POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

RG-PRE-01.05

Edición 06

Responsable de Sistemas IT

Unidad de Sistemas

10/08/2026

ÍNDICE

1. Objetivo Y Alcance

La presente Política de Seguridad de la Información establece el marco estratégico, los principios y las directrices que rigen la gestión de la seguridad de la información en CIRCE.

Su finalidad es garantizar la calidad de la información y la prestación continuada de los servicios, con el objeto de actuar preventivamente ante posibles incidencias y reaccionando con rapidez ante la materialización de las mismas. Con ello, asegurando en todo momento las dimensiones de seguridad:

- Confidencialidad: la información es accesible únicamente a personas y sistemas autorizados.
- Integridad: la información es exacta, completa y no ha sido alterada de forma no autorizada.
- Disponibilidad: los sistemas y la información están accesibles cuando son requeridos.
- Autenticidad: se garantiza el origen legítimo de la información y las identidades de los agentes.
- Trazabilidad: las actuaciones sobre la información son atribuibles de manera unívoca a los responsables.

Esta Política va alineada con los requisitos establecidos dentro de los correspondientes Artículos del ENS.

Asimismo, el ámbito de aplicación comprende:

- Todos los sistemas de información de CIRCE, incluyendo infraestructuras TIC, aplicaciones, datos y servicios en la nube. Incluyendo las unidades y áreas que hagan uso de ellos.
- Todo el personal de CIRCE (trabajadores, becarios, colaboradores internos).
- Proveedores, contratistas y terceros con acceso a sistemas o información de la Organización.
- Los sistemas que soportan el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos.

> *Referencias normativas: ENS (RD 311/2022) — Art. 11 (Política de Seguridad)*

2. Contexto de la organización

2.1 Misión y actividad

CIRCE (Centro de Investigación de Recursos y Consumos Energéticos) es una fundación cuya misión es:

> *Mejorar la competitividad de las empresas mediante la generación y transferencia de tecnología a través de actividades de I+D+i y formación, orientadas al mercado y en el ámbito de la sostenibilidad y la eficiencia de los recursos, las redes energéticas y las energías renovables.*

En el desarrollo de su actividad, CIRCE trata información sensible de carácter científico, tecnológico, contractual y personal, cuya protección resulta esencial para mantener la confianza de los patronos, clientes, entidades financiadoras y personal de CIRCE.

2.2 Partes interesadas y requisitos

CIRCE identifica y evalúa periódicamente los requisitos de seguridad provenientes de las principales partes interesadas como se indica en la ficha de proceso PRE-02 Comunicación con las Partes interesadas.

> *Referencias normativas: ISO/IEC 27001:2022 — Cláusula 4.1, 4.2 • ENS — Art. 11*

3. Liderazgo y compromiso de la Dirección

La Dirección de CIRCE asume de forma explícita el compromiso con la seguridad de la información como un elemento estratégico y transversal de la Organización. Este compromiso implica:

- Establecer, aprobar y comunicar la presente Política de Seguridad de la Información.
- Asignar los recursos humanos, técnicos y económicos necesarios para la implantación y mantenimiento del SGSI.
- Promover una cultura de seguridad en toda la Organización.
- Revisar periódicamente el desempeño del SGSI y esta Política.
- Asegurar que los objetivos de seguridad son compatibles con la dirección estratégica de CIRCE.
- Apoyar la mejora continua del Sistema de Gestión de Seguridad de la Información.

> *Referencias normativas: ENS — Art. 11 (Misión del responsable de seguridad)*

4. Marco normativo de referencia

La presente Política se elabora en cumplimiento del marco jurídico y normativo siguiente:

Norma / Legislación	Descripción
RD 311/2022 — ENS	Esquema Nacional de Seguridad
LO 3/2018 — LOPDGDD	Ley Orgánica de Protección de Datos
Reglamento (UE) 2016/679 — RGPD	Reglamento General de Protección de Datos

5. Organización de la seguridad

Para asegurar el gobierno efectivo de la seguridad de la información, CIRCE establece una estructura organizativa clara con roles, responsabilidades y autoridades definidos y documentados.

5.1 Roles y responsabilidades

El detalle de funciones, procedimientos de designación y renovación de roles se recoge en los documentos 'RG-PRE-01.4 Reglamento del CSI' y 'RG-PRA-01.1 Roles y Responsabilidades'.

> *Referencias normativas: ENS — Art. 11—13 (Responsable de Información, Responsable del Sistema, Responsable de Seguridad)*

6. Gestión de riesgos de seguridad

CIRCE adopta un enfoque sistemático y proactivo para la identificación, evaluación y tratamiento de los riesgos de seguridad que afectan a sus sistemas de información y activos.

6.1 Proceso de evaluación de riesgos

Todos los sistemas de información en el ámbito de esta Política son sometidos a un análisis de riesgos que evalúa las amenazas y vulnerabilidades a las que están expuestos. Este análisis se realizará:

- Con carácter ordinario: al menos una vez al año.
- Cuando se produzcan cambios relevantes en la información tratada o en los servicios prestados.
- Tras la ocurrencia de un incidente de seguridad calificado como grave o muy grave.
- Cuando se reporten vulnerabilidades críticas que afecten a los sistemas.
- Ante cambios significativos en el contexto organizativo, tecnológico o normativo.

Para la estandarización de los riesgos se establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. Dirección promoverá la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.

6.2 Tratamiento de riesgos

Los riesgos identificados serán tratados mediante alguna de las siguientes opciones: mitigación (aplicación de controles), transferencia (seguros, contratos con terceros), aceptación (cuando el riesgo residual es asumible) o eliminación (supresión de la actividad que genera el riesgo). La Dirección garantizará la disponibilidad de los recursos necesarios para implementar el tratamiento acordado.

> *Referencias normativas: ENS — Anexo II (Medidas de seguridad)*

7. Principios y líneas de actuación

La gestión de la seguridad en CIRCE se articula en torno a los siguientes principios operativos:

7.1 Prevención

CIRCE adopta las medidas técnicas y organizativas necesarias para prevenir incidentes de seguridad o minimizar su impacto. Entre ellas:

- Implantación de controles mínimos de seguridad conforme a la legislación vigente y a los resultados del análisis de riesgos.
- Autorización formal de los sistemas de información antes de su puesta en producción.
- Verificación regular de la configuración de seguridad de los sistemas.
- Revisión independiente periódica por parte de terceros (auditorías externas).

7.2 Detección

CIRCE monitoriza de forma continua sus sistemas para detectar anomalías, incidentes y desviaciones respecto a los parámetros de seguridad establecidos. Se dispone de mecanismos de detección, análisis y reporte que alimentan al Responsable de Seguridad y al CSI de forma regular y ante eventos significativos.

7.3 Respuesta y recuperación

CIRCE dispone de procedimientos de respuesta a incidentes y de planes de continuidad de los sistemas TIC, que permiten reaccionar y restaurar la operatividad de los servicios críticos en caso de materialización de un incidente grave. La respuesta a incidentes contempla:

- Contención y análisis del incidente.
- Notificación a las autoridades competentes cuando proceda (AEPD, CCN-CERT).
- Recuperación de los servicios afectados.
- Análisis post-incidente y mejora de controles.

> *Referencias normativas: ENS — Anexo II, medidas op.mon y op.cont*

8. Protección de datos de carácter personal

CIRCE cumple con la legislación vigente en materia de protección de datos personales, en particular el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD). Para ello dispone de políticas, procedimientos y medidas técnicas y organizativas que garantizan la protección de los datos personales bajo su responsabilidad, asegurando las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Todos los sistemas de información que traten datos personales se ajustarán a los niveles de seguridad requeridos en función de la naturaleza y finalidad del tratamiento, aplicando el principio de privacidad desde el diseño y por defecto.

> *Referencias normativas: ENS — Art. 24 • RGPD — Arts. 25, 32*

9. Obligaciones del personal

Todo el personal de CIRCE, con independencia de su vinculación contractual, tiene la obligación de:

- Conocer y cumplir la presente Política de Seguridad y la normativa de seguridad aplicable.
- Completar las acciones de concienciación y formación en seguridad promovidas por la Organización.
- Notificar cualquier incidente o sospecha de incidente de seguridad a través de los canales establecidos.
- No divulgar información confidencial ni facilitar accesos no autorizados a los sistemas.
- Utilizar los activos de información únicamente para los fines autorizados.

Las personas con responsabilidad en la gestión u operación de sistemas de información recibirán formación específica adecuada a sus funciones antes de asumir sus responsabilidades. La formación se renovará ante cambios de puesto o de responsabilidades.

La Dirección es responsable de garantizar que la información sobre la Política llega a todos los afectados y de proporcionar los medios necesarios para su cumplimiento.

> *Referencias normativas: ENS — Art. 30 (Obligaciones del personal)*

10. Terceras partes

CIRCE extiende sus requisitos de seguridad a todos los proveedores, contratistas y terceros que presten servicios o accedan a información de la Organización.

- Los terceros serán informados de esta Política y de la normativa de seguridad aplicable a los servicios prestados.
- Los contratos con terceros incluirán cláusulas de seguridad y protección de datos acordes con los requisitos normativos vigentes.
- Se establecerán canales de reporte y coordinación en materia de incidentes de seguridad.
- Cuando CIRCE actúe como prestador de servicios a otras organizaciones, les comunicará esta Política y articulará los mecanismos de coordinación necesarios.
- Cuando algún aspecto de esta Política no pueda ser satisfecho por un tercero, se requerirá un análisis documentado de los riesgos incurridos y las medidas de tratamiento adoptadas.

> *Referencias normativas: ENS — Art. 28 (Servicios externos)*

11. Gestión documental del SGSI

La documentación del Sistema de Gestión de Seguridad de la Información se gestiona conforme a lo definido en la ficha de proceso 'PRA-04 Herramientas SG'.

El Responsable del Sistema (Director de Sistemas IT) es el custodio de toda la documentación del SGSI. Por otro lado, la sección de Sistemas IT son los únicos con potestad para modificar el nivel de seguridad requerido para cada documento.

Los criterios de clasificación y nivel de seguridad se recogen en el documento 'IT-PRA-09-06.01 Medidas de Seguridad Aplicables a la Información'.

La presente Política tiene carácter PÚBLICO y será publicada en la web corporativa de CIRCE como expresión del compromiso de la Organización con la seguridad de la información.

> *Referencias normativas: ENS — Anexo II, medidas org.3*

12. Mejora continua y revisión de la Política

La presente Política será revisada con la periodicidad establecida en la ficha de proceso 'PRA-04 Herramientas SG', o cuando se produzcan cambios significativos en el contexto de la Organización, en la legislación aplicable o en el entorno de amenazas. La revisión será realizada por el Comité de Seguridad de la Información y aprobada por la Dirección.

CIRCE se compromete a la mejora continua de la eficacia y eficiencia del SGSI, estableciendo objetivos de seguridad medibles y haciendo seguimiento de su cumplimiento mediante indicadores, auditorías internas y revisiones por la dirección.

> *Referencias normativas: ENS — Art. 35 (Auditoría de la seguridad)*

Glosario de términos

A continuación se recogen las definiciones de los principales términos empleados en la presente Política:

Término	Definición
SGSI	Sistema de Gestión de Seguridad de la Información. Marco estructurado de políticas, procesos y controles para gestionar la seguridad de la información.
ENS	Esquema Nacional de Seguridad (RD 311/2022). Marco regulatorio español de seguridad para las Administraciones Públicas y sus proveedores.
RGPD	Reglamento General de Protección de Datos (Reglamento UE 2016/679). Legislación europea sobre tratamiento de datos personales.
CSI	Comité de Seguridad de la Información. Órgano de gobierno del SGSI en CIRCE.
Confidencialidad	Propiedad por la que la información es accesible únicamente a personas, procesos o sistemas autorizados.
Integridad	Propiedad por la que la información es exacta, completa y no ha sido modificada de forma no autorizada.
Disponibilidad	Propiedad por la que los sistemas y la información son accesibles y utilizables cuando son requeridos por usuarios autorizados.
Autenticidad	Propiedad por la que se garantiza la identidad de una entidad o el origen de la información.
Trazabilidad	Propiedad por la que las acciones realizadas sobre la información son atribuibles de forma exclusiva a la entidad que las realizó.
Activo de información	Cualquier información o sistema que tiene valor para la Organización y que debe ser protegido.
Riesgo	Combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas sobre los objetivos de la Organización.