Organización de la Seguridad TIC en la Autoridad Independiente de Responsabilidad Fiscal

1. APROBACIÓN Y ENTRADA EN VIGOR

El día 23 de septiembre de 2016 fue aprobada por el Presidente de la Autoridad Independiente de Responsabilidad Fiscal la primera versión de la Política de Seguridad de la AIReF.

Como consecuencia de cambios en la estructura organizativa de la Institución, se hace necesario actualizar esta política a través del presente documento, que se identifica como "Organización de la Seguridad TIC en la Autoridad Independiente de Responsabilidad Fiscal".

2. MISIÓN Y OBJETIVOS DE LA AIReF

La AIReF tiene por objeto velar por la sostenibilidad de las finanzas públicas como vía para asegurar el crecimiento económico y el bienestar de la sociedad española a medio y largo plazo.

Su misión es garantizar el cumplimiento efectivo por las Administraciones Públicas del principio de estabilidad presupuestaria previsto en el artículo 135 de la Constitución Española, mediante la evaluación continua del ciclo presupuestario y del endeudamiento público.

La AIReF tiene como núcleo de su actividad la elaboración de Informes, Opiniones y Estudios sobre los asuntos contemplados en la Ley Orgánica de creación del organismo. Además, elabora anualmente una Memoria de Actividades a la que da la máxima publicidad y difusión.

La Autoridad Independiente de Responsabilidad Fiscal (AIReF) nace con la misión de velar por el estricto cumplimiento de los principios de estabilidad presupuestaria y sostenibilidad financiera recogidos en el artículo 135 de la Constitución Española.
Contacto AIReF:
C/José Abascal, 2-4, 2º planta. 28003 Madrid. Tel. +34 91 010 08 95
Email: Info@airef.es.
Web: www.airef.es

Los Informes no son vinculantes, pero si la Administración o entidad destinataria del informe se aparta de las recomendaciones deberá motivarlo e incorporar el informe en el correspondiente expediente.

Las Opiniones se formularán a iniciativa propia de la AIReF y la Administración o entidad destinataria podrá apartarse del criterio contenido en la Opinión sin necesidad de motivación, a diferencia de los Informes.

Por otro lado, la AIReF realizará los Estudios que el Gobierno de la Nación, el Consejo de Política Fiscal y Financiera, la Comisión Nacional de la Administración Local o la Comisión Financiera de la Seguridad Social le soliciten. De igual forma, podrá realizar estudios que soliciten las Comunidades Autónomas y las Entidades Locales.

3. MARCO LEGAL DE LA AIReF

Los hitos legales que hicieron posible la creación de una Autoridad Fiscal Independiente en España comenzaron con la modificación del artículo 135 de la Constitución, el 27 de septiembre de 2011.

En un segundo paso, una modificación en la Ley Orgánica de Estabilidad Presupuestaria propició la creación de un Organismo independiente de control fiscal como una de las medidas de garantía del último mandato constitucional.

El 14 de noviembre de 2013, se aprobó la Ley Orgánica 6/2013, que cumple con ese requerimiento y crea la AIReF. Su actividad está también regulada en el Estatuto Orgánico, aprobado por Real Decreto 215/2014, de 28 de marzo.

4. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA AIReF

4.1. PRINCIPIOS BÁSICOS

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a) Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la AIReF para conformar un todo coherente y eficaz.

b) Responsabilidad diferenciada: Se concretarán las obligaciones correspondientes a los distintos responsables: el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

c) Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Gestión de Riesgos: De acuerdo con lo establecido en los artículos 24, 25 y 32 del Reglamento (UE) 2016/679, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, así como en el artículo 6 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en al ámbito de la Administración Electrónica, el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.

e) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido, dedicado y diferenciado.

g) Seguridad desde el diseño y por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

4.2. PRINCIPIOS PARTICULARES Y RESPONSABILIDADES ESPECÍFICAS

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad y que inspiran las actuaciones de la AIReF en dicha materia. Se establecen los siguientes:

a) Protección de datos personales: Se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos. Tal y como se establece en el Reglamento (UE) 2016/679, y en Ley Orgánica 3/2018, de 5 de diciembre, dichas medidas deberán ser apropiadas en función del análisis de riesgos mencionado en el apartado 4.1 d) del presente artículo, así como de una evaluación de impacto relativa a la protección de datos cuando sea probable que un tratamiento, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

b) Gestión de activos de información: Los activos de información de la AIReF se encontrarán inventariados y categorizados y estarán asociados a un responsable.

c) Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que

se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

k) Derechos y deberes de los empleados públicos: Los empleados públicos que prestan servicio en la AIReF tienen el derecho y el deber de conocer y aplicar la Política de seguridad y todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones, así como de participar en acciones de difusión y formación orientadas a mejorar el estado de la seguridad de la información.

3. Aplicabilidad de los principios y requisitos mínimos marcados en el Esquema Nacional de Seguridad.

Sin perjuicio de lo establecido en los apartados 1 y 2 anteriores, la Política de seguridad se establecerá asimismo con base en los principios básicos y se desarrollará aplicando los requisitos mínimos contemplados en los artículos 4 y 11 del Real Decreto 3/2010, de 8 de enero.

5. TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

La AIReF depende de los sistemas de Tecnologías de Información y Comunicaciones (TIC) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, adoptando 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 TIC es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza ante 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 las Divisiones de la AIReF deben aplicar las medidas mínimas de seguridad de acuerdo con el Esquema Nacional de Seguridad (ENS), 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 que garanticen la continuidad de los servicios prestados.

Las diferentes Divisiones 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.

Las Divisiones deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con lo previsto en el art. 7 del ENS.

5.1. PREVENCIÓN

Las Divisiones de la AIReF deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad TIC. Para ello, las Divisiones deben implementar las medidas mínimas de seguridad determinadas en la Política de seguridad, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Para garantizar el cumplimiento de la Política de seguridad, el Responsable del Servicio deberá:

1. Solicitar al Responsable del Sistema la entrada en producción de los sistemas informáticos.

2. Solicitar la revisión periódica anual de la Política de seguridad por parte de terceros con el fin de obtener una evaluación independiente.

3. Efectuar un seguimiento regular de la seguridad a través del Responsable de Seguridad.

5.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, el Responsable del Sistema debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

5.3. RESPUESTA

Por medio del presente documento “Organización de la Seguridad TIC en la Autoridad Independiente de Responsabilidad Fiscal”:

1. Se establecen mecanismos para responder eficazmente a los incidentes de seguridad.

2. Se designa al Responsable de Seguridad como punto de contacto para las comunicaciones de incidentes detectados.

3. Se establece un protocolo para el intercambio de información relacionada con el incidente.

5.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, las Divisiones deben implementar todas las acciones y medidas correctivas descritas en la Política de Seguridad que se adjunta como Anexo I.

En caso de desastre, se activarán las medidas de continuidad de los sistemas TIC descritas en el apartado 10.

6. ORGANIZACIÓN DE LA SEGURIDAD

La estructura propuesta diferencia 3 grandes bloques de responsabilidad:

1. La especificación de las necesidades o requisitos.

2. La operación del sistema de información que se atiene a aquellos requisitos, y

3. La función de supervisión de acuerdo al principio básico del ENS “La seguridad como función diferenciada”.

La especificación de requisitos de seguridad corresponde a los Responsables de la Información y el Servicio. La operación corresponde al Responsable del Sistema. La supervisión corresponde al Responsable de Seguridad.

6.1. ROLES Y RESPONSABILIDADES

Las funciones atribuidas a las figuras del Responsable de la Información y del Responsable del Servicio en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, serán ejercidas por el Comité Directivo de la AIReF (CD), al que corresponde:

- Establecer las funciones y responsabilidades en materia de seguridad de la información.
- Aprobar la Política de seguridad del Organismo.

- Facilitar los recursos adecuados para alcanzar los objetivos propuestos en materia de seguridad de la información.

El Responsable del Sistema es quien tiene la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida. Estas funciones serán asumidas por la División Jurídico-Institucional.

6.2. COMITÉ CONSULTIVO DE SEGURIDAD TIC

Este Comité se crea como órgano consultivo encargado de asesorar al Comité Directivo de la AIReF, cuando este lo requiera.

Este Comité Consultivo estará formado por:

- El Responsable de Seguridad.
- El Administrador de Seguridad del Sistema.
- Un asesor informático, empleado de la AIReF, designado por el Presidente.

El Responsable de Seguridad, designado por el Presidente de la AIReF, previa deliberación del Comité Directivo, tendrá las siguientes responsabilidades:

- Mantenimiento de la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de seguridad de la AIReF que se anexa al presente documento.
- Promoción de la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Determinación de las categorías de sistemas, que quedan recogidas en el apartado 9 del presente documento.
- Análisis de riesgos.
- Proposición, en su caso, de medidas de seguridad adicionales.

- Elaboración de la configuración de seguridad, que queda recogida en el Anexo I de este documento.

El Administrador de Seguridad del Sistema será responsable de la:

- Aplicación de la configuración de seguridad.
- Implantación de las medidas de seguridad.
- Aplicación de los procedimientos operativos de seguridad.
- Monitorización del estado de seguridad del sistema.

Por razones del servicio, las funciones de Administrador de Seguridad del Sistema podrán ser ejercidas por el Responsable de Seguridad.

El Asesor Informático, prestará asistencia a los restantes miembros del Comité Consultivo de Seguridad así como al Comité Directivo sobre temas relacionados con normativa, mejores prácticas, gestión de riesgos de los diferentes sistemas de información del a AIReF.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

Corresponderá al Presidente de la AIReF la designación de los distintos responsables.

7. DATOS DE CARÁCTER PERSONAL

Como consecuencia de la nueva regulación sobre la protección de datos recogida en el Reglamento (UE) del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la AIReF ha adoptado las medidas precisas para proteger los datos de carácter personal cuyo tratamiento le corresponde y para garantizar el ejercicio de los derechos de los interesados.

Todos los sistemas de información de la AIReF 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 Documento de Seguridad.

El Anexo IV recoge las Medidas técnicas y organizativas de seguridad en materia de protección de datos de carácter personal.

Para más información sobre la Política de protección de datos de carácter personal de la AIReF, se puede consultar el siguiente enlace de la página web:

https://www.airef.es/es/sobre-nosotros-proteccion-de-datos/

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a la Política de seguridad deberán ser objeto de un nuevo análisis de riesgos, en los siguientes casos:

- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

9. CATEGORÍAS DE LOS SISTEMAS DE INFORMACIÓN DE LA AIReF

De acuerdo con el ENS, los sistemas de información de la AIReF se clasifican en las siguientes categorías:

- Sistemas que utilizan información de carácter público, disponibles en plataformas web de organismos públicos como el INE, BdE, Ministerios, etc..: **Categoría BÁSICA.**
- Sistemas gestionados por la Gerencia de la AIReF que utilizan información con datos personales relativos a los empleados de la institución: **Categoría MEDIA** (Dimensión de seguridad afectada: Confidencialidad).
- Sistemas que utilizan la información confidencial facilitada a la AIReF en el desempeño de sus funciones, por incluir datos de carácter personal o

sensibles, como por ejemplo la concerniente al proyecto Spending Review: **Categoría MEDIA** (Dimensión de seguridad afectada: Confidencialidad).

La Política de Seguridad de la Información que se adjunta en los Anexos I, II, y III define las medidas de seguridad que se adoptan para conseguir el cumplimiento de los principios básicos y requisitos mínimos establecidos.

10. CONTINUIDAD DEL SERVICIO

Las medidas adoptadas para mantener el servicio en caso de un desastre (evento accidental, natural o malintencionado) que dé lugar a la interrupción de las operaciones o servicios habituales de la AIReF, son las siguientes:

1. Los miembros del Comité Directivo, subdirectores y analistas de la AIReF están dotados de ordenadores portátiles y dispositivos móviles.

2 Disponibilidad de correo mediante interfaz web de Office365.

La activación de estas medidas se llevará a cabo mediante la notificación al Responsable de Seguridad de la interrupción del servicio como consecuencia de un desastre

Actualmente, el plan de continuidad de negocio se encuentra bajo revisión, a la espera del Plan de Continuidad de Negocio que está siendo elaborado para todas las Administraciones Públicas.

11. OBLIGACIONES DEL PERSONAL

Todos los empleados y directivos de la AIReF tienen la obligación de conocer y cumplir la Política de Seguridad de la Información, siendo responsabilidad del Comité Directivo de la AIReF disponer los medios necesarios para que la información llegue a los interesados.

Todos los empleados y directivos de la AIReF atenderán a una sesión de concienciación en materia de seguridad TIC, al menos una vez al año.

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.

12. TERCERAS PARTES

Este documento de “Organización de la Seguridad TIC en la Autoridad Independiente de Responsabilidad Fiscal” estará disponible en la página web de la institución, y los Anexos se publicarán en la intranet de la AIReF y estarán a disposición de los interesados que los soliciten.

En el caso de que la AIReF utilice servicios de terceros o ceda información a terceros, se les hará partícipes de la Organización y de la Política 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.