

# **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

**SGSI.PR.A5.01**

**MVA** | ASOCIADOS

Índice

1.	APROBACIÓN Y ENTRADA EN VIGOR .....	3
2.	INTRODUCCIÓN.....	3
3.	ALCANCE .....	4
4.	PRINCIPIOS .....	5
4.1.	Confidencialidad .....	5
4.2.	Integridad.....	5
4.3.	Disponibilidad.....	5
4.4.	Proporcionalidad .....	6
5.	OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN .....	6
6.	REQUISITOS DE SEGURIDAD.....	6
6.1.	Organización y responsabilidades.....	7
6.2.	Gestión de accesos.....	7
6.3.	Protección de dispositivos y sistemas.....	7
6.4.	Clasificación y tratamiento de la información. ....	7
6.5.	Continuidad del negocio .....	7
6.6.	Gestión de incidentes .....	7
6.7.	Gestión de terceros y colaboradores .....	8
6.8.	Registro de actividad.....	8
6.9.	Gestión de riesgos.....	8
7.	MARCO NORMATIVO DE REFERENCIA .....	9
8.	PROTECCIÓN DE DATOS PERSONALES.....	9
9.	MEJORA CONTINUA Y REVISIÓN DE LA POLÍTICA .....	10
10.	CONSECUENCIAS EN CASO DE INCUMPLIMIENTO.....	10

Rev.	Fecha	Revisado:	Aprobado:	Causa Modificación
1	18/02/2026	BASE10	MVA ASOCIADOS	Aprobación inicial

## 1. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la Información y el conjunto de documentos que conforman el Sistema de Gestión de Seguridad de la Información (SGSI), tales como políticas, procedimientos y registros mostrados a continuación, han sido aprobados por el Consejo de Administración de MVA ASOCIADOS y son de aplicación desde la fecha de aprobación hasta que sean modificados o sustituidos por nuevas versiones formalmente aprobadas.

REFERENCIA	DESCRIPCIÓN
SGSI.PR.A5.01	Política de Seguridad de la Información
SGSI.PR.A5.02	Roles y Responsabilidades en la seguridad de la información
SGSI.PR.A5.06	Normativa Relativa a Obligaciones Internas de Seguridad
SGSI.PR.A5.10	Procedimiento de Cumplimiento Normativo
SGSI.PR.A5.03	Procedimiento de identificación y acceso
SGSI.PR.A5.04	Política Gestión de Terceros
SGSI.PR.A5.05	Procedimiento de Contratación y Seguimiento de Terceros
SGSI.PR.A5.08	Procedimiento Gestión de Incidentes
SGSI.PR.A5.13	Política de uso de la Inteligencia Artificial (IA)
SGSI.PR.A6.01	Procedimiento de Gestión de Personal-Formación
SGSI.PR.A8.02	Política Controles Criptográficos
SGSI.PR.A8.03	Procedimiento de Seguridad Comunicaciones
SGSI.PR.A8.04	Procedimiento de Adquisición, Implantación y Mantenimiento
SGSI.PR.A8.06	Política dispositivos móviles
SGSI.PR.A8.07	Procedimiento de Seguridad de las Operaciones
SGSI.PR.A8.08	Procedimiento gestión de contraseñas
SGSI.PR.A5.12	Procedimiento Evaluación interna del SGSI
SGSI.PR.10.01	Procedimiento de No Conformidades y Acciones Correctivas (NCs y AACCs)
SGSI.PR.A5.07	Clasificación de la Información
SGSI.R.A5.03	Requisitos legales
SGSI.R.A6.01	Perfil Puesto
SGSI.DO-07.01	Tabla de Comunicaciones
SGSI.R.10.01	No Conformidades, y Acciones Correctivas

*Tabla 1:* Documentos Sistema de Gestión de Seguridad de la Información

## 2. INTRODUCCIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) de MVA ASOCIADOS es el marco que organiza y gobierna la seguridad de la información del despacho. Se conforma de políticas, procedimientos, controles y registros necesarios para proteger la **confidencialidad, integridad y disponibilidad** de la información, y se mantiene actualizado mediante revisiones periódicas y mejora continua.

MVA ASOCIADOS reconoce que la información es uno de sus activos más valiosos, especialmente por la naturaleza sensible y confidencial de los datos que gestiona en el marco de su actividad profesional como despacho de abogados.

El uso de tecnologías de la información y la comunicación para el desarrollo de los servicios jurídicos requiere desarrollar medidas adecuadas que garanticen la protección de la información frente a accesos no autorizados, pérdida, alteración o divulgación no autorizada. Este documento demuestra el compromiso de MVA ASOCIADOS y sus órganos de Dirección y Administración con la protección de los activos de información y con el cumplimiento de las normas de referencia en el ámbito de la seguridad de la información. Asimismo, constituye la base sobre la que se desarrollarán políticas específicas, procedimientos operativos y controles técnicos y organizativos destinados a salvaguardar la confidencialidad, integridad y disponibilidad de la información.

### 3. ALCANCE

---

La presente Política de Seguridad de la Información es de aplicación general en MVA ASOCIADOS y se extiende a todas las personas, procesos, sistemas y activos implicados en la gestión de la información dentro del despacho. Es de obligado cumplimiento para todo el personal de MVA ASOCIADOS, incluyendo:

- Socios, empleados, personal administrativo.
- Colaboradores externos y profesionales asociados que participen en actividades del despacho, en la medida en que resulte de aplicación en el marco de sus colaboraciones.
- Proveedores de servicios que, por su relación contractual, accedan o procesen información del despacho, en particular el proveedor de servicios tecnológicos (TI).

Todos ellos deberán conocer, respetar y aplicar las directrices establecidas en esta política, así como en las normas, procedimientos e instrucciones que de ella deriven.

Desde un punto de vista técnico y organizativo, esta política se aplica a:

- Todos los activos de información gestionados por el despacho, independientemente de su formato (físico, digital, audiovisual).
- Los sistemas informáticos y plataformas tecnológicas que procesan, almacenan o transfieren información (NAS, Microsoft Office 365, SharePoint, Teams, etc.)
- Los procesos operativos propios del despacho para ejercer la actividad (prestación de servicios jurídicos, gestión de clientes, administración interna, cumplimiento legal, entre otros).

- Los canales de comunicación utilizados por el despacho, tanto internos como externos.

## 4. PRINCIPIOS

---

La seguridad de la información en MVA ASOCIADOS se basa en un conjunto de principios fundamentales que guían la adopción de decisiones, medidas de seguridad y la actuación del personal en el tratamiento de la información. Estos principios aseguran que los datos tratados por el despacho sean protegidos adecuadamente frente a riesgos internos y externos, cumpliendo con los requisitos legales para el ejercicio de la actividad.

### 4.1. Confidencialidad

Se refiere a la protección de la información para que únicamente sea accesible por personas debidamente autorizadas. El despacho implementará medidas para proteger los datos corporativos o de cualquier otra índole, con la finalidad de limitar el acceso exclusivamente al personal que lo requiera para el desempeño de sus funciones.

### 4.2. Integridad

La integridad de la información implica mantener su exactitud, consistencia y completitud durante todo su ciclo de vida, desde su creación hasta su eliminación. Este principio garantiza que los datos almacenados en los dispositivos, transmitidos por cualquier canal de comunicación o procesados en los sistemas del despacho no hayan sido alterados de forma no autorizada, ya sea por error, manipulación malintencionada o fallo técnico.

### 4.3. Disponibilidad

El principio de disponibilidad hace mención de que la información y los recursos estén accesibles para los usuarios autorizados en el momento en que los necesiten. Este principio asegura el funcionamiento continuo y de forma eficiente de las actividades del despacho, asegurando que los datos estén disponibles sin interrupciones que puedan afectar el desarrollo del negocio.

Se implementarán medidas que no solo impliquen mantener el acceso continuado en condiciones normales de operación, sino también que aseguren la recuperación de la información en caso de incidentes, como pueden ser, fallos técnicos y/o ciberataques.

#### 4.4. Proporcionalidad

Las medidas de protección serán proporcionales al nivel de riesgo, la sensibilidad de la información y la criticidad de los servicios implicados. Se mantendrá un equilibrio entre seguridad, funcionalidad y costes, de forma razonable y sostenible, que permita el correcto desarrollo de las actividades del despacho.

### 5. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

---

Los objetivos de seguridad de la información en MVA ASOCIADOS se establecen para asegurar que la gestión de los activos se realice de forma segura, confiable y conforme con las obligaciones legales, éticas y contractuales que asume el despacho en el ejercicio de su actividad profesional. Los objetivos se definen a continuación:

- Proteger la confidencialidad, integridad y disponibilidad de la información que se gestiona en el despacho, en todas sus formas y medios.
- Garantizar la continuidad de las actividades del despacho mediante la implementación de medidas preventivas, de respaldo y recuperación ante incidentes.
- Fomentar una cultura orientada a la seguridad, a través de la formación y concienciación del personal interno, colaboradores y proveedores sobre sus responsabilidades en relación con la protección de la información.
- Cumplir con la legislación vigente en materia de protección de datos, en particular el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica 3/2018 (LOPDGDD) y otras normativas aplicables.
- Aplicar un enfoque basado en riesgos, que permita identificar, evaluar y tratar los riesgos que puedan comprometer la seguridad de los activos de información del despacho.
- Establecer procedimientos documentados y controlados, que regulen el uso seguro de los sistemas, el acceso a la información y la actuación ante incidentes de seguridad.

Estos objetivos serán revisados periódicamente por el Consejo de Administración y se utilizarán como base para evaluar la eficacia de las medidas implantadas en el despacho.

### 6. REQUISITOS DE SEGURIDAD

---

MVA ASOCIADOS establecerá un conjunto de requisitos mínimos de seguridad que servirán de base para salvaguardar la protección de la información y garantizar la continuidad de sus actividades. Estos requisitos permiten establecer un entorno controlado y resiliente ante los riesgos derivados del uso de las TICs, y se aplican de forma transversal a todo el despacho.

### 6.1. Organización y responsabilidades

El despacho contará con un Responsable de Seguridad, responsable de promover, supervisar y coordinar las medidas de protección, así como de asegurar el cumplimiento de esta política y de las normas que la desarrollen.

### 6.2. Gestión de accesos

Se controlará el acceso físico y lógico a los activos de información, permitiéndose únicamente al personal autorizado en función de su perfil y necesidades para el ejercicio de sus funciones. Se aplicarán mecanismos de autenticación (MFA), políticas de contraseñas y registro de accesos.

### 6.3. Protección de dispositivos y sistemas

Las plataformas tecnológicas, tanto en la nube como locales, deberán mantenerse actualizados, protegidos contra malware y configurados siguiendo principios de seguridad por defecto. Se restringirá el uso de dispositivos no autorizados y se supervisará la instalación y uso de herramientas tecnológicas.

### 6.4. Clasificación y tratamiento de la información.

Toda la información será clasificada según su nivel de sensibilidad (pública, compartida, confidencial), y se le aplicarán controles de seguridad adecuados en función de dicha clasificación, tanto en tránsito como en reposo.

### 6.5. Continuidad del negocio

Se establecerán medidas que permitan, en caso de interrupciones, mantener las operaciones críticas y recuperar la información de forma segura, especialmente ante ciberincidentes o fallos de servicio. Entre las medidas que se adoptarán está la realización de copias de seguridad periódicas de, al menos, la información crítica, serán almacenadas de forma segura y probadas regularmente para garantizar su integridad y disponibilidad en caso de que sea necesario realizar una restauración.

### 6.6. Gestión de incidentes

El despacho dispondrá de procedimientos documentados para la detección, notificación, clasificación, análisis, resolución y lecciones aprendidas para hacer frente a los incidentes de seguridad de la información.

### 6.7. Gestión de terceros y colaboradores

Los proveedores y colaboradores que requieran acceder o tratar información clasificada como no pública, estarán sujetos a cláusulas contractuales de confidencialidad y seguridad, y deberán cumplir con los requisitos mínimos definidos en esta política.

En aquellos casos en los que los servicios contratados supongan acceso o tratamiento por el proveedor de datos de carácter personal se deberá incluir en el contrato el clausulado requerido para el cumplimiento 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 estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

MVA ASOCIADOS se reserva el derecho de restringir o revocar el acceso a sus sistemas a cualquier tercero que no cumpla con las condiciones establecidas, y de exigir las responsabilidades que correspondan en caso de daño, pérdida o uso indebido de la información.

### 6.8. Registro de actividad

MVA ASOCIADOS mantendrá un registro de las acciones realizadas por los usuarios en sus sistemas de información, con el objetivo de supervisar el uso adecuado de los recursos, investigar posibles accesos indebidos o comportamientos no autorizados, y conservar evidencia en caso de presentarse situaciones anómalas.

Dichos registros permitirán la identificación del usuario responsable de cada acción, respetando en todo momento los derechos fundamentales a la intimidad, al honor y a la propia imagen, y cumpliendo estrictamente con lo establecido en la normativa vigente en materia de protección de datos personales.

### 6.9. Gestión de riesgos

La gestión de riesgos es un proceso relevante del sistema de seguridad de la información de MVA ASOCIADOS, este permite identificar, valorar y tratar las amenazas que puedan afectar a la confidencialidad, integridad y disponibilidad de la información.

El despacho aplicará un enfoque sistemático y proactivo en la gestión de riesgos que, será revisada regularmente, al menos una vez al año, y de forma extraordinaria en los siguientes casos:

- Cambios significativos en los sistemas de información, los servicios prestados o la naturaleza de la información tratada.
- Incorporación o sustitución de proveedores que afecten a la gestión o tratamiento de información.
- Detección de vulnerabilidades críticas o la ocurrencia de incidentes de seguridad con impacto relevante para el despacho.

## 7. MARCO NORMATIVO DE REFERENCIA

---

La presente Política de Seguridad de la Información se alinea con las buenas prácticas y los estándares internacionalmente reconocidos en materia de gestión de la seguridad de la información, en especial los establecidos por la norma ISO/IEC 27001.

Asimismo, responde al cumplimiento de la legislación vigente que resulta aplicable al despacho en el ejercicio de su actividad profesional, incluyendo, entre otras:

- El Reglamento (UE) 2016/679, General de Protección de Datos (RGPD).
- La Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- La Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico (LSSI), en lo que corresponda.
- El Código Deontológico del Consejo General de la Abogacía Española, por su implicación en la confidencialidad profesional.

MVA ASOCIADOS se compromete a identificar y cumplir toda otra norma, regulación o cláusula contractual aplicable en materia de protección de la información, incluyendo las exigencias particulares de confidencialidad impuestas por los clientes o por órganos jurisdiccionales en el marco de sus funciones legales.

## 8. PROTECCIÓN DE DATOS PERSONALES

---

MVA ASOCIADOS, en su calidad de responsable del tratamiento, garantiza el cumplimiento estricto de la normativa vigente en materia de protección de datos personales, en particular el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD).

El despacho trata datos personales en el marco de sus actividades jurídicas, administrativas y contractuales, lo cual exige aplicar medidas técnicas, jurídicas y organizativas adecuadas que aseguren la confidencialidad, integridad y disponibilidad de los sistemas que los procesan.

Además, todos los socios, empleados y colaboradores del despacho están obligados a mantener la confidencialidad de los datos personales a los que tengan acceso, incluso después de finalizada su relación profesional con el despacho.

MVA ASOCIADOS cuenta con un procedimiento interno para el ejercicio de derechos por parte de los interesados (acceso, rectificación, supresión, oposición, limitación y portabilidad).

## 9. MEJORA CONTINUA Y REVISIÓN DE LA POLÍTICA

---

MVA ASOCIADOS se compromete a mantener esta Política de Seguridad de la Información actualizada y alineada con la evolución de su entorno tecnológico, normativo y organizativo.

Para ello, adoptará un enfoque de mejora continua, basado en la revisión periódica de su sistema de gestión de seguridad de la información (SGSI) y de los controles implantados.

La política será revisada al menos una vez al año o cuando se produzcan cambios significativos en:

- La estructura organizativa o funcional del despacho.
- Las tecnologías utilizadas para el tratamiento de la información.
- Las exigencias legales o contractuales en materia de seguridad.
- La ocurrencia de incidentes o hallazgos de auditoría que así lo justifiquen.

La revisión será coordinada por el Responsable de Seguridad y presentada al Consejo de Administración para su aprobación.

## 10. CONSECUENCIAS EN CASO DE INCUMPLIMIENTO

---

El incumplimiento de esta Política de Seguridad de la Información por parte del personal, colaboradores o terceros podrá dar lugar a la adopción de medidas correctivas y, en su caso, sancionadoras, en función de la gravedad de los hechos y de la relación jurídica existente con MVA ASOCIADOS.

En particular:

- Para el personal del despacho, el incumplimiento podrá conllevar sanciones disciplinarias conforme al régimen laboral aplicable, sin perjuicio de la posible exigencia de responsabilidades civiles, penales o administrativas, si procede.
- Para los colaboradores y terceros, el despacho podrá ejercer las acciones contractuales correspondientes, incluyendo la resolución anticipada del contrato, la imposición de penalizaciones o la reclamación de daños y perjuicios.

- Si el incumplimiento da lugar a infracciones legales, especialmente en materia de protección de datos personales, se podrán derivar responsabilidades frente a las autoridades competentes y los titulares de los datos afectados.

MVA ASOCIADOS analizará cada caso de forma individual, respetando los principios de objetividad, proporcionalidad y debido proceso, documentando las actuaciones realizadas y aplicando las medidas necesarias para prevenir reincidencias o impactos mayores. Esta política y sus medidas asociadas son obligatorias desde la fecha de su aprobación y podrán ser actualizadas para su adaptación a nuevas exigencias normativas, tecnológicas o estratégicas.