Política de seguridad de la cadena de suministro

Información general

Control documental

Clasificación	Público
Versión	1
Fecha creación	28/04/2026
Fecha última actualización	28/04/2026
Fichero	Política de seguridad de la cadena de suministro

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Oficina de Seguridad	Cumplimiento Normativo	Comité de Seguridad

Control de versiones

Versión	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Creación del documento	Oficina de seguridad	28/04/2026

Índice

1. Introducción

Esta política establece el marco de control para gestionar los riesgos de seguridad asociados a la cadena de suministro de ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. (en adelante, "**esFIRMA**"), como prestador de servicios de confianza.

esFIRMA reconoce que la seguridad de sus servicios depende de la integridad y resiliencia de sus proveedores y prestadores de servicios. Por tanto, en su relación con la cadena de suministro, esFIRMA asume la responsabilidad de:

1. Identificar los requisitos de seguridad necesarios para cada servicio.
2. Comunicar claramente estos requisitos a sus proveedores directos.
3. Supervisar el cumplimiento continuo de los niveles de servicio acordados.

Por ello, el objetivo de esta política es definir los controles para mitigar los riesgos identificados para la seguridad de las redes y los sistemas de información, asegurando que los activos y servicios TIC de terceros cumplan con los mismos niveles de exigencia que los propios.

2. Alcance

La presente política es de aplicación obligatoria (i) para todo el personal de esFIRMA involucrado en la adquisición de productos o servicios TIC y (ii) para todos los proveedores y prestadores de servicios que tengan acceso a la información o infraestructuras de esFIRMA.

3. Criterios de selección y contratación

En línea con lo establecido en el procedimiento PS-06 Selección de proveedores y PS-07-b Compra de activos del sistema de información, la selección de un determinado proveedor, producto o servicio TIC se basará en lo siguiente:

- esFIRMA especificará los requisitos de seguridad mínimos y evaluará los criterios de ciberseguridad que debe cumplir el proveedor, según la criticidad del activo:

Criterio	Descripción
Prácticas de ciberseguridad	Evaluación de sus procedimientos de desarrollo seguro y gestión de vulnerabilidades.
Capacidad técnica	Capacidad para cumplir especificaciones, gestionar riesgos y mantener niveles de clasificación de seguridad.
Resiliencia de productos TIC	Calidad y medidas de gestión de riesgos integradas en los productos de TIC suministrados.
Diversificación	Estrategia para limitar la dependencia de un único proveedor y asegurar la continuidad del servicio.
Certificaciones	Se valorarán certificaciones en normas ISO 27001, ENS, o certificaciones de producto específicas.

- El proveedor debe garantizar: (i) la disponibilidad de actualizaciones de seguridad durante toda la vida útil prevista del activo y (ii) el compromiso de soporte técnico o, en su defecto, un plan de sustitución/transición antes de la finalización del periodo de mantenimiento.

- Para activos complejos, se solicitará al proveedor información descriptiva de los componentes de hardware y software, declaración de funciones de ciberseguridad implementadas y guía de configuración para un funcionamiento seguro.

4. Gestión de riesgos de proveedores

esFIRMA definirá procesos para gestionar los riesgos asociados al uso de productos o servicios de terceros:

- **Evaluación inicial:** antes de la contratación, esFIRMA verificará el cumplimiento del producto/servicio a nivel de riesgos, seguridad, protección de datos y condiciones contractuales y requisitos medioambientales (cuando resulte procedente). En particular, se valorará el producto atendiendo a las conclusiones del análisis de riesgos, así como a las necesidades técnicas, de formación y de financiación.

  Para la evaluación inicial se tendrán en cuenta criterios como: calidad del producto o servicio suministrado, experiencia del proveedor, relación histórica con el mismo, precio, reputación, certificaciones de producto o empresa. En particular, se analizará el riesgo del proveedor desde el punto de vista de la seguridad de la información y, en función de dicho riesgo, se exigirán las salvaguardas oportunas.

  Además, si el producto o servicio suministrado por el proveedor puede tener un impacto medioambiental significativo, en esta evaluación inicial se tendrán en cuenta posibles certificaciones o salvaguardas que el proveedor tenga en relación con el medioambiente.

- **Evaluación periódica:** los proveedores están sometidos a una evaluación periódica (anual) y cuando se produzca cualquier modificación significativa en los productos o servicios suministrados.

5. Requisitos contractuales obligatorios

Los contratos con proveedores y los acuerdos de nivel de servicio (SLA) deberán especificar:

- Requisitos técnicos específicos para la adquisición de servicios o productos.
- Obligación de formación y capacitación en seguridad para el personal del proveedor.
- Requisitos de idoneidad para los empleados del proveedor que accedan a sistemas críticos.
- Obligación de informar a esFIRMA, sin demora indebida, de cualquier incidente que afecte a la seguridad de la red o de la información de esFIRMA.
- Facultad de esFIRMA para realizar auditorías o recibir informes de auditoría de terceros.
- Compromiso de gestionar vulnerabilidades que representen un riesgo para esFIRMA.
- Normas para la subcontratación, exigiendo el cumplimiento de los mismos requisitos de seguridad.
- Protocolos de recuperación y eliminación segura de la información al término de la relación.

6. Supervisión y control

Para garantizar la efectividad de esta política, esFIRMA:

- Revisará periódicamente los informes de cumplimiento de los acuerdos de nivel de servicio (SLA).
- Analizará los incidentes relacionados con productos de TIC proporcionados por terceros.
- Evaluará la necesidad de revisiones adicionales basadas en el nivel de riesgo detectado.
- Mantendrá una vigilancia constante sobre el desempeño de los proveedores aceptados, mediante su evaluación continua.

7. Revisión y actualización

Esta política se revisará, al menos, anualmente y siempre que se produzcan cambios en las prácticas de ciberseguridad de los proveedores y prestadores de servicios, o cambios significativos en las operaciones de suministro o incidentes de seguridad relevantes que afecten a la cadena de suministro.