III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

14621 *Resolución de 8 de noviembre de 2012, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueba la política de seguridad de la información de la Agencia Estatal de Administración Tributaria.*

Desde la creación de la Agencia Estatal de Administración Tributaria (en adelante Agencia Tributaria) la implantación de las Tecnologías de la Información y las Comunicaciones (TIC) ha permitido un gran avance en la calidad del servicio ofrecido al ciudadano y en la lucha contra el fraude. Paralelamente ha producido un incremento en la eficacia y eficiencia del personal en el desempeño de sus funciones, con la consecuente mejora continua de sus resultados y del valor entregado a la sociedad en el cumplimiento de su misión.

Sin embargo, la evolución de la sociedad y de las TIC genera cambios en el escenario en que la Agencia Tributaria presta sus servicios. En este sentido, deben garantizarse las condiciones para que esta evolución pueda ser asumida como oportunidad para ofrecer mejores servicios, cumpliendo en todo momento la legislación relacionada con el uso de las TIC en el ámbito de las Administraciones Públicas.

Por tanto, se requiere una actualización, modernización y adaptación de la normativa de seguridad de la información de la Agencia Tributaria, con el objetivo de mejorar, reforzar y racionalizar el modelo actual.

Esta revisión debe sentar las bases para que la seguridad de la información se aborde con una orientación amplia, acorde a los nuevos retos, dedicando los recursos humanos y materiales necesarios y garantizando que los objetivos de seguridad estén al servicio de los objetivos del resto de la organización.

El documento fundamental para abordar la actualización de la normativa de seguridad de la Agencia Tributaria es su Política de Seguridad de la Información, que establece los principios y directrices a tener en cuenta en su posterior desarrollo normativo y define la estructura organizativa de la seguridad de la información.

La Política de Seguridad de la Información debe ser conforme con los requisitos que figuran 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, que establece que todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de una Política de Seguridad de la Información aprobada por el órgano superior correspondiente.

En virtud de lo expuesto, de conformidad con lo establecido en el artículo 103.Tres de la Ley 31/1990, de 27 de diciembre, y en el artículo 11 del Real Decreto 3/2010, de 8 de enero, dispongo:

Primero. *Aprobación de la Política de Seguridad de la Información de la Agencia Tributaria.*

Se aprueba la Política de Seguridad de la Información de la Agencia Tributaria que se incorpora como Anexo de esta Resolución y que se aplicará y observará por todos los órganos y unidades centrales y territoriales de la Agencia Tributaria, en todos sus sistemas de información y por todo el personal destinado en dichos órganos y unidades, así como por el personal de otros organismos o entidades que en virtud de norma legal, acuerdo o convenio tengan acceso a los sistemas de información de la Agencia Tributaria.

cve: BOE-A-2012-14621

Segundo. *No incremento del gasto público.*

La aplicación de esta Resolución no conllevará incremento del gasto público, atendiéndose el desarrollo normativo y la estructura organizativa contemplados en la Política de Seguridad de la Información con los recursos humanos y materiales disponibles en la Agencia Tributaria.

Disposición transitoria única. *Vigencia de normas.*

En tanto no se publiquen las normas o procedimientos específicos previstos en esta Política de Seguridad de la Información, mantendrán su vigencia las normas o procedimientos en materia de seguridad de la información establecidos en la Agencia Tributaria.

Disposición final única. *Entrada en vigor.*

Esta Resolución entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

Madrid, 8 de noviembre de 2012.–El Presidente de la Agencia Estatal de Administración Tributaria, Miguel Ferre Navarrete.

ANEXO

Política de seguridad de la información de la Agencia Estatal de Administración Tributaria

ÍNDICE

I. *Política de Seguridad de la Información*

1. La Política de Seguridad de la Información identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

2. La Política de Seguridad de la Información es el instrumento en que se apoya la Agencia Estatal de Administración Tributaria (en adelante, Agencia Tributaria) para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en la Agencia Tributaria.

3. La Política de Seguridad de la Información pretende dar soporte al desarrollo, coordinación y racionalización de la normativa específica y a la actualización de los conceptos según la evolución de las TIC y de la legislación vinculante y alcanzar de esta forma un conjunto normativo equilibrado y completo.

cve: BOE-A-2012-14621

II. *Misión y marco normativo de la Agencia Tributaria*

1. Los objetivos de la Agencia Tributaria están definidos en el artículo 103 de la Ley 31/1990, de 27 de diciembre, de Presupuestos Generales del Estado para 1991, mediante el que se crea la Agencia Tributaria como la organización administrativa responsable, en nombre y por cuenta del Estado, de la aplicación efectiva del sistema tributario estatal y del aduanero, y de aquellos recursos de otras Administraciones y Entes Públicos nacionales o de la Unión Europea cuya gestión se le encomiende por Ley o por convenio.

2. Corresponde a la Agencia Tributaria desarrollar las actuaciones administrativas necesarias para que el sistema tributario estatal y el aduanero se apliquen con generalidad y eficacia a todos los obligados tributarios, mediante procedimientos de gestión, inspección y recaudación.

3. El marco normativo en el que la Agencia Tributaria desarrolla sus actividades está regulado, esencialmente, por las siguientes disposiciones:

a) Ley 58/2003, de 27 de diciembre, General Tributaria, y sus disposiciones reglamentarias de desarrollo.

b) Artículo 103 de la Ley 31/1990, de 27 de diciembre, de Presupuestos Generales del Estado para 1991, mediante el que se crea la Agencia Tributaria.

4. Adicionalmente y debido al carácter personal y reservado de la información manejada y a los servicios puestos a disposición de los ciudadanos en el ámbito de la Administración Electrónica, la Agencia Tributaria desarrolla sus actividades de acuerdo a la normativa vigente en dichas materias, de entre las que actualmente cabe destacar por su especial relevancia:

a) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

b) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley anterior.

c) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

d) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

e) Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

III. Principios de la seguridad de la información

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 Agencia Tributaria para conformar un todo coherente y eficaz.

b) Responsabilidad diferenciada: En los sistemas de información se diferenciará 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.

cve: BOE-A-2012-14621

La responsabilidad de la seguridad de la información estará por tanto diferenciada de la responsabilidad sobre la prestación de los servicios.

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: 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 establecerá 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 y dedicado.

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

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 de la Información y que inspiran las actuaciones de la Agencia Tributaria en dicha materia. Se establecen los siguientes:

a) Protección de datos de carácter personal: La Agencia Tributaria adoptará las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

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

c) Seguridad ligada a las personas: La Agencia Tributaria implantará 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: La Agencia Tributaria establecerá los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. 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: La Agencia Tributaria 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

cve: BOE-A-2012-14621

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: La Agencia Tributaria contemplará 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: La Agencia Tributaria implantará los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: La Agencia Tributaria implantará 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: La Agencia Tributaria adoptará las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

IV. *Estructura normativa*

1. Dada la diversidad de las competencias y funciones de la Agencia Tributaria, la amplitud de los temas que afectan a la seguridad de la información y su rápida evolución, se hace necesario estructurar el desarrollo de la normativa de seguridad de la información en distintos niveles relacionados jerárquicamente:

a) Primer nivel normativo: Política de Seguridad.
b) Segundo nivel normativo: Normas de Seguridad.
c) Tercer nivel normativo: Procedimientos de Seguridad.

2. La estructura jerárquica permite adaptar con eficiencia los niveles normativos inferiores a los cambios en los entornos operativos de la Agencia Tributaria, sin necesidad de revisar su estrategia de seguridad.

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

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

Constituye el primer nivel normativo la Política de Seguridad de la Información, recogida en el presente documento y aprobada por Resolución de la Presidencia de la Agencia Tributaria.

2. Segundo nivel normativo: Normas de Seguridad de la Información

1. El segundo nivel normativo desarrolla la Política de Seguridad de la Información mediante normas específicas que abarcan un área o aspecto determinado de la seguridad de la información. Las Normas de Seguridad de la Información desarrollarán, al menos, los aspectos recogidos en los Principios particulares y responsabilidades específicas de esta Política de Seguridad de la Información.

2. Las Normas de Seguridad de la Información tienen aplicabilidad en todo el ámbito de la Agencia Tributaria, siendo el órgano responsable de su preparación y aprobación la Comisión de Seguridad y Control de Informática Tributaria, siempre que el rango normativo de la disposición y la atribución de competencias de la Comisión lo permitan.

3. En el ámbito de sus funciones, la Comisión de Seguridad y Control de Informática Tributaria propondrá a la Dirección General de la Agencia Tributaria las medidas que

cve: BOE-A-2012-14621

considere necesarias para el desarrollo o adecuación de la Política de Seguridad de la Información.

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

1. El tercer nivel normativo está constituido por los Procedimientos de Seguridad de la Información, instrucciones 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.

2. Dependiendo del aspecto tratado, se aplicarán a un ámbito específico o a un sistema determinado. La responsabilidad de la aprobación de las normas de este nivel dependerá de su ámbito de aplicación.

V. *Organización de la seguridad*

1. La organización de la seguridad debe tener en cuenta la propia organización de la Agencia Tributaria, en el que se añade al sistema de información centralizado la complejidad de la distribución territorial y funcional de su personal. En consecuencia, las responsabilidades en seguridad de la información deben emerger en todos los ámbitos.

2. Son órganos que intervienen en la seguridad de la información de la Agencia Tributaria:

a) Dirección General de la Agencia Tributaria. Como responsable último del funcionamiento de los servicios, la Dirección General de la Agencia Tributaria apoya explícitamente las actividades relativas a la seguridad de las TIC en todo el ámbito de la Agencia Tributaria.

b) Directores de los Departamentos y Servicios, Director del Gabinete, Delegado Central de Grandes Contribuyentes, Delegados Especiales y Delegados. Responsables del cumplimiento de la normativa de seguridad en su ámbito respectivo.

Dentro del marco establecido en el Esquema Nacional de Seguridad, los Directores de los Departamentos y de los Servicios de la Agencia Tributaria, tienen en su ámbito las funciones de Responsable del Servicio y Responsable de la Información, con la potestad de establecer los requisitos, en materia de seguridad, de los servicios y de la información que manejen. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

c) Departamento de Informática Tributaria. Se ocupa de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones e instalación y de la verificación de su correcto funcionamiento.

Dentro del marco establecido en el Esquema Nacional de Seguridad, el Director del Departamento de Informática Tributaria ejercerá las funciones de Responsable del Sistema.

d) Comisión de Seguridad y Control de Informática Tributaria. La Agencia Tributaria dispone de una Comisión de Seguridad y Control de Informática Tributaria creada por la Resolución de 26 de enero de 1998 de la Presidencia de la Agencia Estatal de Administración Tributaria, que creó comisiones sectoriales de seguridad y control en todas las áreas y reguló la composición, funciones, normas de funcionamiento y seguimiento de las actuaciones de las comisiones sectoriales.

La Comisión de Seguridad y Control de Informática Tributaria es el órgano colegiado encargado de analizar y evaluar los riesgos, de establecer y mantener actualizados los criterios y directrices generales sobre seguridad de la información y de acordar y hacer operativas medidas para mejorar y reforzar los sistemas de seguridad y control.

La Comisión podrá recabar de otros órganos asesoramiento sobre temas en los que tenga que decidir o emitir una opinión, organizándose en grupos de trabajo para abordar trabajos o actividades específicas.

cve: BOE-A-2012-14621

e) Administradores de Seguridad. Todos los Departamentos y Servicios de la Agencia Tributaria, el Gabinete de la Dirección General, las Unidades Centrales, la Delegación Central de Grandes Contribuyentes y las Delegaciones Especiales y Delegaciones designarán un Administrador de Seguridad.

A criterio del Delegado Especial, el Administrador de Seguridad de la Delegación Especial y el Administrador de Seguridad de la Delegación podrán coincidir en las cabeceras de las Delegaciones Especiales.

Los Administradores de Seguridad dependen directamente, y a los efectos de seguridad de la información exclusivamente, de los Directores de Departamentos y Servicios, Director del Gabinete de la Dirección General, Jefes de Unidades Centrales, Delegado Central de Grandes Contribuyentes, Delegados Especiales o Delegados de la Agencia Tributaria.

Son responsables, en sus respectivos ámbitos, de impulsar, coordinar y controlar las medidas de seguridad establecidas en la organización y la ejecución de los planes de actuación que establezca la Comisión de Seguridad y Control de Informática Tributaria.

f) Administrador de Seguridad del Departamento de Informática Tributaria. Encargado de coordinar la actuación de los Administradores de Seguridad y en particular de darles a conocer la normativa y procedimientos de seguridad, en cumplimiento de las directrices y planes que establezca la Comisión de Seguridad y Control de Informática Tributaria, en la que ejercerá de Secretario.

Dentro del marco establecido en el Esquema Nacional de Seguridad, el Administrador de Seguridad del Departamento de Informática Tributaria tiene las funciones de Responsable de Seguridad.

g) Unidad de Seguridad de la Información. Radicada en el Departamento de Informática Tributaria, proporciona una visión integrada de la seguridad de la información y facilita la implantación de medidas de seguridad que afecten a distintas áreas de la Agencia Tributaria.

h) Servicio de Auditoría Interna. Es el órgano especializado de control interno y auditoría de la Agencia Tributaria, responsable de comprobar el grado de implantación y el cumplimiento de la Política de Seguridad de la Información y su normativa de desarrollo, así como de supervisar el uso adecuado de la información y la gestión y seguridad de los sistemas de información de la Agencia Tributaria.

3. Responsable de Seguridad Física del Sistema. El Coordinador del Área de Seguridad de la Agencia Tributaria, dependiendo del Servicio de Gestión Económica, será el Responsable de Seguridad Física del Sistema, encargado de coordinar la actuación del Jefe de Seguridad de los Servicios Centrales y de los Jefes Regionales de Seguridad en el marco del Plan de Seguridad de la Agencia Tributaria, impartiendo directrices a los mismos y proporcionando la adopción de las medidas oportunas para garantizar la seguridad de las personas y de los edificios de la Agencia Tributaria.

4. Resolución de conflictos. En caso de conflicto en materia de seguridad de la información entre los diferentes órganos que intervienen en la misma, este será resuelto por el superior jerárquico correspondiente.

VI. *Protección de datos de carácter personal*

1. Además de las responsabilidades establecidas por esta política en materia de seguridad de la información, la legislación sobre protección de datos de carácter personal establece una serie de responsables con funciones específicas. De acuerdo a la legislación en esta materia, en el ámbito de la Agencia Tributaria:

a) El Director General de la Agencia Tributaria asume las funciones de responsable del fichero.

b) Los Directores de los Departamentos y Servicios asumen las funciones de responsables de los tratamientos que se efectúen en su ámbito de actuación.

cve: BOE-A-2012-14621

c) El Administrador de Seguridad del Departamento de Informática Tributaria asume las funciones de responsable de seguridad.

2. El documento de seguridad relacionado con el tratamiento de datos de carácter personal, debe ser aprobado por la Dirección General de la Agencia Tributaria, conforme a su función de responsable del fichero.

VII. *Gestión de riesgos*

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información y contemplar un análisis de riesgos avanzado que evalúe los riesgos residuales y proponga tratamientos adecuados.
2. La gestión de riesgos sobre el sistema de información estará alineada con la gestión de riesgos establecida en la Agencia Tributaria, centrada en el Mapa de Riesgos de la organización.
3. La Comisión de Seguridad y Control de Informática Tributaria, en el ejercicio de sus funciones, se encargará de analizar y evaluar los riesgos de funcionamiento de los servicios a fin de establecer las correspondientes medidas preventivas.
4. Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y en especial las guías elaboradas por el Centro Criptológico Nacional.

VIII. *Formación y concienciación*

1. La Agencia Tributaria desarrollará actividades específicas orientadas a la formación y concienciación de su personal en materia de seguridad de la información, así como a la difusión de la Política de Seguridad de la Información y su desarrollo normativo, en particular entre el personal de nueva incorporación.
2. A estos efectos, los Planes de Formación de la Agencia Tributaria incluirán actividades formativas específicas sobre esta materia.
3. La Agencia Tributaria promoverá una cultura de la seguridad de la información alineada con la Política de Seguridad de la Información entre aquellas organizaciones y usuarios externos que tengan acceso por acuerdo o convenio a los sistemas de información de la Agencia Tributaria.

IX. *Actualización y revisión periódica*

1. La Política de Seguridad de la Información deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de la Administración Electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.
2. Las propuestas de revisión de la Política de Seguridad de la Información se elaborarán por la Comisión de Seguridad y Control de Informática Tributaria, que con tal objetivo revisará regularmente la oportunidad, idoneidad, completitud y precisión de lo establecido en la Política de Seguridad de la Información.

cve: BOE-A-2012-14621