ASIREC S.L.	**ESQUEMA NACIONAL DE SEGURIDAD**
DOCUMENTO	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**
FECHA APROBACIÓN	**15 DE ENERO DE 2018**
FECHA REVISIÓN	**17 DE FEBRERO DE 2026**
Versión	**3**

asirec®

SERVICIOS DE GESTIÓN
DE TRIBUTOS Y TRABAJOS
CATASTRALES

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ASIREC S.L.	**ESQUEMA NACIONAL DE SEGURIDAD**
DOCUMENTO	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**
FECHA APROBACIÓN	**15 DE ENERO DE 2018**
FECHA REVISIÓN	**17 DE FEBRERO DE 2026**
Versión	**3**

1. APROBACIÓN Y ENTRADA EN VIGOR

La primera versión de esta política fue aprobada el día 18 de enero de 2018 y revisada el 6 de septiembre de 2019 por la Junta General de Socios de ASIREC SL. de acuerdo con la anterior legislación.

Esta política fue revisada por el Comité de Seguridad el 17 de febrero de 2026 con motivo de la implantación de la ISO 27001.

2. INTRODUCCIÓN

ASIREC S.L. depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.
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 presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos

en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

3. PRINCIPIOS Y DIRECTRICES

3.1. PREVENCIÓN

ASIREC debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad.

Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, ASIREC debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

3.3. RESPUESTA

ASIREC debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

3.4. CONSERVACIÓN

A fin de garantizar la conservación de los datos ASIREC establecerá procedimientos seguros de copias de seguridad de la información en soporte electrónico.

Para garantizar la disponibilidad de los servicios críticos, ASIREC debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

4. ALCANCE

Esta Política se aplica a todos los sistemas TIC de ASIREC S.L. y a todos los miembros de la organización, sin excepciones. También se aplica sobre personal en prácticas y personal externo que puedan participar en los procesos de negocio de manera directa o indirecta.

La Política de Seguridad es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

1.Primer nivel: *Política de Seguridad de la Información.*

Constituye el primer nivel la Política de Seguridad de la Información, recogida en el presente texto.

2.Segundo nivel: *Normativa de Seguridad de la Información.*

El segundo nivel desarrolla la Política de Seguridad de la Información mediante instrucciones específicas que abarcan un área o aspecto determinado de la seguridad de la información. Las Instrucciones se estructurarán en normativas y serán aprobadas por el Comité de Seguridad de la Información.

3.Tercer nivel: *Procedimientos de Seguridad de la Información.*

El tercer nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con

la seguridad de la información y la protección de la información y de los servicios.

Los procedimientos serán aprobados por el Responsable de Seguridad de la Información o por los Responsables de la Información o los de los Servicios, según su ámbito de competencia.

Esta estructura jerárquica permitirá a ASIREC adaptar con eficiencia sus entornos operativos y garantizar la Seguridad en sus procesos de negocio.

El personal de ASIREC tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Instrucciones y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones.

El responsable de seguridad enviará e-mail informativo a todos los trabajadores de Asirec cada vez que se produzca la aprobación o modificación de la documentación señalada en el párrafo anterior, indicando la modificación producida, así como el área/unidad a la que afecta.

La Política de Seguridad de la Información, la Normativa de Seguridad y todas las Instrucciones y Procedimientos de Seguridad de la Información se encuentran ubicados en la carpeta denominada “Calidad”, ubicada en el servidor, a la que todos los trabajadores tienen acceso, link:

\\Srvalhama\CALIDAD\Documentos ENS y LOPD

5. MISIÓN

ASIREC S.L. es una organización privada, especializada en la prestación de servicios a Administraciones Públicas. La organización desarrolla sus actividades de manera local sobre los Municipios de Alhama de Murcia y Totana.

ASIREC presta los siguientes servicios en el ámbito de Aplicación del Esquema Nacional de Seguridad:

UNIDAD	SERVICIO
INFORMACIÓN GENERAL	**Servicio Punto de Información**

GESTIÓN TRIBUTARIA	**Actualización de Datos**
	Gestión de Plusvalías
	Expedientes
	Informes y Certificados de Bienes
RECAUDACIÓN	**Cobros de Deudas**
	Consultas y Duplicados
	Aplazamientos y Fraccionamientos
	Informes de Deudas
TRÁFICO	**Gestión de Expedientes Sancionadores**
SUBSEDE ELECTRÓNICA	**Actualización de Datos Fiscales**
	Objetos Tributarios
	Recaudación
	Simuladores
	Estado de trámites y gestiones

De forma estrecha con cada municipio, ASIREC colabora en la mejora de los servicios municipales, en especial impulsando la Administración Electrónica.

6. MARCO NORMATIVO

A continuación, se detalla el marco normativo que debe cumplir la organización:

MARCO NORMATIVO	
ADMINISTRACIONES PÚBLICAS	▯ **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. ▯ **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público.

INTEROPERABILIDAD	▯ **Real Decreto 4/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
SEGURIDAD DE LA INFORMACIÓN	▯ **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	▯ **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos de Personales. ▯ **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 estos datos.

7. ORGANIZACIÓN DE LA SEGURIDAD

7.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

7.1.1. CONSTITUCIÓN

El **Comité de Seguridad de la Información**, en adelante el "Comité", asume los **roles de Responsable de la Información y Responsable del Servicio.**

El Comité presenta estructura orgánica y está formado por delegados de las partes interesadas en la óptima gestión de la Seguridad de la Información. La postura oficial del Comité ante cuestiones sometidas a votación será delimitada por mayoría simple.
Los integrantes del Comité de Seguridad de la Información se detallan en la siguiente tabla.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD	DELEGADO/A	FUNCIÓN	RESPONSABILIDAD
ADMINISTRACIÓN ELECTRÓNICA	Ricardo Martínez San Andrés	**Presidente**	
ÁREA JURÍDICA	Álvaro Leal Baños	**Secretario**	**Responsable de Seguridad**
ÁREA RECURSOS HUMANOS	Ana Belén Gómez Redondo	Vocal	**Delegada de Protección de Datos**
INFORMÁTICA	Daniel Cánovas Martinez	Vocal	**Responsable del Sistema**
SEDE ALHAMA DE MURCIA	Jesús Manuel Delgado Fernández	Vocal	
SEDE TOTANA	Juan Antonio Cano Izquierdo	Vocal	

El **Secretario del Comité y Responsable de Seguridad** es Alvaro Leal Baños y tiene como funciones del cargo:

- Convocar las reuniones del Comité.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el Acta de Reunión.
- Impulsar la ejecución directa o delegada de las decisiones del Comité.

El **Presidente del Comité** es Ricardo Martínez San Andrés y es responsable de presidir las reuniones. Así mismo, será responsable de revisar las Actas de Reunión y aprobarlas formalmente con su firma.

7.1.2. FUNCIONES Y RESPONSABILIDADES

El **Comité de Seguridad de la Información** reportará a la Junta General de Socios sus propuestas y decisiones en aquellas áreas que le competen. El Comité tendrá las siguientes funciones:

- Atender las inquietudes de los socios y de los diferentes departamentos de la empresa.

- Informar regularmente del estado de la seguridad de la información a los socios de la empresa.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar anualmente) la Política de Seguridad de la Información.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Comunicar los incidentes de seguridad a través de los canales gubernamentales establecidos al efecto.

7.2. ROLES

7.2.1. ESTRUCTURA

En ASIREC los roles del Esquema Nacional de Seguridad se asignan de la siguiente forma:

FIGURA RESPONSABLE	ROL	FUNCIONES Y RESPONSABILIDADES
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Responsable de la información	Tratamiento / Protección de la información
	Responsable del servicio	Definir requisitos de seguridad de los servicios prestados
RESPONSABLE DE SEGURIDAD	Responsable de la Seguridad	Responsable del Cumplimiento ENS
RESPONSABLE DEL SISTEMA	Responsable del sistema	Mantenimiento y continuidad de los Sistemas
	Administrador de la Seguridad	Monitorización y configuración de medidas de Seguridad

Los roles nominativos del Esquema Nacional de Seguridad son ejercidos por los siguientes trabajadores:

FIGURA RESPONSABLE	NOMBRAMIENTO	CONTACTO
Responsable de Seguridad	Álvaro Leal Baños	alvaro.leal@asirec.es
Responsable del Sistema	Daniel Cánovas Martinez	informatica@asirec.es

Relativo al Cumplimiento de la normativa en Protección de Datos, se realiza la designación de la figura de Delegado de Protección de Datos que colaborará activamente en el Comité de Seguridad de la Información.

FIGURA RESPONSABLE	NOMBRAMIENTO	CONTACTO
Delegada de Protección de Datos	Ana Belén Gómez Redondo	ana.gomez@asirec.es

7.2.2. FUNCIONES Y RESPONSABILIDADES

La figura de **Responsable de Seguridad** tiene como principales funciones y responsabilidades:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
- Realizar o promover auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación de la Unidad de Informática dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados y supervisará su implantación.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el propietario del sistema, incluyendo los incidentes más relevantes del periodo.
- Aprobación de los procedimientos de seguridad elaborados por el Administrador del Sistema.
- Elaboración de la normativa de seguridad de la entidad.

Por su parte, el **Responsable del Sistema** tendrá como principales funciones y responsabilidades:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y los procedimientos de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Detener el 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. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de Seguridad, antes de ser ejecutada.
- Elaboración de los procedimientos de seguridad necesarios para la operativa en el sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.

Las funciones y responsabilidades listadas en este apartado podrán ser delegadas tal como estipula la Guía de Adecuación 801 sobre Responsabilidades y Funciones en el Esquema Nacional de Seguridad.

7.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad será aprobado por el Comité de Seguridad de la Información. El nombramiento se revisará anualmente o cuando el puesto quede vacante.

Cada Unidad propondrá cada dos años a su delegado/a en el Comité de Seguridad de la Información, que será elegido por consenso entre los miembros de la Unidad. Los representantes nombrarán al Presidente del Comité, mientras que la figura de Secretario corresponderá a la persona Responsable de la Seguridad del Esquema Nacional de Seguridad.

7.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad de la Información la revisión **anual** de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Junta General de Socios y difundida para que la conozcan todas las partes afectadas.

La difusión se practicará vía e-mail, por el Responsable de Seguridad, a todos los trabajadores de la empresa, indicando la ubicación del texto definitivo de la Política en el servidor, link: \\Srvalhama\CALIDAD\Documentos ENS y LOPD

8. DATOS DE CARÁCTER PERSONAL

ASIREC S.L. trata datos de carácter personal. El documento "**Registro de Actividades de Tratamiento**" al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados, los responsables correspondientes y las actividades de tratamiento realizadas.

Todos los sistemas de información de ASIREC S.L. se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado "Registro de Actividades de Tratamiento".

9. ANÁLISIS Y 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

Para la armonización de los 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 de carácter horizontal.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de ASIREC S.L. aplicadas en materia de Protección de Datos de Carácter Personal.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará 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.

La normativa de seguridad estará disponible en la intranet en la carpeta compartida ubicada en el Servidor denominada “Calidad”, teniendo todos los equipos un acceso directo a esta carpeta desde su escritorio.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros de ASIREC S.L. 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 disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de ASIREC S.L. atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año, preferiblemente en los meses de verano por existir menor carga de trabajo (julio y septiembre). Se establecerá un programa de concienciación continua para atender a todos los miembros, 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.

El personal que atienda la seguridad del sistema deberá estar cualificado e instruido en todas las fases de su ciclo de vida. Se determinarán los requisitos de formación y experiencia necesarios para cubrir estos puestos de trabajo.

12. TERCERAS PARTES

Cuando ASIREC S.L. 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 de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando ASIREC S.L. 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.

Cuando algún aspecto de la Política 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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Este documento ha sido aprobado por la dirección.