1. Aprobación y entrada en vigor

Texto aprobado el día 17 de octubre de 2025 por la Dirección de INTERFILM SERVICING, S.L.

Esta Política de Seguridad de la Información entra en vigor en la fecha de su aprobación y permanecerá vigente hasta su sustitución por una nueva Política.

2. Introducción

INTERFILM SERVICING, S.L. depende de sus sistemas de información para alcanzar sus objetivos. Estos sistemas se administran con diligencia, aplicando medidas proporcionales al riesgo para proteger la autenticidad, trazabilidad, integridad, confidencialidad y disponibilidad de la información y la continuidad de los servicios.

La seguridad se integra en todo el ciclo de vida, con enfoque preventivo, vigilancia continua y respuesta ágil a incidentes, incluyendo su planificación y contratación.

3. Alcance

Esta Política aplica al sistema de información de Interfilm Servicing, S.L., que soporta los servicios de gestión integral de recintos, venta de entradas y relación con clientes mediante la plataforma PatronBase en modalidad Cloud/SaaS.

Todos los servicios de la organización se apoyan en una infraestructura externalizada, conforme a las exigencias de seguridad, disponibilidad y confidencialidad establecidas en el Esquema Nacional de Seguridad (ENS).

Estos servicios se gestionan a través de un sistema de información único garantizando la seguridad de la información en todas las áreas de la empresa.

El alcance abarca la totalidad de los sistemas, procesos y servicios de la organización relacionados con la prestación de los servicios mencionados, conforme a la Declaración de Aplicabilidad vigente

4. Misión y objetivos

- Garantizar Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad de la información y la continuidad de los servicios.
- Implementar medidas de seguridad según el riesgo y seguridad por defecto.
- Asegurar trazabilidad, mínimo privilegio y deber de confidencialidad.
- Desplegar seguridad física adecuada a los riesgos.
- Proteger la seguridad de comunicaciones y datos en tránsito.
- Controlar adquisición, desarrollo y mantenimiento en todas las fases del ciclo de vida, garantizando seguridad desde el diseño.
- Controlar el cumplimiento de medidas en la prestación de servicios y en la incorporación de nuevos componentes.
- Gestionar incidentes (detección, contención, mitigación, resolución y no repetición).
- Proteger datos personales conforme a RGPD/LOPDGDD.
- Supervisar continuamente el sistema y mejorar de forma continua.

5. Principios rectores

- Alcance estratégico y compromiso de toda la organización.
- Seguridad integral (técnica, humana, organizativa y física).
- Gestión basada en riesgos y proporcionalidad.
- Prevención, detección, respuesta y conservación.
- Líneas de defensa (seguridad en capas).
- Vigilancia continua y reevaluación periódica.
- Seguridad por defecto y desde el diseño.

6. Marco normativo

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Reglamento (UE) 2016/679 (RGPD), de 27 de abril de 2016.
- Ley Orgánica 3/2018 (LOPDGDD), de 5 de diciembre.
- Decisiones de la Comisión Europea sobre transferencias internacionales de datos (decisiones de adecuación, SCC, etc.).
- Ley 34/2002 (LSSI-CE), de 11 de julio.
- Real Decreto-ley 13/2012, de 30 de marzo (cookies y comunicaciones).
- Reglamento (UE) 910/2014 (eIDAS), de 23 de julio de 2014.
- Reglamento (UE) 2022/2065 (DSA), de 19 de octubre de 2022.
- Real Decreto Legislativo 1/1996, de 12 de abril, Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto-ley 2/2018, de 13 de abril (modifica LPI).
- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- Real Decreto 39/1997, de 17 de enero, Reglamento de los Servicios de Prevención.
- Guías CCN-STIC Serie 800 (ENS)

7. Organización de la seguridad

Comité de Seguridad de la Información: funciones y responsabilidades

Dada la dimensión y estructura de Interfilm Servicing, S.L., la Dirección de la empresa asume los roles de Responsable de la Seguridad (RSEG), Responsable del Servicio (RSERV) y Responsable de la Información (RINFO), asegurando la diferenciación funcional con el Responsable del Sistema (RSIS), conforme al artículo 11 del Real Decreto 311/2022.

En el marco del Esquema Nacional de Seguridad (ENS), el Comité de Seguridad de la Información (CSI) está constituido por:

- Dirección / Responsable de Seguridad (RSEG), que asume igualmente las funciones de Responsable del Servicio (RSERV) y Responsable de la Información (RINFO).
- Responsable del Sistema (RSIS), encargada de la gestión técnica y operativa de las medidas de seguridad.
- Apoyo externo especializado en protección de datos y cumplimiento normativo, prestado por empresa externa, con carácter consultivo y de asesoramiento especializado.

Esta estructura permite mantener la independencia mínima exigida entre la Dirección (RSEG/RINFO/RSERV) y la Responsable del Sistema (RSIS), contando además con apoyo externo para la supervisión en materia de protección de datos personales y cumplimiento RGPD/LOPDGDD.

Entre las principales funciones del Comité se incluyen:

- Supervisar el análisis de riesgos y la evolución de los indicadores de seguridad.
- Revisar y documentar los incidentes de seguridad y su gestión.
- Controlar la Declaración de Aplicabilidad (DoA) y el grado de implantación de las medidas ENS.
- Aprobar los resultados de auditorías y supervisar las acciones correctoras (PAC).
- Revisar y validar los planes de continuidad y recuperación (PCN/DRP).
- Evaluar a los proveedores críticos y verificar su cumplimiento ENS.
- Revisar la Política de Seguridad y proponer mejoras cuando se detecten necesidades o cambios.
- Impulsar la mejora continua y la revisión anual del sistema ENS.

Roles: funciones y responsabilidades

- **Dirección / RSEG / RSERV / RINFO:** define, aprueba y supervisa las medidas de seguridad, el cumplimiento normativo y la protección de datos.
- **RSIS (Responsable del Sistema):** ejecuta y mantiene las medidas técnicas y operativas, informando a la Dirección de incidencias y necesidades de mejora.
- **Apoyo externo:** proporciona asesoramiento legal y técnico en materia de protección de datos y cumplimiento ENS.

Procedimientos de designación y suplencias

Los roles de seguridad definidos por el ENS (RSEG, RSIS, RSERV, RINFO) son designados formalmente por la Dirección y documentados en el Acta de Constitución del Comité de Seguridad de la Información.

Dadas las limitaciones de tamaño de la empresa, los roles de RSEG, RSERV y RINFO son ejercidos por la misma persona (Dirección), garantizando la independencia de criterio mediante la revisión cruzada con el RSIS y el apoyo del consultor externo.

Los nombramientos se revisarán anualmente, o antes si se producen cambios relevantes en la estructura, los servicios o los sistemas. Se documentarán suplencias temporales en caso de ausencias prolongadas para garantizar la continuidad operativa.

Resolución de conflictos

En caso de discrepancias entre los responsables designados (RSEG, RSIS, RINFO/RSERV), la Dirección de Interfilm Servicing, S.L. actuará como órgano decisor final. Cuando proceda, podrán establecerse particularidades específicas para servicios sujetos a requisitos adicionales o normativas sectoriales.

8. Tratamiento de datos personales

INTERFILM SERVICING, S.L. trata los datos personales conforme al Registro de Actividades de Tratamiento. Se evalúan los riesgos y, cuando procede, se elaboran planes de actuación para la corrección de dichos riesgos; para tareas de asesoramiento especializado y apoyo en la implantación de medidas, se cuenta con un consultor externo. La Dirección fija la valoración de referencia por tipos de información/servicio, promueve inversiones horizontales y coordina los planes de tratamiento del riesgo.

9. Gestión de riesgos

Todos los sistemas sujetos a esta Política realizarán análisis de riesgos:

- Anualmente;
- Cuando cambie la información o los servicios;
- Tras un incidente grave o una vulnerabilidad crítica;
- Ante modificaciones relevantes en RGPD/EIPD.

La Dirección de INTERFILM SERVICING, S.L. fijará una valoración de referencia por tipos de información y servicio y promoverá inversiones horizontales. Se tendrán en cuenta los riesgos en protección de datos. Las funciones de asesoramiento especializado en materia de seguridad y protección de datos son realizadas por un consultor externo que apoya al Responsable de Seguridad. Asimismo, se coordinarán los planes de tratamiento del riesgo

10.Desarrollo de la política y normativa asociada

Esta Política de Seguridad de la Información complementa/se integra junto con otras políticas de INTERFILM SERVICING, S.L. en diferentes materias: Política de Control de Accesos, Política de Copias de Seguridad, Política de Gestión de Contraseñas, Política de Teletrabajo, entre otras.

La normativa estará disponible para los usuarios que deban conocerla.

11. Obligaciones del personal y formación

Todo el personal debe conocer y cumplir esta Política y su normativa.

Se impartirá concienciación anual a todo el personal y formación previa a asumir responsabilidades de uso/operación/administración. La formación es obligatoria en onboarding y ante cambios de puesto o responsabilidades.

12. Terceras partes / prestadores de servicios / proveedores

En los servicios prestados a terceros o con información de terceros se compartirá esta Política y las normas aplicables, respetando en todo momento la normativa de protección de datos en los que INTERFILM SERVICING, S.L. actúe como encargado.

En la contratación de terceros se exigirá el cumplimiento del ENS o equivalentes, la inclusión de cláusulas de seguridad, puntos de contacto para notificación de incidentes, así como requisitos específicos para servicios en la nube y, cuando aplique, para IA.

Si un tercero no satisface alguno de estos aspectos, el Responsable de Seguridad elaborará un informe de riesgos. La Dirección decidirá si autoriza o no la contratación del tercero, asumiendo los riesgos detectados.

13. Gestión de incidentes de seguridad

INTERFILM SERVICING, S.L. dispondrá de un procedimiento para la gestión ágil de eventos e incidentes que amenacen la información y los servicios, coordinado con otras normas aplicables (por ejemplo, RGPD), con notificación a las autoridades competentes cuando proceda.

Este procedimiento se integrará con otros relacionados con incidentes de seguridad que pudieran derivarse de otras normativas aplicables (como la de protección de datos personales), con el fin de coordinar la respuesta desde los diferentes enfoques normativos y comunicar a los organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad del Estado o a los juzgados.

El Comité de Seguridad será el responsable de activar y coordinar este procedimiento.

14. Aprobación, revisión y sustitución de la Política

El Comité de Seguridad podrá introducir ajustes en esta Política cuando se detecten ineficiencias y la revisarán al menos una vez al año.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona con las debidas competencias.

La sustitución de la Política será propuesta por el Comité de Seguridad, ratificada por la persona con las debidas competencias y comunicada por los canales establecidos a todas las partes interesadas.