Política de seguridad

Información general

Control documental

Clasificación	Público
Versión	3
Fecha creación	29/04/2016
Fecha última actualización	28/04/2026
Fichero	Política de seguridad

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Oficina de Seguridad	Responsable de Seguridad	Comité de Seguridad

Control de versiones

Versión	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Creación del documento	Oficina de seguridad	29/04/2016
1.1	Revisión	Oficina de seguridad	10/03/2017
2.0	Revisión de los roles y sus nombramientos	Oficina de seguridad	02/06/2017
2.1	Revisión de roles y separación de nombramientos a documento Anexo.	Oficina de seguridad	08/06/2017
2.2	Se añade el rol del Oficial de revocación. Se sustituye la referencia a AULOCE por ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.	Oficina de seguridad	02/10/2020
2.3	Se incluye rol de Operador de registro	Oficina de seguridad	14/04/2023
2.4	Se revisa el detalle de las funciones del Responsable de	Oficina de seguridad	11/03/2025

	seguridad (ETSI EN 319 401 (v3.1.1))		
2.5	Se revisa y aclara la redacción de las funciones del rol de Auditor	Oficina de seguridad	28/03/2025
3	Adaptación a la nueva versión de la ETSI EN 319 401, actualización de formato e inclusión de rol de Responsable de desarrollo	Oficina de seguridad	28/04/2026

Índice

1. Introducción

ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. con CIF A-50.878.842 y con domicilio en Calle Bari 39, C.P. 50.197 (Zaragoza), inscrita en el Registro Mercantil de Zaragoza al tomo 2.649, Folio 215, hoja Z-28722, opera bajo el nombre comercial "**esFirma**" como prestador de servicios de certificación.

esFIRMA actúa de acuerdo con la normativa nacional y europea que le resulta de aplicación, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios. Entre otras:

- Reglamento (UE) nº 910/2014 sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interno (Reglamento eIDAS).
- Normas técnicas del ETSI aplicables a la expedición y gestión de certificados cualificados, principalmente ETSI EN 319 411-1 y ETSI EN 319 411-2.
- Normativa nacional en materia de firma electrónica.

esFIRMA ha impulsado la elaboración de una política de seguridad que sirva como guía para la protección de los sistemas de información y de las redes que dan soporte a la prestación de sus servicios de certificación. Esta política es apropiada y complementaria a la estrategia y los objetivos comerciales de esFirma, integrando la seguridad como un elemento fundamental para la continuidad y el desarrollo del servicio.

La dirección de esFirma se compromete a proporcionar los recursos necesarios para la implementación efectiva de esta política, asegurando la disponibilidad de capital humano especializado, dotación financiera suficiente, así como los procesos, las soluciones tecnológicas y la infraestructura requeridas.

2. Alcance

Esta política de seguridad abarca todos los servicios de certificación prestados por esFIRMA y es de obligado cumplimiento para todo el personal esFirma, así como para terceras partes que presten o utilicen servicios y cedan o manejen información cuyo responsable sea esFirma (en adelante, referidos conjuntamente como el "**personal**").

3. Principios

Esta política se desarrollará, con carácter general, de acuerdo con los siguientes principios:

- **Principio de confidencialidad.** Los activos TIC deberán ser accesibles sólo por aquellas personas o procesos autorizados.

- **Principio de integridad y calidad.** Se deberá garantizar el mantenimiento de la integridad de la información, así como de los procesos de tratamiento de la misma.

- **Principio de disponibilidad y continuidad.** Se garantizará un nivel alto de disponibilidad de los activos TIC y se dotarán de los planes y medidas necesarios para asegurar la continuidad de los servicios.

- **Principio de trazabilidad.** Se implantarán medidas para asegurar que en todo momento se puede determinar quién y cuándo se desencadenó una acción con el fin de tener capacidades de análisis sobre incidentes de seguridad que se detecten.

- **Principio de autenticidad.** Se deberán articular medidas para garantizar la fuente de información de la que proceden los datos y que las entidades donde se originan los datos son confiables.

- **Principio de gestión del riesgo.** Se analizarán los riesgos y se establecerán las medidas de seguridad necesarias para minimizarlos.

- **Principio de proporcionalidad en coste.** Se buscará que las medidas de seguridad adoptadas para mitigar los riesgos se implanten bajo una perspectiva de proporcionalidad en los costes que supongan.

- **Principio de concienciación y formación.** Todas las personas encargadas de la gestión de los sistemas de información serán formadas con el objeto de que puedan conocer sus obligaciones respecto al tratamiento seguro de la información que manejan.

- **Principio de prevención.** Se llevarán a cabo iniciativas para la prevención de incidentes de ciberseguridad.

- **Principio de mejora continua.** esFirma mantendrá un compromiso explícito con la mejora continua de la seguridad de sus redes y sistemas de información, revisando periódicamente sus controles y adaptándolos a las nuevas amenazas.

- **Principio de seguridad TIC en el ciclo de vida de los sistemas de información**: En todas las fases del ciclo de vida de los activos se aplicarán las especificaciones de seguridad y procedimientos de control correspondientes.

- **Principio de seguridad desde el diseño y por defecto**: esFIRMA establecerá y aplicará reglas de desarrollo seguro de redes y sistemas de información que abarquen todas las fases: especificación, diseño, desarrollo, implementación y pruebas.

- **Principio de función diferenciada.** La responsabilidad sobre la seguridad de los sistemas de información estará separada de la responsabilidad sobre el servicio.

4. Objetivos de seguridad

esFirma establece los siguientes objetivos estratégicos en materia de seguridad de redes y sistemas de información:

- **Salvaguarda de activos.** Proteger la confidencialidad de la información de los usuarios y garantizar la integridad absoluta de los procesos de emisión, gestión y revocación de certificados.

- **Resiliencia operativa.** Implementar mecanismos de detección y respuesta proactivos, asegurando la continuidad de negocio mediante planes de recuperación que garanticen la resiliencia de los servicios de confianza ante contingencias.

- **Cumplimiento normativo.** Asegurar el cumplimiento íntegro y continuado del marco legal aplicable a esFIRMA.

- **Generación de confianza:** Fortalecer la reputación de esFIRMA ante sus grupos de interés mediante una gestión transparente de la seguridad y el mantenimiento de altos niveles de disponibilidad del servicio.

5. Organización de la seguridad

La organización de esFirma se articula según los roles descritos a continuación. Las funciones, responsabilidades y roles asignados se revisarán anualmente y cuando ocurran incidentes significativos o cambios en las operaciones o riesgos.

5.1. Comité de Seguridad

El Comité de Seguridad estará formado por tres miembros: su Presidente, el Responsable de Información y servicio y el Responsable de Seguridad. Corresponde al Comité de Seguridad:

a) Aprobación del nivel de apetito al riesgo y del umbral de tolerancia al riesgo.
b) Aprobación del análisis de riesgos y, en su caso, del plan de tratamiento de riesgos.
c) Aprobación de nuevos documentos o modificaciones relevantes del marco normativo de seguridad y documentación relevante de la autoridad de certificación (plan de cese, plan de continuidad, declaración de prácticas de certificación, política de seguridad ...).

5.2. Oficina de seguridad

La Oficina de Seguridad se corresponde con el departamento de Cumplimiento Normativo y está formada por el Responsable de Seguridad y el personal que se considere necesario en cada momento para el desarrollo de sus funciones.

Entre sus funciones cabe destacar:

a) Realización de la evaluación anual de riesgos y, en su caso, del plan de tratamiento de riesgos, que deberá ser aprobado por el Comité de Seguridad.
b) Elaboración de propuestas relativas a la revisión del marco normativo de seguridad y documentación relevante de la autoridad de certificación (plan de cese, plan de continuidad, declaración de prácticas de certificación, política de seguridad ...), que deberá ser aprobado por el Comité de Seguridad.

c) Modificaciones de carácter menor sobre normativas, procedimientos, instrucciones y demás elementos dentro de la estructura normativa de seguridad.
d) Formación al personal en materia de seguridad de la información.
e) Reporte de información al Comité de Seguridad, a través del Responsable de Seguridad, sobre asuntos relacionados con la seguridad de las redes y los sistemas de información.

Para el desarrollo de sus funciones, la Oficina de Seguridad se apoya en el Centro de Operaciones de Seguridad (SOC) como unidad responsable de la vigilancia activa y el mantenimiento del entorno de seguridad de esFirma (monitorización continua, detección temprana y análisis de amenazas, respuesta ante incidentes, etc.).

5.3. Roles de confianza

Las personas que desempeñan cada uno de los roles se encuentran definidas en el documento ANEXO. ESFIRMA – DEFINICIÓN DE ROLES DE CONFIANZA.

5.3.1. Roles y funciones en el ámbito de la CA

- **Administrador de Sistemas**. Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación.

- **Administrador de CA**. Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.

- **Auditor**. Autorizado a ver los archivos y auditorías de log con el propósito de auditar las operaciones del sistema conforme a las políticas de seguridad establecidas. Las tareas de Auditor son incompatibles con la operación y administración de los sistemas.

- **Operador de CA**. Responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.

- **Responsable de Seguridad**. Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de esFIRMA. Responsable de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc, así como de reportar a la alta dirección a través del Comité de Seguridad.

- **Responsable de información y servicio**. Define los requisitos de la información y de los servicios en materia de seguridad. Este rol tiene la responsabilidad última del uso que se haga de la información y los servicios y por tanto de su nivel de protección.

- **Especialista en validación**. Responsable de la validación de las solicitudes de certificados.

- **Oficial de revocación**. Responsable de la operación de cambio de estado de los certificados.

- **Operador de registro**. Responsable de la aprobación de las peticiones de certificación por el suscriptor.

- **Responsable de desarrollo.** Asume las funciones de implementación y control del ciclo de vida de desarrollo de los sistemas de software y firmware de PKI.

5.3.2. Roles y funciones en el ámbito del sistema de firma remota (firma con pin)

- **Responsable de seguridad**. Responsabilidad global de administración e implementación de las prácticas y políticas de seguridad.

- **Administrador del sistema L1**. Autorizados con quorum mínimo (3/5) a inicializar y actualizar SSCDs. Los SSCD son inmutables una vez inicializados. Son los poseedores de un share de la clave de activación del sistema

- **Administrador del sistema L2**. Autorizado a configurar y mantener el sistema de firma con PIN con acceso controlado a la información de seguridad. Pueden ajustar la

fuente de tiempo. Pueden crear credenciales de acceso para el SSA. Realizar copias de seguridad de esas credenciales.

- **Operador del sistema**. Responsable de la operativa diaria del sistema. No pueden en ningún caso administrar o configurar el sistema.

- **Auditor**. Autorizado a ver los archivos y auditorías de log con el propósito de auditar las operaciones del sistema conforme a las políticas de seguridad establecidas. Las tareas de Auditor son incompatibles con la operación y administración de los sistemas.

- **Responsable de desarrollo.** Asume las funciones de implementación y control del ciclo de vida de desarrollo del sistema de firma remota.

6. Estructura normativa de seguridad

La política de seguridad genera una estructura normativa de seguridad compuesta por la propia política, normativas de seguridad y procedimientos, con niveles relacionados jerárquicamente, tal y como se describe a continuación:

6.1.1. Primer nivel: Política de seguridad de la información.

La política de seguridad es aprobada por el Comité de seguridad. La política de seguridad se comunica y se pone a disposición del personal de esFirma y de terceras partes interesadas mediante un enlace permanente en la página web de esFIRMA.

6.1.2. Segundo nivel: Normas de seguridad de la Información

Las normas de seguridad surgen como desarrollo de la política en un área determinada de la seguridad de la información. Entre otras, cabe destacar:

- ✓ Normativa de uso de recursos y acceso a los sistemas de información
- ✓ Normativa de trabajo fuera de las instalaciones
- ✓ Normativa de clasificación de la información
- ✓ Normativa de uso de Servicios Cloud
- ✓ Normativa de uso de correo electrónico
- ✓ Normativa de gestión de soportes
- ✓ Normativa de gestión de ciberincidentes
- ✓ Normativa de borrado seguro de datos
- ✓ Política de configuración de contraseñas

Las normativas de seguridad se comunican al personal de esFirma y están disponibles para consulta de manera permanente en la Intranet de la compañía.

6.1.3. Tercer nivel: Procedimientos de seguridad de la información.

Los procedimientos indican el flujo de las actividades relacionadas con los servicios o activos de información que realiza esFirma.

6.1.4. Cuarto nivel: Instrucciones Técnicas

Las instrucciones técnicas son los comandos que especifican cómo hacer lo estipulado en los procedimientos.

7. Desarrollo seguro de redes y sistemas

Antes de cualquier despliegue de software, red o sistema de información, esFIRMA aplicará las siguientes directrices de seguridad:

- Análisis de requisitos: se realizará un análisis de seguridad en las fases iniciales de especificación y diseño de cualquier proyecto o adquisición de productos TIC.

- Ingeniería segura: Se aplicarán principios de ingeniería de sistemas seguros y de codificación segura, promoviendo arquitecturas de "confianza cero".

- Entornos controlados: se establecerán requisitos específicos para garantizar la seguridad de los entornos de desarrollo, preproducción y pruebas.

- Ciclo de pruebas: se implementarán procesos de pruebas de seguridad durante todo el ciclo de vida del desarrollo.

- Gestión de datos de prueba: los datos utilizados en entornos de desarrollo y pruebas serán seleccionados y protegidos adecuadamente; mediante la depuración y anonimización de datos.

- Desarrollo externalizado: en caso de subcontratación, se exigirá contractualmente a los proveedores el cumplimiento de estos mismos requisitos.

esFIRMA dispone de procesos de gestión del cambio, adquisición de activos del sistema de información, diseño y desarrollo seguro que completan y desarrollan lo indicado en la presente Política.

8. Cumplimiento

8.1. Cumplimiento por parte del personal

Todo el personal de esFirma tiene la responsabilidad de conocer, comprender y cumplir estrictamente la presente política de seguridad, así como las normas y procedimientos derivados que afecten a sus funciones específicas; siendo cada persona responsable del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

Asimismo, el personal tiene la obligación de comunicar de manera inmediata y sin dilación indebida cualquier incidente de seguridad, a través de los mecanismos puestos a su disposición por esFIRMA.

Para garantizar la efectividad de este compromiso, esFirma implementa las siguientes acciones:

- **Comunicación interna:** la política es comunicada y reconocida formalmente por todos los empleados. Se encuentra permanentemente disponible para su consulta en la página web de esFIRMA.

- **Concienciación y capacitación:** se ejecutan programas periódicos de formación en materia de seguridad de la información, para asegurar que el personal identifique riesgos y actúe conforme a los protocolos establecidos.

Se aplicarán las sanciones disciplinarias correspondientes al personal que infrinja la presente política o las normativas de seguridad que la desarrollan, de conformidad con lo establecido en la legislación laboral aplicable.

8.2. Cumplimiento por terceras partes

Las terceras partes que presten servicio a esFIRMA o manejen información responsabilidad de esFIRMA deberán cumplir con lo establecido en esta Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. En particular, las terceras partes deberán poner en conocimiento de esFIRMA cualquier incidencia de la que tengan conocimiento y que pueda afectar a un sistema de información y/o la información que se trata o los servicios que se prestan.

Se fomentará que el personal de terceros está adecuadamente concienciado en materia de seguridad y privacidad, al menos al mismo nivel que el establecido en esta Política.

9. Gestión de la documentación y conservación

esFirma mantiene un inventario de la documentación del sistema de gestión de seguridad de la información (políticas, normativas, instrucciones técnicas...).

Toda la documentación, registros y datos de los servicios de confianza se conservarán de acuerdo con los plazos legales establecidos en el Reglamento eIDAS y la Ley 6/2020, garantizando su disponibilidad por un periodo mínimo de 15 años (o según determine la normativa vigente en cada momento).

10. Supervisión e indicadores

Para supervisar la implementación efectiva de esta política y determinar el nivel de madurez de esFirma en materia de seguridad de redes y sistemas de información, se establece un marco de medición continua, apoyado en la actividad del SOC (Centro de Operaciones de Seguridad).

Este marco utiliza los siguientes indicadores clave:

- **Indicadores de gestión de Incidentes:** supervisión de la capacidad de respuesta y tratamiento de eventos de seguridad detectados a través del SOC, asegurando una gestión eficaz de las anomalías y la mitigación de posibles riesgos operativos.

- **Eficiencia de los controles:** medición del nivel de madurez técnica mediante escaneos de vulnerabilidades periódicos y pruebas de penetración.

- **Cultura de seguridad:** evaluación del nivel de capacitación del personal mediante indicadores de participación y éxito en los programas de formación y campañas de concienciación.

- **Disponibilidad y continuidad:** supervisión de los niveles de disponibilidad de los servicios de confianza y análisis de los resultados obtenidos en las pruebas periódicas de los planes de continuidad y recuperación ante desastres.

11. Revisión

La presente política, así como las normativas de seguridad, son objeto de revisión periódica para asegurar su adecuación a los riesgos y al entorno operativo de esFirma.

Esta revisión se realizará, al menos, anualmente y siempre que se produzcan incidentes de seguridad significativos o cambios sustanciales en las operaciones, las tecnologías empleadas o el análisis de riesgos.

La Oficina de Seguridad evaluará la vigencia del documento y propondrá las actualizaciones necesarias cuando proceda. El Comité de Seguridad es el responsable de la aprobación formal de esta política.

El resultado de cada revisión, independientemente de si genera una actualización del documento o no, deberá quedar debidamente documentado para asegurar la trazabilidad del proceso de gobierno de la seguridad.