CIES seresco

Sistema de Gestión Integrado de CIES

TLP:CLEAR

Mayo 2026

v 1.8

Política de Seguridad de la Información, Privacidad e IA

10.24V1

Información sobre el documento

Catalogación de la información contenida en este informe:

Código	¿Cuándo utilizarlo?	¿Cómo compartirlo?
TLP:RED	Se debe utilizar TLP:RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente.
TLP:AMBER TLP:AMBER + STRICT	Se debe utilizar TLP:AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que deban estar al tanto para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información. Nota: se debe especificar TLP:AMBER+STRICT, si la fuente desea restringir la compartición sólo a la propia organización.
TLP:GREEN	Se debe utilizar TLP:GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.
TLP:CLEAR	Se debe utilizar TLP:CLEAR cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información TLP:CLEAR puede ser distribuida sin restricciones, sujeta a controles de Copyright.

versión 2.0 de TLP

Este documento está catalogado como: TLP:CLEAR

HISTORIAL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	5/06/18	Responsable de Seguridad	Versión inicial del documento
1.1	13/07/18	Responsable de Seguridad	Inclusión en el apartado de legislación aplicable, las ITS de Auditoría de 27/03/2018 y a la ITS de Notificación de incidentes de 13/04/2018. Referencia al procedimiento de organización de la documentación
1.2	13/04/20	Responsable de Seguridad	Inclusión de Grupo CIES, actualización de la información sobre los servicios del Grupo, actualización de legislación aplicable, actualización de composición del Comité, nuevo rol de Administrador de seguridad
1.3	30/07/20	Responsable de la Seguridad	Incorporación del término de "Responsable de la Seguridad" como equivalente al de "Responsable de Seguridad", y la recomendación de uso en el SGSI de Grupo CIES. Ampliación de la información de alcance de SGSI de Grupo CIES en el documento de Política
1.4	15/02/22	Responsable de la Seguridad	Se revisa el contenido de la política, se actualiza el alcance
1.5	15/06/22	Responsable de la Seguridad	Se revisa el contenido de la política, se añade referencia al Real Decreto 311/2022
1.6	15/07/22	Responsable de la Seguridad	Se revisa el contenido de la política y las designaciones

1.7	13/06/24	Responsable de la Seguridad	Se revisa el contenido de la política y las designaciones, se adecua al ENS (Real Decreto 311/2022). Se modifica el Comité de Seguridad conforme a los cambios de la organización.
1.8	20/05/26	Responsable de la Seguridad	Se actualiza la Política, teniendo en cuenta la política de seguridad de SERESCO. Se integra el SIG ENS con ISO 27001, 27701 y 42001. Se modifica el título del documento.

CONTROL DE FIRMAS

	FECHA	
ELABORADO POR: Responsable del Sistema y Responsable de Seguridad Delegado	20/05/26	
REVISADO POR: Responsable de Seguridad Delegada de Protección de Datos Responsable de IA	20/05/26	
	FECHA	FIRMA
APROBADO POR: Comité de Seguridad	26/06/26	SANTIRSO MENENDEZ MARIA JESUS - 09427744K Firmado digitalmente por SANTIRSO MENENDEZ MARIA JESUS - 09427744K Fecha: 2026.06.26 11:04:29 +02'00'

Índice

Plaza Santa Bárbara, edif. 2. portal 4. Oficinas 18-19 Parque Empresarial de Asipo - 33428 Llanera (Asturias)
(+34) 985 547 414
(+34) 985 543 313
www.ciescc.es

1 INTRODUCCIÓN

La organización ha considerado la necesidad de gestionar la seguridad como un todo completo, transversal en la entidad en cada proceso interno y externo, como una cuestión estratégica de la organización.

La implementación de un sistema de gestión de la seguridad de la información está condicionada a las necesidades de negocio y a las líneas marcadas por los objetivos organizacionales, entre los que se encuentran actualmente, los objetivos de seguridad de la organización. Todos los procesos internos y externos quedan adscritos y afectos, a la presente política, o cuantas políticas transversales se desarrollen para dar cumplimiento a la misma.

La seguridad, por tanto, debe ser entendida como el conjunto de principios básicos y requisitos mínimos requeridos para una protección adecuada de la información tratada y los servicios prestados a los terceros.

Nuestra organización ya ha venido dando pasos en este sentido, y ha considerado prioritario establecer los objetivos de seguridad con plena alineación con los objetivos de negocio que ha culminado con la certificación del sistema de gestión conforme a los requisitos establecidos en el Real Decreto 311/2022.

Por defecto, la Dirección de Infraestructura, Ciberseguridad y Cumplimiento (ICC) que tiene delegadas sus funciones por la Dirección de CIES -Grupo Seresco- (en adelante la Dirección), ha considerado que la organización es la responsable de los activos de información y de los recursos de su propiedad y asume, que las tareas relacionadas con la seguridad de la información son una parte fundamental para el desarrollo de negocio.

La organización considera que la seguridad de la información debe evolucionar continuamente para adecuarse a los requerimientos de negocio, sin impactar injustificadamente en el mismo y teniendo en cuenta la adecuada relación entre costes y beneficios. En esta concepción, la organización considera que se deben integrar otros aspectos críticos que, si bien tienen su propia independencia y normativa rectora, son imprescindibles para que los activos estén protegidos. Es por ello que en esta Política se integra también el compromiso de la organización con el cumplimiento de la normativa de protección de datos personales y el adecuado cumplimiento del uso de la inteligencia artificial (IA) a la normativa vigente, siendo además esta tecnología, un riesgo emergente que debe ser considerado.

Para desarrollar esta política, se establecerán normas, procedimientos e instrucciones detalladas, los cuales serán publicados y comunicados a todos los usuarios, terceros y socios de negocio de CIES Ciberseguridad y Cumplimiento, S.L. (Grupo Seresco), en adelante CIES, cuando los mismos se vean afectados. La presente Política será accesible para las partes internas y externas afectadas.

1.1 Estándar de Seguridad de la Información, Privacidad e IA

Se considerarán todos los elementos de seguridad necesarios, y específicamente el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad) y a los controles establecidos en el Anexo II.

Se considerarán todos los requisitos y controles de la seguridad de la información del Anexo A de la norma UNE-ISO/IEC 27001:2023.

Se considerarán los requisitos de privacidad definidos en la norma UNE-ISO/IEC 27701, en base a la vigente normativa de protección de datos.

Se consideran todos los requisitos de los sistemas de inteligencia artificial (IA) en la norma ISO /IEC 42001 y en la vigente normativa que regula el uso de la IA.

En base a estos estándares, se ha impuesto un sistema, con los requisitos propios de un sistema de gestión de seguridad de la información, protección de datos e IA, considerando las particularidades del negocio, de la organización y del cliente tipo.

La organización puede considerar la necesidad de someterse a una certificación de un tercero externo independiente, que permita acreditar la alineación el sistema de gestión implantado a la/s norma/s, según descripción de la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad (ENS) y a los requisitos de certificación de las normas ISO. La organización, en relación con la seguridad de la información, considerará otras normas de uso no obligatorio, pero de referencia, y específicamente la serie de Guías 800 publicadas por el Centro Criptológico Nacional CCN-CERT. Así mismo, en el marco de las especialidades de la protección de datos personales y de la IA atenderá a los criterios interpretativos de las autoridades de control en la medida que le afecten como el Comité Europeo de Protección de Datos Personales, la Agencia Española de Protección de Datos y al Agencia Española de Supervisión de Inteligencia Artificial (AESIA).

La organización debe cerciorarse que la seguridad es una parte integral de cada etapa del ciclo de vida del sistema (incluyendo los de IA) y de la información (incluyendo los datos personales), desde el diseño de un producto o un servicio hasta su retirada. Incluyendo las diferentes fases de desarrollo o adquisición y la propia producción o explotación. El sistema deberá estar diseñado para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad que afecten a los diferentes activos, teniendo también en cuenta las diferentes obligaciones que en función de los activos puedan verse afectadas.

La organización mantendrá un inventario actualizado de sistemas de IA, modelos, casos de uso, proveedores y responsables asociados.

2 ESTRATEGIA CORPORATIVA

Se implanta una estrategia corporativa en CIES, alineada en el marco del Plan Estratégico de SERESCO S.A. y SERESCO Atlántico, Unipessoal, Lda y acorde a su misión para garantizar la seguridad del sistema y el adecuado servicio prestado garantizar la protección de datos personales y el uso adecuado a la norma y dentro de los estándares éticos del Grupo para la IA, lo que implica necesariamente que todos los recursos deben disponer y aplicar las medidas mínimas de seguridad exigidas, y en concreto las que sean de aplicación de las contenidas en el Anexo II del Real Decreto 311/2022, en el Anexo A de la norma UNE-ISO/IEC 27001, los requisitos definidos en la norma UNE-ISO/IEC 27701 y la ISO/IEC 42001.

3 OBJETIVO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, PRIVACIDAD E IA

El objetivo de la Seguridad de la Información es garantizar la calidad de la información, incluyendo el tratamiento de datos personales y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con urgencia ante estos para recuperarse lo antes posible y minimizar el impacto tanto en la organización como en los derechos y libertades de las personas afectadas.

Este objetivo de la política de la seguridad de la información se complementa por la protección de los activos que soportan el sistema de información de la organización y los procesos internos, implicados en los servicios declarados en este documento, quedando afectadas las tres dimensiones de seguridad –*confidencialidad, integridad y disponibilidad*-, y cuando fuera preciso, incorporando otras dimensiones –autenticidad y trazabilidad- (por requerimiento legal), quedando alineada plenamente con los objetivos de negocio e integrándose en la estrategia de la organización.

Esta Política se desarrolla por medio de la Normativa de Seguridad y por las distintas políticas, procedimientos, instrucciones y/o directrices definidas por SERESCO que son de aplicación para todas las empresas participadas, puestas a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Por último, deberá alinearse con el requerimiento legal 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 esos datos – Reglamento General de Protección de Datos (RGPD), por lo que se considera a todos los efectos, este documento como el documento de alto nivel que declara la Privacidad como integrada en la Estrategia de Seguridad corporativa y en el Objetivo General de Seguridad.

Esta política, asimismo, tiene como objetivo establecer directrices claras para la, implementación y uso de tecnologías de inteligencia artificial (IA) en CIES. asegurando que se utilicen de manera ética, segura y en cumplimiento con las leyes y regulaciones aplicables.

Además, se alinea con los objetivos de un comportamiento adecuado a la norma y dentro de los estándares de comportamiento ético definidos en la medida que, como empresa participada afecta a la organización, y por el Reglamento 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (Reglamento Europeo de Inteligencia Artificial).

3.1 Servicios - Línea de negocio

CIES está especializada en servicios de ciberseguridad organizada en diversas unidades de negocio en diferentes disciplinas, con una filosofía de cumplimiento global que incluye no solo la seguridad sino también la garantía del derecho a la protección de datos y el uso responsable de la IA, que ofrece un servicio integral de seguridad, sobre la base de un equipo multidisciplinar con más de 15 años de experiencia, en las Administraciones y Sector Público. Principales servicios: cumplimiento normativo, e Esquema Nacional de Seguridad (ENS), Reglamento General de Protección de Datos (RGPD/GDPR), Transparencia y adecuaciones a la normativa en Inteligencia Artificial. Proyectos de seguridad basados en certificaciones de estándares internacionales (ISO 27001, 27701, 20000 y 22301, 42001), actividades de formación, tanto presencial como a través de plataformas on-line, servicios relacionados con la protección de activos mediante seguridad ofensiva (hacking ético, hacking social, auditoría seguridad tecnológica,

etc.), y seguridad defensiva con la implantación de herramienta para facilitar el cumplimiento de las medidas de seguridad (Firewalls, NAC, Cifrado datos, Antimalware, IDS, SIEM, soluciones IRM/DLP, etc.) así como proyectos de apoyo en la implantación de las Leyes 39 y 40 de 2015, a través de procesos de transformación digital, sistemas de monitorización y detección temprana de incidentes (SOC). Objetivos particulares de seguridad de la información.

Los objetivos de seguridad de la información definidos por CIES, han sido desarrollados y aprobados por la Dirección, considerando los requerimientos identificados de las partes interesadas (internas y externas), la gestión de los riesgos y para cumplir con los requisitos de seguridad establecidos por la alta dirección.

La organización ha establecido como objetivos clave de la seguridad de la información y la garantía de la protección de datos, los siguientes:

- Mantener el pleno cumplimiento legal alineando los procesos y los servicios, a la normativa vigente[1] en cada momento, y que afecta de manera indirecta o directa, al perfil de cliente (privado o administración pública), a la información implicada (pública, restringida o secreta) o en general a la seguridad de la información. Especial referencia al declarado REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 y en obviamente, al Real Decreto 311/2022, UNE-ISO/IEC 27001 e UNE-ISO/IEC 27701.
- Mantener una gestión adecuada del sistema de gestión de seguridad, mediante la eficiencia y eficacia de la seguridad, de acuerdo con los estándares de seguridad y las buenas prácticas del sector.
- Alinear el requisito legal y la gestión del sistema con la privacidad y la seguridad.
- Establecer y difundir los roles y responsabilidades relacionados con la Seguridad de la Información.
- Sensibilizar y concienciar de manera estable y permanente al usuario de la organización mediante el impulso de acciones por la Dirección y la ejemplificación de esta, en las tareas de seguridad más críticas.
- Fomentar y mantener el buen nombre de la organización en relación con los servicios desarrollados, saber hacer y respuesta activa –reactiva y proactiva- ante incidentes de seguridad, manteniendo la imagen y reputación.
- Asegurar que los activos de la organización, sólo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, según perfiles definidos o según asignaciones extraordinarias.
- Gestionar la implementación de un sistema de seguridad que proporcione ventajas competitivas en relación a otros agentes del sector, aprovechando la inercia competitiva que puede otorgar la gestión adecuada de la seguridad.
- Proteger la información interna y la relacionada con la prestación de los servicios / clientes, considerando las dimensiones de:

[1] La legislación vigente se encuentra identificada en el Anexo 1 de esta política, documento: "01-org.1-Anexo1-Registro_Requisitos_Legales"

- Confidencialidad: Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
- Integridad: Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
- Disponibilidad: La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.

La organización podrá considerar otras dimensiones relacionadas con la seguridad, derivadas de requerimientos legales (o en su caso, de requerimientos de negocio), considerándose:

- Trazabilidad: Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
- Autenticidad: Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a dudas.

Por defecto la organización mantendrá las tres primeras dimensiones de seguridad. Cuando sea preciso se añadirán los dos restantes.

La organización ha establecido como objetivos clave en el uso de la IA, los siguientes:

- Garantizar el uso ético y responsable de la IA. La organización se compromete a que todos los sistemas de inteligencia artificial bajo su control se utilicen de forma ética y responsable, respetando los derechos fundamentales y contribuyendo al bienestar social. Esto implica integrar principios éticos desde el diseño hasta la operación de los sistemas, prevenir impactos negativos injustificados y fomentar una cultura organizacional que promueva la responsabilidad en el uso de la IA, en línea con la normativa vigente y los estándares internacionales.
- Cumplir con el marco legal y normativo aplicable. La organización establece un firme compromiso a garantizar que todos los sistemas de inteligencia artificial que desarrolla adquieren o utiliza cumplan con la legislación vigente y los marcos normativos aplicables a nivel local, nacional e internacional. Esto incluye, entre otros, el Reglamento General de Protección de Datos (RGPD), el Reglamento de Inteligencia Artificial (AI Act), y la norma ISO/IEC 42001:2023, correspondiente al marco normativo de la presente política. Se establecerán mecanismos de seguimiento y evaluación continua para asegurar la conformidad legal, así como procesos de actualización normativa que permitan adaptar los sistemas de IA a los cambios regulatorios. Este compromiso refuerza la transparencia, la rendición de cuentas y la confianza de las partes interesadas.
- Gestionar eficazmente los riesgos asociados a la IA. La organización se compromete a identificar, evaluar y mitigar de forma proactiva los riesgos que puedan derivarse del desarrollo, implementación y uso de sistemas de inteligencia artificial. Esto incluye riesgos técnicos, éticos, legales, sociales y de seguridad, tanto para las personas como para el entorno. Se establecerán procesos sistemáticos de gestión de riesgos, alineados con la norma ISO/IEC 42001, que permitan anticipar impactos negativos, aplicar medidas correctivas y fomentar una toma de decisiones informada. Esta gestión integral de riesgos es esencial para garantizar la fiabilidad, la seguridad y la aceptación social de la IA.

- Fomentar la transparencia y la explicabilidad. La organización promoverá la transparencia y la explicabilidad en todas las fases del ciclo de vida de los sistemas de inteligencia artificial. Esto implica proporcionar información clara y accesible sobre el funcionamiento, los objetivos y las decisiones automatizadas de los sistemas, de forma comprensible para los distintos grupos de interés. Se adoptarán prácticas y herramientas que faciliten la trazabilidad de los modelos, la documentación adecuada y la comunicación efectiva de los resultados. Este enfoque refuerza la confianza de los usuarios, facilita la supervisión humana y contribuye al cumplimiento de los principios éticos y normativos.
- Confiabilidad y robustez. La organización se compromete a implementar sistemas de inteligencia artificial que sean técnicamente confiables, robustos y resilientes frente a fallos, manipulaciones o condiciones imprevistas. Esto implica aplicar buenas prácticas de diseño, validación, pruebas y mantenimiento continuo, asegurando que los sistemas funcionen conforme a sus especificaciones y con un nivel de rendimiento adecuado en distintos contextos. Asimismo, se promoverá la supervisión humana y la capacidad de recuperación ante errores.
- Promover la equidad y prevenir la discriminación. La organización garantizará que los sistemas de inteligencia artificial se diseñen, desarrollen y utilicen de forma justa, evitando sesgos injustificados y resultados discriminatorios. Para ello, se aplicarán metodologías de evaluación de impacto, auditorías algorítmicas y mecanismos de supervisión que permitan detectar y corregir posibles desigualdades en los datos, modelos o decisiones automatizadas. Este enfoque busca asegurar que la IA beneficie a todas las personas por igual, respetando la diversidad y los derechos fundamentales, en coherencia con los principios de equidad.
- Proteger la privacidad y los datos personales. La organización se compromete a salvaguardar la privacidad de las personas y a garantizar la protección de los datos personales en todos los procesos relacionados con sistemas de inteligencia artificial. Esto implica aplicar principios de minimización de datos, anonimización, consentimiento informado y seguridad desde el diseño, conforme al Reglamento General de Protección de Datos (RGPD). Se establecerán controles técnicos y organizativos adecuados para prevenir accesos no autorizados, usos indebidos o filtraciones de información, promoviendo una gestión responsable y transparente de los datos en todo el ciclo de vida de la IA.
- Impulsar la mejora continua del sistema de gestión de IA. La organización fomentará la mejora continua del sistema de gestión de inteligencia artificial mediante la evaluación periódica de su desempeño, la revisión de procesos y la incorporación de aprendizajes y avances tecnológicos. Se establecerán mecanismos de retroalimentación, auditorías internas y análisis de resultados que permitan identificar oportunidades de optimización y adaptación a nuevas necesidades, riesgos o requisitos normativos. Este enfoque dinámico garantiza que el sistema de gestión de IA evolucione de forma sostenible, eficaz y alineada con los valores y objetivos estratégicos de la organización.
- Promover la formación y la cultura organizacional en IA. La organización se compromete a impulsar una cultura organizacional que favorezca el conocimiento, la comprensión y el uso responsable de la inteligencia artificial en todos los niveles. Para ello, se promoverán programas de formación continua, sensibilización y capacitación adaptados a los distintos perfiles profesionales, con el fin de fortalecer las competencias técnicas, éticas y normativas relacionadas con la IA. Esta iniciativa busca no solo mejorar la toma de decisiones y la gestión de riesgos, sino también fomentar una actitud crítica, colaborativa y alineada con los valores de la organización y los principios establecidos en la normativa.

- **Garantizar el respeto a los derechos de Propiedad Intelectual.** La organización se compromete a asegurar que el desarrollo, entrenamiento, implementación y uso de sistemas de inteligencia artificial respeten los derechos de propiedad intelectual de terceros y de la propia entidad. Esto incluye la utilización responsable de datos, modelos, algoritmos y software, verificando que su origen, licencia y condiciones de uso sean legítimos y estén debidamente documentados.

Estos objetivos reflejan el compromiso de la organización con una gestión de la inteligencia artificial que sea ética, legal, segura y alineada con los más altos estándares internacionales, asegurando su contribución positiva y sostenible a largo plazo.

Los objetivos del SGIA se establecerán anualmente y serán medibles mediante indicadores definidos por la Dirección.

4 PRINCIPIOS DE SEGURIDAD, PRIVACIDAD Y USO DE LA IA

La Dirección ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles Esquema Nacional de Seguridad, de la norma UNE-ISO/IEC 27001, UNE-ISO/IEC 27701 y la ISO/IEC 42001.

El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por la Dirección. Existirá un procedimiento de gestión documental, que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Todo el sistema estará enmarcado por los siguientes principios.

4.1 Seguridad y privacidad por defecto

La seguridad y privacidad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

Las funciones de operación, administración y registro de actividad, así como el tratamiento de datos personales, serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde localizaciones o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso.

El uso del sistema será sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Para mantener el proceso de seguridad y privacidad integral, se realizará una calificación de la información, así como la identificación de los datos tratados y de los colectivos afectados-, conforme a los principios de protección frente a pérdidas, accesos indebidos, divulgación o uso indebido, deterioro de la información, alteración o pérdida de disponibilidad. La calificación conllevará necesariamente una política de etiquetado y manipulación y, en su caso, con el registro de actividades del tratamiento.

Se deberá conocer en todo momento el estado de seguridad del sistema o de sus componentes o el tratamiento de datos personales, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les puedan afectar.

4.2 Seguridad basada en el liderazgo y en la organización

La seguridad y la protección de datos deberá comprometer a todos los miembros de la organización, en base a sus diferentes roles, considerando diferentes responsabilidades.

La Dirección será quien lidere la organización y promueva la cultura de seguridad y la garantía del derecho a la protección de datos, asignando los roles requeridos y potenciando la transversalidad de la seguridad y privacidad en cada proceso desarrollado o servicio a terceros.

La seguridad del sistema y la protección de datos personales será revisada de conformidad a los requisitos, la política y los procedimientos aprobados por la Dirección. Las revisiones serán por parte de la Dirección y por revisiones internas o auditorias del sistema. Específicamente la entidad y el sistema se podrán someter a procesos de certificación externos, conforme a lo establecido por el Esquema Nacional de Seguridad, ISO 27001, ISO 27701, ISO 42001 y cualquier otro estándar de seguridad que le pudiera interesar.

4.3 Organización e implantación del proceso de seguridad

Se establece una estructura organizativa en la organización, con roles específicos, pero siempre considerando el principio de separación de funciones. Se designarán a las personas que ocuparán los roles, por periodos anuales, pudiendo ser renovados automáticamente cuando transcurra el citado plazo y la Dirección no establezca una nueva persona para ocupar el cargo[2].

4.4 Seguridad basada en un sistema de gestión

La seguridad del sistema se documentará a través de los procedimientos, registros, instrucciones técnicas, y manuales que serán puestos a disposición de los usuarios implicados en el mismo. Los cambios serán gestionados, las capacidades del sistema serán medidas y controladas y los entornos estarán separados. Se desarrollarán procedimientos de protección del sistema, incluyendo procedimientos de copias y restauración, y cuantas vulnerabilidades pudieran tener el sistema. Estas podrán tener forma de procedimiento general o especificaciones técnicas acordes a los operadores del sistema y de la seguridad.

Se documentarán los acuerdos con proveedores y colaboradores formando parte del sistema, cuando exista un tratamiento de datos personales se suscribirá un contrato de encargado del tratamiento. La cadena de suministro será controlada con relación a los requisitos de seguridad, la prestación de servicios o los cambios de suministradores.

Los proveedores de sistemas IA serán evaluados periódicamente considerando transparencia, seguridad, privacidad, cumplimiento normativo y riesgos asociados.

[2] Mediante el Anexo 2 de la presente Política se definirán los miembros del Comité de Seguridad, documento: "01-org.1-Anexo2-Composición_Comité".

4.5 Análisis y gestión de los riesgos

La gestión de riesgos será parte esencial del proceso de seguridad y privacidad y deberá mantenerse permanentemente actualizado en el seno de la organización, bajo el liderazgo de la Dirección.

La gestión de riesgos se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema de información y la organización, basándose en una metodología detallada y documentada que permita la repetición de la medición y análisis.

La organización establece y mantiene un proceso de gestión de riesgos de IA con el fin de identificar, analizar, evaluar, tratar y monitorizar los riesgos derivados del diseño, adquisición, desarrollo, despliegue, uso, mantenimiento y retirada de sistemas de IA, así como de sus componentes, datos, modelos y proveedores asociados.

La gestión de riesgos se aplicará de forma continua y proporcional al nivel de riesgo, al contexto de uso y al impacto potencial sobre las personas, la organización, los terceros y la sociedad, incluyendo impactos legales, éticos, operativos, de seguridad, privacidad, reputacionales y de continuidad del negocio.

Con carácter no exhaustivo, la organización considerará riesgos de IA relacionados con:

- Falta de transparencia y explicabilidad. La incapacidad de proporcionar información adecuada a las partes interesadas puede ser una fuente de riesgo (es decir, en términos de confiabilidad y responsabilidad de la organización).
- Nivel de automatización. El nivel de automatización puede tener un impacto en varias áreas de preocupación, como la seguridad, la equidad o la protección.
- Problemas con el ciclo de vida del sistema. Las fuentes de riesgo pueden aparecer a lo largo de todo el ciclo de vida del sistema de IA (por ejemplo, defectos de diseño, despliegue inadecuado, falta de mantenimiento, problemas con el desmantelamiento).
- Errores o degradación del rendimiento: resultados incorrectos, alucinaciones, fallos de generalización, sensibilidad a cambios de contexto.
- Sesgos y discriminación: sesgos en datos, variables proxy, resultados desigualitarios, falta de equidad y accesibilidad.
- Decisiones automatizadas y supervisión humana: uso indebido de automatización, sobreconfianza, ausencia de intervención humana eficaz, explicabilidad insuficiente para el caso de uso.
- Privacidad y protección de datos: uso de datos no autorizados, reidentificación, filtraciones, retención excesiva, finalidades incompatibles, transferencias no previstas.
- Seguridad de la información y ciberseguridad: accesos indebidos, exposición de información sensible, vulnerabilidades en integraciones, cadena de suministro.
- Impactos éticos, reputacionales y sociales: daño a confianza, afectación a derechos fundamentales, impactos en transparencia, accountability o percepción pública.
- Cumplimiento normativo y contractual: incumplimientos de RGPD/LOPDGDD, propiedad intelectual, requisitos sectoriales, condiciones de licencias, obligaciones con clientes/proveedores.

- **Riesgos operativos y de continuidad:** dependencia de terceros, indisponibilidad de servicios, cambios unilaterales del proveedor, obsolescencia o falta de soporte.
- **Riesgos de calidad de datos:** datos incompletos, desactualizados, no representativos, ausencia de linaje, trazabilidad o controles de calidad. La organización aplicará su metodología corporativa de gestión de riesgos (alineada con el marco de gestión global de riesgos), adaptada a la naturaleza de la IA.

4.6 Incidentes de seguridad

El proceso de gestión de incidentes incluirá la detección y notificación de los incidentes de seguridad, los relacionados con la normativa de protección de datos y la IA, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas –especialmente cuando afecta a terceros- y el registro de las actuaciones ejecutadas.

Los incidentes de seguridad permitirán la recopilación de evidencias, de manera que se podrá identificar, documentar la recogida, la adquisición y preservación de la información. Cuando estas evidencias afecten a acreditaciones de carácter legal, deberá contarse con el Delegado de Protección de Datos (DPD) y, en su caso, al Responsable del Sistema de IA.

4.7 Continuidad de la actividad

La continuidad formará parte del sistema de gestión, conforme a las necesidades de la organización y los controles establecidos. La organización considera el análisis de impacto y las consecuencias de la información que el mismo muestre.

4.8 Gestión de personal y profesionalidad

Todo el personal relacionado con el sistema y con la información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad, debiendo ser controlados y sus acciones supervisadas.

Cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se conozca, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

La responsabilidad será exigible mediante un **procedimiento disciplinario,** que al igual que pautas de seguridad, conocerá previamente el usuario. Este procedimiento estará alineado con la normativa laboral.

El usuario con acceso concedido al sistema pueda o no desarrollar acciones, estará sometido a secreto y reserva, aun cuando finalice su relación con la organización. Ningún usuario accederá al sistema sin estar previamente informado de este extremo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Se determinan los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

4.9 Protección de las instalaciones

La organización prevendrá los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Las áreas podrán ser de control propio o derivada al propio prestador afectado.

4.10 Autorización y control de los accesos

El acceso controlado a los sistemas de información está limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

4.11 Adquisición de productos de seguridad y contratación de servicios de seguridad

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información, se utilizarán, de forma proporcionada al nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

4.12 Mínimo privilegio

El sistema de información se diseña y configura otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias.
- Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue.
- Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

4.13 Integridad y actualización del sistema

La inclusión de cualquier elemento físico o lógico en el inventario de activos, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

4.14 Protección de la información almacenada y en tránsito

Se implementarán mecanismos para proteger la información almacenada o en tránsito, especialmente cuando ésta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Se desarrollarán procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos. De igual modo, se implementarán mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren los documentos, para garantizar que toda información en soporte no electrónico relacionada estará protegida con el mismo grado de seguridad que la electrónica.

4.15 Registro de la actividad y detección de código dañino

Se habilitarán registros de la actividad de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del ENS, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función laboral, y demás disposiciones que resulten de aplicación.

Se dispondrá de una solución integral de antivirus, tanto en puestos de trabajo como en servidores, que incorpore funcionalidades tanto de EPP (primera línea de defensa en los puestos de la empresa, basada en la prevención), como de EDR (complementa la protección de la solución EPP, detectando código dañino, incorporando mecanismos de respuesta así como medidas para revertir los daños) y de integración con los cortafuegos perimetrales, para bloqueo de funcionalidades en caso de detección de amenazas.

4.16 Mejora continua del proceso de seguridad

El Sistema de Gestión de la Seguridad de la Información implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

4.17 Seguridad y privacidad como requisitos legales

La Dirección ha establecido como compromiso de seguridad la privacidad y el uso responsable de la IA, el pleno cumplimiento de las obligaciones legales y contractuales, ligadas a la información. Los requisitos serán identificados y organizados, para su correcta gestión.

Quedan implicadas todas las normas del sector, normas internacionales, comunitarias, nacionales, autonómicas y locales que sean de aplicación, pero específicamente por su relevancia en el tema, se detallan en el Registro de Requisitos Legales.

4.18 Principio de licitud, lealtad y transparencia

Los datos personales los serán tratados de manera lícita, leal y transparente en relación con el interesado.

4.19 Principio de limitación de la finalidad

Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Salvo, que se procedan a tratar los datos personales posteriormente con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales (de conformidad con el artículo 89.1 del RGPD).

4.20 Principio de minimización de datos

Los datos personales tratados por la entidad serán los adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

4.21 Principio de exactitud

Los datos personales serán exactos y, si fuera necesario, actualizados. Se deberán adoptar las medidas necesarias para suprimir o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

4.22 Principio de limitación del plazo de conservación

Los datos personales serán mantenidos de forma que se permita la identificación de las personas afectadas durante no más tiempo del necesario para los fines del tratamiento de los datos personales. Los datos personales podrán ser conservados durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos según el artículo 89.1 del RGPD, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas con el fin de proteger los derechos y libertades de las personas afectadas.

4.23 Principio de integridad y confidencialidad

Los datos serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

4.24 Principio de legalidad y cumplimiento normativo

La IA se utilizará respetando toda legislación aplicable, incluyendo protección de datos personales (RGPD), propiedad intelectual, normativa laboral y las normas vigentes o emergentes en materia de IA.

4.25 Principio de solidez técnica y seguridad

La solidez técnica y la seguridad son principios fundamentales que exigen que los sistemas de inteligencia artificial funcionen de manera fiable, robusta y segura en todas las fases de su ciclo de vida. Esto implica diseñar e implementar mecanismos que aseguren su correcto desempeño incluso en condiciones adversas o frente a intentos de manipulación. Se deben adoptar medidas preventivas para evitar fallos, vulnerabilidades y usos indebidos, protegiendo tanto a las personas como a los entornos en los que opera la IA. Este principio requiere una supervisión continua, pruebas rigurosas y una gestión activa de los riesgos técnicos y operativos.

4.26 Principio de transparencia y explicabilidad

La transparencia exige que los sistemas de inteligencia artificial operen de forma comprensible y trazable para todas las personas involucradas en su desarrollo, supervisión o uso. Este principio implica proporcionar información clara y accesible sobre el propósito, el funcionamiento, las limitaciones y el grado de automatización de cada sistema. La transparencia permite a las partes interesadas tomar decisiones informadas, facilita la rendición de cuentas y refuerza la confianza en el uso de la IA dentro de la organización. La explicabilidad es un principio fundamental que exige que los sistemas de inteligencia artificial operen de manera comprensible para los seres humanos. Esto implica que las decisiones,

recomendaciones o resultados generados por la IA deben poder ser explicados de forma clara, accesible y proporcional al nivel de impacto del sistema. La explicabilidad permite a las personas entender cómo y por qué se ha llegado a un determinado resultado, facilitando la supervisión, la confianza y la rendición de cuentas en el uso de la IA.

4.27 Principio de responsabilidad y rendición de cuentas

La responsabilidad y la rendición de cuentas son principios que exigen que toda actividad relacionada con el desarrollo, uso y supervisión de sistemas de inteligencia artificial esté sujeta a una asignación clara de responsabilidades. Esto implica que las decisiones automatizadas deben poder ser auditadas, explicadas y, cuando sea necesario, corregidas. La existencia de mecanismos de control y supervisión garantiza que los impactos negativos puedan ser gestionados adecuadamente, refuerza la trazabilidad de los procesos y fortalece la confianza de las partes interesadas en el uso de la IA.

4.28 Privacidad y confidencialidad

Se garantiza la protección de datos personales y confidenciales; no se introducirá en herramientas de IA información privada o sensible que pueda violar nuestras políticas de seguridad de la información o protección de datos.

4.29 Mejora continua

Implementar un enfoque de mejora continua para evaluar y mejorar los sistemas de IA. o Realizar auditorías internas y externas periódicas para identificar áreas de mejora y asegurar el cumplimiento de la política.

Estos principios proporcionan un marco que equilibra el desarrollo tecnológico con la ética, la responsabilidad y el bienestar social, fomentando el uso seguro y beneficioso de la inteligencia artificial.

4.30 Fiabilidad y seguridad

Todo resultado generado por la IA será verificado para asegurar su exactitud y adecuación, y se desplegarán controles para prevenir errores significativos o riesgos de seguridad. La organización se compromete a mantener la IA bajo un ciclo de mejora continua para minimizar riesgos y asegurar la calidad y seguridad de sus resultados.

4.31 Supervisión humana y rendición de cuentas

Las personas siguen siendo responsables finales de las decisiones apoyadas por la IA.
Cualquier acción que incida en procesos de negocio debe ser revisada y aprobada por personal competente, asegurando que no se delegue la responsabilidad ni el juicio crítico a la máquina.

4.32 Principio de bienestar social y ambiental

El bienestar social y ambiental es un principio que orienta el desarrollo y uso de la inteligencia artificial hacia la generación de impactos positivos en las personas y en el entorno. Esto implica evaluar y mitigar los posibles efectos adversos que los sistemas de IA puedan tener sobre la salud, la seguridad, la cohesión social, la inclusión, el medio ambiente o el desarrollo sostenible.

5 ALCANCE

La política de seguridad de la información, será de aplicación a toda la información, incluyendo los datos personales del sistema con independencia del soporte o medio en el que se encuentre, tipología o categoría, a todo el personal de CIES y también a terceros colaboradores, que accedan al sistema y/o presten servicios a la organización, así como a cualquier activo, incluyendo los relacionados con la IA, de información propiedad de la organización, o en régimen de uso y que afecte al sistema, considerándose en cualquier momento del ciclo de vida del sistema de seguridad, protección de datos o IA, de manera que cuando el sistema se encuentre en fase de actualización, el activo no registrado se vea obligado por la política.

Con respecto a los sistemas de información afectados por el Real Decreto 311/2022, norma UNE-ISO/IEC 27001 e UNE-ISO/IEC 27701, ISO/IEC 42001 la organización ha decidido, que el *alcance* de su sistema de SIG, será:

"Sistema de Información, que se puede apoyar en el uso de IA, necesario para la adecuada prestación de servicios las organizaciones públicas y privadas y relacionados con servicios de:

- *Red Team: Auditorías de Seguridad.*
- *Blue Team: Servicios de Seguridad Defensiva.*
- *Consultoría GRC: Gestión de riesgos, cumplimiento normativo, continuidad de negocio y actividades de formación y sensibilización.*
- *Servicio de DPD.*
- *Servicio de CISO As A Service.*
- *Servicio de CSIRT (Recuperación y Respuesta).*
- *Servicio de Oficina Técnica de Ciberseguridad y Cumplimiento Normativo.*
- *Despliegue de herramientas de Ciberseguridad y Cumplimiento Normativo.*
- *Servicios de Seguridad Gestionada (MSSP).*
- *Centro de Operaciones de Seguridad (SOC-NOC) mediante la solución MONSE*
- *Servicios de vigilancia digital.*

Conforme a los requisitos del Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, la norma UNE-ISO/IEC 27001 de 2023 e UNE-ISO/IEC 27701 de 2019 e ISO/IEC 42001 de 2023 según la Declaración de Aplicabilidad vigente."

6 Roles y responsabilidades

El Comité de Seguridad será el órgano encargado de desarrollar las directrices y estrategia de seguridad. Estará formado por:

- La Dirección de Infraestructura, Ciberseguridad y Cumplimiento (ICC) que tiene delegadas sus funciones por la Dirección de CIES -Grupo Seresco-(en adelante la Dirección).
- El Responsable de Seguridad.
- El Responsable de Seguridad Delegado.
- El Responsable del Sistema.
- La Delegada de Protección de Datos (participará en las reuniones del Comité cuando se aborden temas relacionados con la protección de Datos personales).

- La Responsable de Inteligencia Artificial (participará en las reuniones del Comité cuando se aborden temas relacionados con la Inteligencia Artificial).

El Comité de Seguridad tiene atribuidas las funciones asociadas a las de un Responsable de Información y Servicios, por lo que se encargará de:

- Establecer los requisitos/niveles de la información en materia de seguridad.
- Establecer los requisitos/niveles del servicio en materia de seguridad.

El Comité, puede recabar regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.

Este Comité será convocado, con carácter extraordinario, cuando, aparezcan incidentes de seguridad graves y específicamente cuando surjan nuevas necesidades de seguridad o cuando sea preciso por la urgencia de los asuntos a tratar, debiendo convocarse al menos con 24 horas de antelación.

El Comité se reunirá al menos una vez al año de manera ordinaria, con una convocatoria previa, de al menos 3 días laborales, efectuada por la Dirección, mediante correo electrónico. El Comité podrá ser requerido por el Responsable de Seguridad, en cuyo caso la Dirección deberá convocarlo en un periodo máximo de 15 días laborales.

6.1 Dirección

La Dirección, como órgano de gobernanza, alinea la seguridad con el negocio y asume la aprobación, supervisión y decisión estratégica en materia de riesgos, políticas, continuidad, recursos y accesos críticos

Funciones

a) Proponer al Comité de Seguridad las personas que serán designadas como el Responsable de Seguridad y al Responsable del Sistema.
b) Aprobar la Política de Seguridad de la Información, Privacidad e IA y la Normativa.
c) Aprobar el análisis de riesgos y los planes de tratamiento.
d) Aprobar el informe de revisión por la Dirección.
e) Validar los planes de continuidad.
f) Solicitud de compras e inversión.
g) Gestionar los procesos de certificación.
h) Gestión comercial, reclamaciones, cambios en contratos
i) Definir los permisos de accesos de personal a servicios o información considerada crítica

6.2 Responsable de Seguridad

El Responsable de Seguridad se encargará de planificar, decidir, aprobar, supervisar, monitorizar, reportar y coordinar lo que se ha de hacer en materia de seguridad.

Gestionará la seguridad entendida como objetivo transversal u embebido en la estrategia corporativa. Mantendrá y verificará los requisitos de seguridad del sistema y de la información que se pudiera gestionar.

El Responsable de Seguridad actuará como punto de contacto (POC).

Perfil:

Rol ocupado por el CISO de Grupo SERESCO.

Funciones:

a) Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, en su ámbito de responsabilidad.
b) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
c) Designar ejecuciones de análisis de riesgos, revisiones de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema. En la realización de las evaluaciones de riesgos estará apoyado por el Responsable del Sistema y los Responsables de los Activos.
d) Gestionar las revisiones externas o internas del sistema, incluyendo la recogida de indicadores específicos.
e) Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.

6.3 Responsable de Seguridad Delegado

El Responsable de Seguridad delegará funciones en el Responsable de Seguridad Delegado, encargado de ejecutar y/o supervisar funciones concretas que le han sido delegadas, normalmente sobre sistemas.

Perfil:

Persona con conocimientos técnicos, que pueda comprender los riesgos que afronta la organización, alineando los requisitos de seguridad con los requisitos de negocio.

Funciones:

a) Mantener la seguridad de la información manejada por CIES y de los servicios prestados por los sistemas de información, en su ámbito de responsabilidad.
b) Identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
c) Elevar al Responsable de Seguridad la aprobación de cambios y otros requisitos del sistema.
d) Aprobar los cambios en la configuración vigente del Sistema de Información.
e) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes

6.4 Responsable del Sistema

Su función es desarrollar las operaciones sobre el sistema que mantengan la plena seguridad y contará con el apoyo de los Administradores de la Seguridad del Sistema para ejecutar los cambios.

Será considerado el operador del sistema. Podrá incluso paralizar o dar suspensión al acceso a la información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

Perfil:

Persona con perfil que pueda comprender la ejecución y el desarrollo de las operaciones sobre el sistema desde una parcela más práctica y operativa, que conozca la arquitectura de la organización y las tecnologías aplicadas.

Responsabilidades:

a) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
d) El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos, previa consulta con el Responsable de Seguridad y el Responsable de Seguridad Delegado, antes de ser ejecutada.
e) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
f) La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
g) La aplicación de los Procedimientos Operativos de Seguridad.
h) Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información
i) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes
j) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema
k) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución

Los siguientes roles participarán en el Comité de Seguridad cuando sea necesaria su participación:

- Delegada de Protección de Datos
- Responsable de IA

6.5 Responsable del sistema de IA (Responsable del SGIA):

Responsable encargado de dirigir, supervisar y garantizar el uso seguro, ético y conforme a la normativa de los sistemas de inteligencia artificial a lo largo de todo su ciclo de vida.

Perfil:

Perfil profesional con capacidad para comprender tanto la ejecución como el desarrollo de las operaciones del sistema desde una perspectiva práctica y operativa, con conocimiento de la arquitectura organizativa y de las tecnologías implementadas.

Responsabilidades:

- Gobernanza y dirección estratégica de la IA
- Alinear el SGIA con la estrategia, los valores y los principios de IA responsable de la organización
- Proponer a la alta dirección la política de IA, los criterios de priorización, autorización, suspensión y retirada de sistemas de IA, y elevarlos para aprobación.
- Asegurar la coherencia entre la política de IA y el resto de las políticas corporativas (seguridad, privacidad, calidad, compras, recursos humanos, continuidad de negocio).
- Mantener actualizada la matriz RACI de los roles de IA y su encaje con el DPD, el Responsable de Seguridad ENS y los Responsables de la Información, del Servicio y del Sistema ENS.
- Inventario, clasificación y ciclo de vida de los sistemas de IA
- Mantener el inventario de sistemas de IA y de casos de uso, con su finalidad, datos utilizados, lógica general, proveedor y responsables.
- Clasificar cada sistema según el nivel de riesgo del RIA (prohibido, alto riesgo, riesgo limitado, riesgo mínimo,) y según la criticidad ENS, registrando la justificación de la clasificación.
- Supervisar el ciclo de vida (diseño y adquisición, desarrollo, validación, despliegue, operación, mantenimiento y retirada), verificando que en cada fase se aplican los controles organizativos, técnicos y legales.
- Validar los hitos clave del ciclo de vida desde la perspectiva de gobernanza y riesgo. Las decisiones técnicas de operación corresponden al Responsable del Sistema ENS.
- Gestión de riesgos de IA
- Coordinar la identificación, análisis, evaluación y tratamiento de los riesgos de IA (éticos, derechos fundamentales, sesgos, seguridad, privacidad, operativos, reputacionales y ambientales) e integrarlos en el sistema corporativo de gestión de riesgos.
- Validar la proporcionalidad de las medidas de mitigación y promover su implantación. La implantación técnica recae en los responsables operativos correspondientes.
- Activar revisiones extraordinarias ante cambios sustanciales, incidentes o nuevas evidencias (deriva del modelo, cambios regulatorios, cambios contractuales del proveedor).
- Coordinar con el DPD la realización de la Evaluación de Impacto en la Protección de Datos (EIPD, art. 35 RGPD) y con las áreas competentes la Evaluación de Impacto en los Derechos Fundamentales (FRIA, art. 27 RIA) cuando proceda, sin sustituir el dictamen independiente del DPD.
- Cumplimiento normativo y regulatorio
- Promover y supervisar el cumplimiento del RIA, RGPD/LOPDGDD, ENS, ISO/IEC 42001 y normativa sectorial aplicable, coordinándose con el DPD, el Responsable de Seguridad ENS y la Asesoría Jurídica, preservando el dictamen independiente del DPD.

- Asegurar que la organización cumple las obligaciones de responsable del despliegue (art. 26 RIA): uso del sistema conforme a las instrucciones del proveedor, supervisión humana, monitorización, conservación de logs e información a las personas afectadas (art. 26.11 y art. 86 RIA).
- Coordinar la notificación de incidentes graves a la autoridad competente (art. 73 RIA) y la comunicación de brechas de datos personales al DPD conforme al RGPD.
- Verificar el registro de los sistemas que lo requieran en la base de datos de la UE (art. 49 RIA) cuando aplique.
- Analizar las propuestas de nuevos casos de uso de IA y emitir recomendación de autorización a la dirección, según el procedimiento de autorización de casos de uso del SGIA.
- Gestión de inquietudes.

- Transparencia, documentación y trazabilidad

- Asegurar que existe y se mantiene actualizada la documentación obligatoria de cada sistema (ficha de sistema, finalidad, datos, lógica general, evaluación de riesgos, controles aplicados, evidencias y decisiones de gobernanza).
- Garantizar la trazabilidad de las decisiones relevantes (autorización, modificaciones, retirada e incidentes).
- Velar por que los sistemas mantengan registros automáticos (logs) conforme al art. 12 del RIA, durante el plazo aplicable, y promover su revisión periódica.
- Facilitar evidencias a auditorías internas, externas, autoridades de control, AEPD y autoridades de vigilancia del mercado del RIA.

- Supervisión humana e impacto en personas

- Garantizar que cada sistema de IA dispone de mecanismos efectivos y proporcionados de supervisión humana (art. 14 RIA).
- Asegurar que se informa a las personas afectadas cuando interactúan con un sistema de IA o cuando se les aplica una decisión basada en IA (art. 26.11, art. 50 y art. 86 RIA), coordinándose con el DPD para los requisitos derivados del RGPD (art. 13, 14 y 22).

- Supervisión de proveedores y terceros

- Participar en la evaluación, selección y revisión periódica de los proveedores de soluciones de IA.
- Verificar que los contratos y acuerdos con terceros incluyen cláusulas sobre uso responsable, transparencia, seguridad, propiedad intelectual, datos de entrenamiento, subcontratación, derechos de auditoría, notificación de incidentes y obligaciones derivadas del RIA (cooperación del proveedor conforme a los art. 25 y 26).
- Supervisar los sistemas de IA de terceros integrados y los cambios de servicio relevantes.

- Formación y alfabetización en IA (art. 4 RIA)

- Definir y mantener el plan de alfabetización en IA para todo el personal, ajustado al rol y al nivel de exposición de cada colectivo.
- Promover la sensibilización sobre prácticas prohibidas, límites de los sistemas, sesgos y buenas prácticas de uso.

- Mejora continua, supervisión y reporte
- Supervisar el desempeño del SGIA y la eficacia de los controles, promoviendo la mejora continua.
- Elaborar informes periódicos a la dirección sobre estado del SGIA, riesgos emergentes, incidentes, métricas e indicadores.
- Escalar riesgos críticos a la alta dirección y proponer, en su caso, la suspensión o retirada de sistemas.

7 CLASIFICACIÓN DE LA IA

Con carácter previo a su despliegue y puesta en uso, todo sistema de inteligencia artificial deberá ser evaluado y clasificado en función de su nivel de riesgo, conforme a los criterios establecidos por la organización. A tal efecto, se establecen las siguientes categorías:

- Sistemas prohibidos
- Sistemas de alto riesgo.
- Sistemas de riesgo limitado
- Sistemas de riesgo mínimo

La clasificación deberá quedar debidamente documentada y formar parte del proceso de gobierno, gestión y control del sistema de inteligencia artificial.

8 EXCEPCIONES

Cualquier desviación o excepción a esta política debe ser autorizada por la Alta Dirección o el Comité de Seguridad, tras evaluar justificadamente la necesidad y establecer controles compensatorios.

9 CUMPLIMIENTO

Esta Política tendrá vigencia desde la aprobación por el Comité de Seguridad y mientras no se apruebe una posterior, se mantendrá vigente. La Política será puesta en conocimiento de todos los afectados –internos y externos-.

La Política será alineada con las directrices de las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al Responsable del Sistema.

10 APROBACIÓN, SEGUIMIENTO Y REVISIÓN

La Dirección, asume el compromiso de proveer todos los recursos y medios para la correcta implementación de la presente Política.

La Dirección demostrará su compromiso, mediante la revisión y aprobación de las políticas y otras normas que desarrollan el sistema, revisando los riesgos y los planes de tratamiento, considerando el informe de evaluación de impacto o el FRIA, participando en el Comité de Seguridad, promoviendo la cultura de seguridad, promoviendo la seguridad y especialmente, dotando de asignación efectiva a esta política mediante recursos y medios.

La Política tendrá vigencia desde la aprobación mientras no se apruebe una posterior, se mantendrá vigente. La Política será puesta en conocimiento de todos los afectados –*internos y externos*-a través del repositorio corporativo.