Creado por:	Responsable de Seguridad
Aprobado por:	Dirección y Responsable de Seguridad
Nivel de confidencialidad:	Uso interno

Fecha	**Elaborado**	**Revisado**	**Aprobado**
Nombre:	FERNANDO MARTINEZ	RAMON MARIN	RAFAEL BARRENA
Cargo:	Responsable de Seguridad	Responsable de Sistemas	Dirección
Fecha:	26/01/2026	30/01/2026	30/01/2026
Firma:			

Historial de modificaciones

Fecha	**Versión**	**Creado por**	**Descripción de la modificación**
26/01/2026	01	Responsable de Seguridad	Creación del documento
30/01/2026	02	Dirección	Completar el doc

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 30 de enero de 2026 por la Dirección y Responsable de Seguridad de **CEDYC S. COOP.** (en adelante, **CEDYC**). Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

La Dirección y el Responsable de Seguridad de **CEDYC**, aprueba la siguiente Política de Seguridad de la Información del Esquema Nacional de Seguridad (en adelante, ENS) y norma ISO 27001:2022.

El objetivo de esta Política es definir y establecer los principios, criterios y objetivos de mejora que rigen las actuaciones en materia de seguridad de la información de los sistemas que se encuentran sujetos al ENS y norma ISO 27001:2022. Así como establecer las directrices y principios que regirán el modo en que **CEDYC** gestionará y protegerá su información y sus servicios, cumpliendo con los objetivos y directrices de la Política de Seguridad de la Información corporativa, a través de la implantación, mantenimiento y mejora de un SGSI y aplicando los requisitos y medidas de seguridad dentro del marco regulatorio del Esquema Nacional de Seguridad (ENS) y norma ISO 27001:2022.

2. INTRODUCCIÓN, OBJETO Y ALCANCE

CEDYC es una empresa que apuesta desde sus inicios por un servicio integral a sus clientes, teniendo como objetivo primordial conseguir su plena satisfacción ofreciendo un servicio de calidad y en constante mejora. El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con rapidez a las incidencias.

Tomando en cuenta el contexto en el cual se determinan las cuestiones internas y externas de la organización, las partes interesadas que son relevantes y sus requisitos para la seguridad de la información, así como las interfaces y dependencias entre las actividades realizadas por la entidad y las que se llevan a cabo por otras organizaciones en el cumplimiento. Esta Política se circunscribe a los servicios y sistemas incluidos en el alcance del ENS que dan cobertura al cumplimiento de los requisitos y medidas de seguridad establecidas en el Esquema Nacional de Seguridad y norma ISO 27001:2022 en lo relativo a:

- Integración de soluciones de Ciberseguridad.
- Mejora de diseño de redes digitales.
- Detección de respuestas de *Endpoint* (EDR).
- Servicio de monitorización de sistemas (SIEM).
- Servicios antispam.
- Análisis forense y respuesta anti incidentes (DFIR).
- Bastionado y fortalecimiento de sistemas.
- Realización y gestión de copias de seguridad.
- Consultoría legal y cumplimiento normativo.
- Formación y concienciación en seguridad.
- Auditorías técnicas.
- Detección y prevención de intrusos.
- Gestión integral de vulnerabilidades.
- Ciberseguridad industrial IoT.
- Apoyo a la Gestión de la Seguridad.
- Gestión de riegos.

El alcance del SGSI cubre todos los sistemas de información, activos, procesos, servicios y personal implicados en la provisión de los servicios definidos, así como sus interfaces con terceros. El alcance se documenta y revisa de forma periódica conforme al procedimiento de gestión del alcance del SGSI.

3. OBJETIVOS Y MISIÓN DE LA ORGANIZACIÓN

En el área de TECNOLOGIA – CONSULTORIA INFORMATICA, nuestra misión es proporcionar soluciones tecnológicas innovadoras y seguras que ayuden a proteger la información sensible de las empresas y a maximizar la eficiencia en sus operaciones informáticas. Con un enfoque en la excelencia y la seguridad, nos comprometemos a ofrecer a nuestros clientes las herramientas y los conocimientos necesarios para enfrentar los desafíos del mundo digital con confianza y éxito.

En el área de CONSULTORIA EMPRESARIAL Y NUEVOS NEGOCIOS, nuestra misión es cumplir con el cliente, con la normativa en materia contable, fiscal y laboral y hacerlo con una atención especializada y personalizada.

Cedyc sostiene un compromiso inquebrantable con la excelencia en el servicio y la total satisfacción del cliente. Este compromiso impulsa nuestra constante búsqueda de mejoras y nuestra dedicación a la innovación en todos los aspectos de nuestros procesos. Nos esforzamos por establecer estándares de calidad excepcionales y por superar continuamente nuestras propias expectativas. Nuestro enfoque en la mejora continua y la innovación nos permite adaptarnos a las necesidades cambiantes del mercado y proporcionar soluciones que realmente agreguen valor a nuestros clientes.

Mediante esta Política, **CEDYC** asume y promueve los siguientes principios generales que deben guiar todas sus actividades:

- Garantizar el cumplimiento con los objetivos y principios generales detallados en la Política de Seguridad de la Información aprobada y promovida por la Dirección de la empresa.

- Asegurar el establecimiento y cumplimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de la empresa.

- Asegurar la integración y el cumplimiento de los requisitos aplicables del ENS y de la Norma ISO 27001:2022 en los servicios y procesos de la sociedad.

- Asegurar que los recursos necesarios para el ENS estén disponibles.

- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del ENS y de la Norma ISO 27001:2022.
- Asegurar que el ENS consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del ENS.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, así como la protección de los datos personales.
- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Asimismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta lo que se va a hacer, los recursos necesarios, el responsable y el plazo de consecución.

4. MARCO LEGAL Y REGULATORIO

El marco normativo que afecta al desarrollo de las actividades y competencias de **CEDYC** está constituido por normas jurídicas estatales orientadas a la administración electrónica, a la seguridad de la información y los servicios que la manejan, así como a la protección de datos de naturaleza personal.

Las normas que constituyen dicho marco se encuentran recogidas en un registro al efecto, "SGSI- Legislación aplicable" el cual se mantiene actualizado según señala el correspondiente procedimiento de requisitos legales.

5. ORGANIZACIÓN DE LA SEGURIDAD

La Dirección de **CEDYC** tiene como responsabilidad fundamental la de liderar y comprometerse con respecto al ENS.

CEDYC cuenta con un Comité de Seguridad de la Información que dispone de las siguientes funciones:

- Asegurarse de que se establecen, implementan y mantienen los procesos necesarios para el SGSI y el cumplimiento del ENS.
- Asegurarse de que se promueva la toma de conciencia de los requisitos del cliente y resto de Partes Interesadas en todos los niveles de la organización.

El Comité de Seguridad de la Información (CSI), estará compuesto por:

- Dirección, representada por el Director.
- Responsable del sistema.
- Responsable de la seguridad del sistema.
- Responsable del servicio y de la información.
- Administrador de Seguridad del Sistema.

Funciones y responsabilidades de seguridad

- El/la Responsable de la Información, determina los requisitos de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, con el asesoramiento del Responsable de Seguridad. Tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección.

- La persona Responsable del Servicio, determina los requisitos de seguridad de los servicios prestados dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, con el asesoramiento del Responsable de Seguridad y la opinión del Responsable del Sistema.

- El/la Responsable de Seguridad, su función es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho.

- El/la Responsable del Sistema de Información, es el encargado de las operaciones del sistema.

Designación de funciones.

La Dirección asegura, con la colaboración del RSGSI, que el personal dispone de la necesaria formación teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones.

Las funciones y responsabilidades inherentes a cada puesto de trabajo dentro del SGSI, así como los requisitos de formación y experiencia necesarios, están recogidas en los perfiles de puesto de trabajo y en el Manual de Organización, debiendo ser aprobadas las modificaciones por la dirección en el CSI.

Procedimientos de designación

CEDYC procederá a realizar la constitución del comité y de las distintas responsabilidades. Todos los nombramientos se revisarán cada 3 años o cuando los puestos queden vacantes.

La coordinación se lleva a cabo en el seno de la Dirección que podrá delegar sus funciones en el Comité de Seguridad de la Información.

Los nombramientos correrán a cargo de la Dirección.

6. GESTIÓN DE RIESGOS

Las actividades objeto de esta política de seguridad incluidas en el ámbito del ENS y de la ISO 27001:2022 tiene su correspondiente gestión de riesgos.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se realice cualquier cambio significativo del sistema o del SGSI.

Para la armonización del análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones a realizar.

CEDYC dispone de una metodología documentada para la realización del análisis de riesgos recogida en el documento “PR-IT-011 Metodología de análisis de riesgos”.

7. ESTABLECIMIENTO, IMPLANTACIÓN, MANTENIMIENTO Y MEJORA DEL SGSI Y DIRECTRICES PARA LA GESTIÓN DE LA DOCUMENTACIÓN

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada que deberá ser revisada y aprobada por la dirección.

Las medidas de seguridad establecidas se alinean con los controles del Anexo II del ENS para nivel Medio y con los controles del Anexo A de la norma ISO/IEC 27001:2022, conforme a la Declaración de Aplicabilidad (SoA) vigente.

En cumplimiento del artículo 12 del Real Decreto del ENS, la presente Política de Seguridad se desarrollará aplicando los siguientes requisitos mínimos que se encuentran incluidos en la documentación del sistema:

- **Organización e implantación del proceso de seguridad**. Considerando las directrices desarrolladas en la Política del Sistema de Gestión, se desarrollará un conjunto de procedimientos operativos que garanticen la implantación de directrices y la consecución de los objetivos de la organización en materia de seguridad de la información.

- **Análisis y gestión de los riesgos**. El proceso de análisis y gestión de los riesgos, recogido en el documento relativo a la metodología de análisis de riesgos (véase PR-IT-011 Metodología de Análisis de Riesgos), se realizará de acuerdo con las siguientes actividades:

    - Identificación de activos.
    - Análisis y valoración.
    - Cálculo del riesgo.
    - Determinación del riesgo aceptable.

- **Gestión de personal**. La Dirección se asegurará que el personal dispone de la formación necesaria teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones. Para lograr los objetivos de seguridad de la información todo el personal debe estar involucrado en el tratamiento y saber de qué forma se puede contribuir a su consecución. Estas medidas se encuentran desarrolladas en el procedimiento de seguridad relativa a los recursos humanos.

- **Profesionalidad**. La Dirección deberá garantizar que el personal dispone del conocimiento y habilidades necesarios para el adecuado desempeño de sus funciones. Además, deberá proporcionarla formación necesaria cuando se detecten carencias en el cumplimiento de las actividades.

- **Autorización y control de los accesos**. Los sistemas de información deberán disponer de un mecanismo de control de accesos que limite su acceso a los usuarios y dispositivos que estén debidamente autorizados, restringiendo el acceso a las funciones que le son permitidas. Las medidas de seguridad aplicadas se encuentran descritas en el procedimiento de control de acceso.

- **Protección de las instalaciones**. La organización deberá disponer de un conjunto de controles de acceso físico a las instalaciones, que permita limitar el acceso únicamente a las personas autorizadas a las zonas de almacenamiento y/o procesamiento de información confidencial. Las medidas de protección se encuentran descritas en el procedimiento de seguridad física y del entorno.

- **Adquisición de productos**. La adquisición de productos deberá considerar y garantizar el cumplimiento con los requisitos de seguridad establecidos por la Dirección, tal y como se detalla en el procedimiento de adquisición, desarrollo y mantenimiento.

- **Seguridad por defecto**. Los sistemas deberán configurarse según las políticas y procedimientos de seguridad definidos. El procedimiento de seguridad de las operaciones desarrolla las medidas de seguridad que se deben aplicar a los sistemas de información.

- **Integridad y actualización del sistema**. Se deberán aplicar medidas que permitan conocer el estado de seguridad de los sistemas, y que permitan identificar y gestionar los riesgos de seguridad de estos. Estas medidas se encuentran desarrolladas en el procedimiento de seguridad de las operaciones.

- **Protección de la información almacenada y en tránsito**. Se deberán aplicar medidas de seguridad que permitan garantizar un adecuado nivel de protección de la información almacenada y en tránsito. Estas medidas se encuentran detalladas en el procedimiento de gestión de activos.

- **Prevención ante otros sistemas de información interconectados**. Se deberán analizar y gestionar los riesgos derivados de las conexiones de los sistemas de información con redes públicas, y aplicar las medidas necesarias de protección según el nivel de seguridad requerido por el sistema.

- **Registro de actividad**. Los sistemas de información deberán contar con registros de actividad de los usuarios que permitan custodiar la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas. Estas medidas se encuentran detalladas en el procedimiento de seguridad de las operaciones.

- **Incidentes de seguridad**. Los sistemas de información deberán contar con un sistema de detección y reacción frente a código dañino. Además, existirá un registro de incidentes

de seguridad que permitirá realizar un seguimiento de la resolución de estos y aplicar mejoras a través de las lecciones aprendidas. Estas medidas se encuentran detalladas en el procedimiento de Gestión de Incidentes de Seguridad.

- **Continuidad de la actividad**. Se deberán establecer, en la medida de lo posible y según el nivel de riesgo asociado, los mecanismos necesarios para garantizar la recuperación de la información y la continuidad de las operaciones.

- **Mejora continua del proceso de seguridad**. La Dirección deberá llevar a cabo una revisión periódica del sistema para asegurarse de su conveniencia, adecuación y eficacia continua. Ante la ocurrencia de cualquier desviación respecto a los resultados esperados, se deberá iniciar el proceso de tratamiento de la misma mediante los procesos establecidos.

Esta Política se desarrollará por medio de normativa y procedimientos de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización dentro del alcance que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo), que tendrá la obligación de aplicarla en la realización de sus actividades

La información documentada será clasificada en: información de uso público, información de uso interno e información confidencial, dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en la Política de Gestión de Activos (véase documento “Gestión de Activos y Clasificación de la Información”).

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo con los requisitos generales del Sistema Integrado de Gestión que se recogen en el documento “**CEDYC** -Manual del Sistema de Gestión”.

Toda la información documentada relativa al Sistema Integrado de Gestión se aloja en los Sistemas de Información de **CEDYC**.

Esta Política de Seguridad del ENS será aprobada por la Dirección y revisada junto a la Política de los Sistemas de Gestión de forma periódica o cuando circunstancias técnicas u organizativas lo requieran para evitar que quede obsoleta.

8. OBLIGACIONES DEL PERSONAL

Todos los miembros de **CEDYC** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **CEDYC** atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **CEDYC**, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

9. TERCERAS PARTES

Cuando **CEDYC** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **CEDYC** utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que

resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.

Esta política será objeto de revisión al menos una vez al año por la Dirección, como parte del proceso de revisión del SGSI, o siempre que se produzcan cambios significativos en el entorno tecnológico, organizativo o normativo.