## 1. Aprobación y entrada en vigor

Texto aprobado el día **22 de septiembre de 2025** por la Dirección de Círculo de Comunicación, 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

CÍRCULO DE COMUNICACIÓN, 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 a todos los sistemas de información que dan soporte a las actividades/servicios de Círculo de Comunicación, S.L., relativos a comunicación, marketing digital, creación de contenidos, desarrollo de páginas web, SEO (Search Engine Optimization) y gestión de redes sociales.

Este alcance incluye la infraestructura tecnológica, CPD propio y servicios cloud, aplicaciones, redes y servicios asociados empleados para la prestación de dichos servicios, así como la información tratada en su desarrollo. Incluyendo también su sede única en Madrid y teletrabajo.

De acuerdo con el proceso de categorización conforme al Real Decreto 311/2022 (ENS), los sistemas de información se clasifican con categoría BÁSICA en todas las dimensiones de seguridad.

Afecta a empleados, colaboradores, becarios y terceros que traten información o presten servicios en nombre de la empresa.

## 4. Misión y objetivos

- Garantizar Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad de la información.
- Implementar medidas de seguridad según el riesgo y bajo el principio de 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 de sistemas y servicios.
- 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.
- Vigilancia continua y reevaluación periódica.
- Seguridad por defecto y desde el diseño.
- Diferenciación de responsabilidades (independencia RSEG ≠ RSIS).

## 6. Marco normativo

La presente Política de Seguridad de la Información se sustenta en el siguiente marco legal y reglamentario:

- 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, incluidas las decisiones de adecuación y cláusulas contractuales tipo (SCC).
- Ley 34/2002 (LSSI-CE), de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.
- Real Decreto-ley 13/2012, de 30 de marzo, sobre comunicaciones electrónicas y cookies.
- Reglamento (UE) 910/2014 (eIDAS), de 23 de julio de 2014, sobre identificación electrónica y servicios de confianza.
- Reglamento (UE) 2022/2065 (DSA), de 19 de octubre de 2022, sobre servicios digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Texto Refundido de la Ley de Propiedad Intelectual (LPI).
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica la Ley de Propiedad Intelectual.
- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- Real Decreto 604/2006, de 19 de mayo, de desarrollo de las previsiones de la Ley 31/1995.
- Real Decreto 39/1997, de 17 de enero, Reglamento de los Servicios de Prevención.
- Ley 38/2003, de 17 de noviembre, General de Subvenciones.
- Real Decreto 887/2006, de 21 de julio, que aprueba el Reglamento de la Ley 38/2003.
- Ley 2/1995, de 8 de marzo, de Subvenciones de la Comunidad de Madrid.
- Guías CCN-STIC Serie 800, del Centro Criptológico Nacional, que desarrollan las medidas de seguridad del ENS.

El cumplimiento de este marco normativo se supervisa internamente por el Comité de Seguridad de la Información (CSI) y el Responsable de Seguridad (RSEG), quienes realizan un seguimiento periódico de la legislación aplicable y de las actualizaciones de las Guías CCN-STIC y demás normas técnicas de referencia.

Cuando se detectan modificaciones legales, reglamentarias o técnicas relevantes, el marco normativo se actualiza, registrándose los cambios en el Listado Documental ENS y comunicándose al personal afectado.

## 7. Organización de la seguridad

### I. Comité de Seguridad de la Información: funciones y responsabilidades

El Comité de Seguridad (CSI) está formado por los socios igualitarios de la empresa, que conforman la Dirección, y ostentan además los roles ENS:

- Responsable de la Información (RINFO)
- Responsable de los Servicios (RSER)
- Responsable de la Seguridad (RSEG)
- Responsable del Sistema (RSIS)

La segregación mínima entre RSEG y RSIS está garantizada.

El CSI ejerce directamente las funciones de gobierno, supervisión y mejora del sistema de seguridad de la información, sin necesidad de elevar decisiones a otra instancia jerárquica.

Sus funciones principales son:

**Funciones principales:**

- Supervisar el análisis de riesgos, los indicadores de seguridad (KPIs) y las medidas implantadas.
- Revisar los incidentes de seguridad y de protección de datos, asegurando su correcta gestión y cierre.
- Controlar la Declaración de Aplicabilidad (DoA) y la autoevaluación ENS anual.
- Validar y actualizar los procedimientos, políticas y registros ENS conforme a los resultados de las revisiones.
- Revisar periódicamente la continuidad de servicio, las copias de seguridad y los mecanismos de recuperación.
- Evaluar los proveedores críticos y servicios externos, verificando su cumplimiento de las medidas ENS.
- Resolver conjuntamente las discrepancias o decisiones técnicas que afecten a la seguridad del sistema.
- Coordinar la actualización del marco normativo y la adaptación del sistema a cambios legales, tecnológicos u organizativos.

El CSI se reunirá al menos una vez al año, y siempre que se produzca un incidente grave, un cambio relevante o una necesidad de revisión.

De cada sesión se levantará acta, firmada por los miembros del CSI y archivada en el Repositorio ENS.

## II. Roles: funciones y responsabilidades

Los roles definidos en el marco del Esquema Nacional de Seguridad (ENS) son desempeñados por los socios igualitarios de CÍRCULO DE COMUNICACIÓN, S.L., conforme a la designación formal recogida en el Acta de constitución del Comité de Seguridad de la Información y nombramiento de responsables.

- **Responsable de la Información (RINFO)**

  Propietario del uso, clasificación y protección de la información tratada por la organización. Determina los niveles de seguridad aplicables según las dimensiones del ENS y autoriza el tratamiento, almacenamiento o eliminación de la información.

- **Responsable del Servicio (RSERV)**

  Propietario del servicio y de su nivel de prestación. Garantiza que los servicios digitales (comunicación, marketing, desarrollo web, SEO, redes sociales, etc.) se mantengan dentro de los niveles de seguridad, disponibilidad y continuidad definidos en el ENS.

- **Responsable de Seguridad (RSEG)**

Supervisa la implantación y eficacia de las medidas de seguridad. Coordina el sistema ENS, promueve la mejora continua, la formación y la concienciación del personal. Además, lidera la gestión de incidentes y el seguimiento de la Declaración de Aplicabilidad (DoA).

Tiene autoridad para registrar incumplimientos y promover acciones correctoras o preventivas.

- **Responsable del Sistema (RSIS)**

  Administra y mantiene los sistemas de información durante su ciclo de vida. Aplica las medidas técnicas, gestiona configuraciones, actualizaciones y copias de seguridad, y colabora con el RSEG en la gestión de incidentes, cambios y análisis de riesgos.

- **Delegado de Protección de Datos (DPD)**

  Actualmente no se designa un DPD interno, al no concurrir los supuestos exigidos por el artículo 37 del RGPD. Las funciones de supervisión y asesoramiento en materia de protección de datos se asumen internamente por el RSEG, con apoyo de una consultoría externa especializada.

Se mantiene la segregación mínima exigida entre el RSEG y el RSIS, garantizando la independencia funcional entre la supervisión y la operación, conforme al artículo 11 del Real Decreto 311/2022.

### III. Procedimientos de designación y suplencias

Los roles ENS fueron designados directamente por los socios igualitarios de CÍRCULO DE COMUNICACIÓN, S.L., que actúan de forma colegiada como Dirección y como miembros del CSI. Los nombramientos y su aceptación formal constan en el *Acta de constitución del CSI y nombramiento de responsables*.

Los cargos se revisarán cada dos años o antes si se producen cambios organizativos, vacantes o incumplimientos.

Cuando sea necesario, el CSI documentará suplencias temporales para ausencias prolongadas o periodos críticos, garantizando la continuidad operativa del sistema ENS.

### IV. Resolución de conflictos

Dado que los miembros del CSI son los socios igualitarios de la empresa, las discrepancias o conflictos funcionales entre roles se resolverán internamente en el propio Comité, mediante consenso.

Si no fuera posible alcanzar acuerdo, el CSI podrá solicitar asesoramiento técnico o dictamen externo independiente (por ejemplo, de un auditor ENS o consultor acreditado) para la toma de decisión más adecuada.

## 8. Tratamiento de datos personales

CÍRCULO DE COMUNICACIÓN, S.L. trata datos personales de carácter básico -como nombre, apellidos, correo electrónico y número de teléfono- exclusivamente para la gestión de sus servicios de comunicación, marketing digital, creación de contenidos, desarrollo web, SEO y redes sociales.

De acuerdo con lo establecido en el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD), la empresa no está obligada a designar un Delegado de Protección de Datos (DPD), al no cumplir los supuestos previstos en el artículo 37 del RGPD (no se observan personas de forma habitual ni se tratan categorías especiales de datos a gran escala).

Las funciones de supervisión y cumplimiento en materia de protección de datos personales son asumidas directamente por el Responsable de Seguridad (RSEG), con apoyo puntual de una consultoría externa especializada en protección de datos cuando se requiera asesoramiento legal o técnico.

El tratamiento de los datos personales se gestiona de forma coordinada con el Sistema ENS, garantizando la aplicación de las medidas técnicas y organizativas adecuadas en los siguientes ámbitos:

- **Gestión de riesgos:** Los riesgos para los derechos y libertades de las personas se evalúan dentro del análisis general de riesgos ENS.
- **Gestión de terceros:** Los encargados del tratamiento y proveedores externos cumplen con el ENS y el RGPD, incluyendo cláusulas contractuales específicas.
- **Gestión de incidentes:** Cualquier incidente que afecte a datos personales se registra, analiza y comunica siguiendo los procedimientos de incidentes ENS y, cuando proceda, conforme al artículo 33 del RGPD.
- **Actualización y mejora continua:** El CSI revisa anualmente el cumplimiento de las medidas de protección de datos y actualiza los registros de actividades cuando se incorporan nuevos tratamientos o servicios.

Con esta integración, CÍRCULO DE COMUNICACIÓN, S.L. garantiza el cumplimiento conjunto del ENS, RGPD y LOPDGDD, aplicando el principio de seguridad desde el diseño y por defecto.

## 9. Gestión de riesgos

El análisis de riesgos se realizará de forma proporcional a la categoría básica de los sistemas. Se llevará a cabo:

- Con carácter anual, como parte de la revisión general del sistema ENS.
- Cuando se produzcan cambios relevantes en los servicios, la información tratada o la infraestructura tecnológica.
- Tras la detección de un incidente grave o una vulnerabilidad crítica.
- Ante modificaciones significativas en la normativa aplicable, especialmente en materia de ENS, RGPD o LOPDGDD.

El RSEG, con la colaboración del RSIS, coordinará la identificación, valoración y tratamiento de los riesgos, aplicando los criterios definidos por el CSI.

Los resultados se documentarán en el Informe de Análisis de Riesgos y se mantendrán actualizados en el Repositorio ENS, junto con los registros de medidas y controles asociados.

El CSI establecerá una valoración de referencia por tipo de activo, información o servicio, y promoverá la adopción de medidas horizontales de seguridad que refuercen la protección común del sistema.

En lo relativo a la protección de datos personales, los riesgos específicos para los derechos y libertades de las personas se evaluarán conjuntamente con los riesgos ENS.

El RSEG, con apoyo de consultoría externa en protección de datos, asegurará la coherencia entre ambos análisis y la correcta coordinación de 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 CÍRCULO DE COMUNICACIÓN, 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 en un repositorio interno 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

CÍRCULO DE COMUNICACIÓN, S.L. contrata determinados servicios externos de soporte técnico, alojamiento web, copias de seguridad, mantenimiento y gestión administrativa.
Dichos proveedores pueden acceder a información o sistemas incluidos en el alcance del ENS, por lo que su gestión se realiza conforme a los principios de seguridad, confidencialidad y cumplimiento normativo establecidos en esta Política.

Cuando los servicios impliquen el tratamiento de información o datos personales, se garantizará que los terceros:

- Cumplen con los requisitos del Esquema Nacional de Seguridad (ENS) aplicables a su nivel.
- Incorporan en los contratos las cláusulas de confidencialidad, protección de datos y seguridad necesarias.
- Notifican con diligencia cualquier incidente de seguridad que pudiera afectar a la información de la empresa.
- Aceptan el derecho de auditoría o verificación por parte de CÍRCULO DE COMUNICACIÓN, S.L. o del CSI.
- En el caso de servicios en la nube, garantizan el cumplimiento de la normativa ENS y RGPD, incluyendo la ubicación de los datos dentro del Espacio Económico Europeo o en países con decisión de adecuación.

Antes de formalizar cualquier nueva contratación o renovación, el Responsable de Seguridad (RSEG) evaluará el cumplimiento del proveedor y, en caso de detectar desviaciones o riesgos, elaborará un informe de evaluación de riesgos de terceros.
Este informe será revisado por el CSI, que decidirá de forma colegiada si procede la contratación o renovación, asumiendo expresamente los riesgos residuales identificados.

La Dirección/CSI mantendrá actualizada una relación de proveedores críticos y sus contratos asociados, controlando la vigencia de las cláusulas de seguridad y protección de datos, y revisándolas anualmente o ante cualquier cambio significativo.

## 13. Gestión de incidentes de seguridad

CÍRCULO DE COMUNICACIÓN, S.L. dispone de un procedimiento para la gestión ágil de eventos e incidentes que puedan afectar a la información y a los servicios. Este procedimiento se coordina con las medidas y obligaciones establecidas en otras normas de aplicación directa, especialmente el RGPD, la

LOPDGDD y la LSSI-CE, para garantizar una respuesta coherente ante incidentes que afecten tanto a la seguridad de la información como a la protección de datos personales.

La gestión la realizan directamente el Responsable de Seguridad (RSEG) y el Responsable del Sistema (RSIS), aplicando medidas de contención, recuperación y prevención según la gravedad del incidente.

Si el incidente afecta a datos personales, se actuará conforme al RGPD y la LOPDGDD, notificando a la Agencia Española de Protección de Datos (AEPD) cuando proceda.

En caso de que el incidente sea grave, implique riesgos para terceros o exista posible delito o intrusión, se informará sin demora a las Fuerzas y Cuerpos de Seguridad del Estado o, si corresponde, a las autoridades judiciales.

Todos los incidentes se registran en el Repositorio ENS, y tras su resolución, el CSI (RSEG y RSIS) analiza las causas, documenta las lecciones aprendidas y actualiza las medidas de seguridad y el Plan de Acciones Correctoras (PAC).

## 14. Aprobación, revisión y sustitución de la Política

La presente Política de Seguridad de la Información ha sido aprobada por la Dirección de CÍRCULO DE COMUNICACIÓN, S.L., integrada por los socios igualitarios que conforman el Comité de Seguridad de la Información (CSI).

El CSI (RSEG y RSIS) revisará esta Política al menos una vez al año, o antes si se producen cambios relevantes en la organización, los servicios, la normativa aplicable o el análisis de riesgos.

Las modificaciones menores (actualización de referencias, corrección de ineficiencias o ajustes de forma) podrán incorporarse directamente por el RSEG, manteniendo el control de versiones en el Repositorio ENS.

Cualquier cambio sustancial que afecte a los principios, responsabilidades o alcance del sistema será aprobado formalmente por el CSI/Dirección, documentándose en acta y comunicándose al personal afectado.

La versión actualizada de la Política se conservará en el Repositorio ENS y estará disponible para todo el personal que deba conocerla.