mantener una política de control de acceso cerrado por defecto, disponiendo que la información y los sistemas que la tratan o almacenan se encuentren inicialmente cerrados, y permitiendo su acceso con posterioridad, solo cuando resulte necesario, en función de su nivel de clasificación. Asimismo, asegurar el control de su ciclo de vida, desde su creación hasta su eventual eliminación segura.
- Establecer medidas específicas para el acceso seguro desde dispositivos corporativos o en situaciones de trabajo remoto, incluyendo el uso de redes VPN, autenticación multifactor, cifrado de dispositivos y control de configuración mínima, para garantizar la protección de los elementos y sistemas de información frente a accesos no autorizados.
- Precisar un conjunto de funciones y responsabilidades en materia de seguridad de la información, claramente definidas.
- Segregar las funciones y responsabilidades en materia de seguridad de la información, de forma que resulten claramente definidas y asignadas en el organigrama de UM, evitando posibles conflictos de intereses y reduciendo al mínimo imprescindible el número de personas con acceso a la información.
- Dotar a UM de procedimientos y herramientas de análisis, prevención, detección, respuesta y recuperación, que permitan adaptarse con agilidad a los cambios del entorno tecnológico y a las nuevas amenazas, incluyendo un proceso sistemático, documentado y continuo de análisis y gestión de riesgos. Este proceso permitirá identificar, evaluar, tratar y monitorizar los riesgos que puedan afectar a la confidencialidad, integridad y disponibilidad de los elementos y sistemas de información de UM.
- Diseñar e implementar varios niveles de seguridad que sean acordes al análisis de riesgos realizado sobre los distintos elementos y sistemas de información que almacenan, procesan o gestionan la información, para así favorecer una defensa en profundidad, asegurar la continuidad operativa en caso de incidentes críticos o desastres y garantizar que las medidas de seguridad implantadas sean proporcionales al nivel de riesgo identificado.
- Sensibilizar a todos los miembros de UM acerca de los riesgos de seguridad y garantizar que disponen de formación en seguridad de la información, así como de las capacidades tecnológicas necesarias para proteger la seguridad de los sistemas de información de UM.
- Colaborar con los organismos y agencias gubernamentales relevantes para la mejora de la seguridad de UM y el cumplimiento de la legislación vigente.

- Establecer vías de comunicación rápidas y accesibles de posibles incidentes de seguridad.
- Respalda un proceso de revisión y actualización continua del modelo de gestión de la seguridad para adecuarlo en todo momento a las amenazas emergentes que puedan afectar a UM y garantizar su efectividad continuada.

Esta política fue aprobada por el Comité de Seguridad de la Información de UM a 24 de febrero de 2026.

Para la consecución de los principios establecidos en esta política, UM gestiona la seguridad de la información conforme a los estándares internacionales y a las mejores prácticas en la materia, habiendo obtenido el certificado ISO/IEC 27001:2022.

