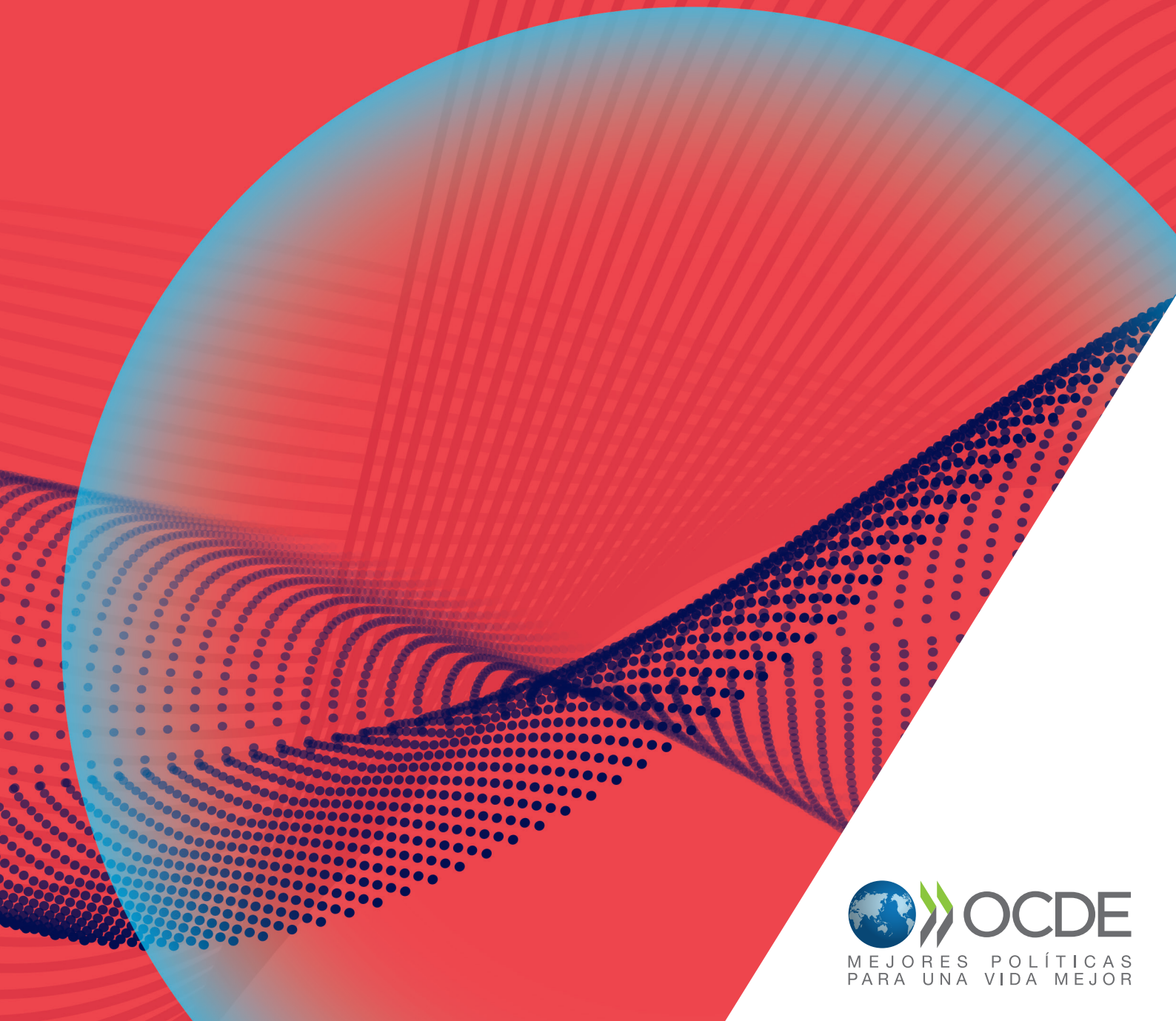
FORO GLOBAL SOBRE
TRANSPARENCIA E INTERCAMBIO DE INFORMACIÓN CON FINES FISCALES

Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información



OCDE
MEJORES POLÍTICAS PARA UNA VIDA MEJOR

Esta guía práctica ha sido elaborada por la Secretaría del Foro Global sobre Transparencia e Intercambio de Información con Fines Fiscales (Foro Global).

Índice

Índice

Abreviaturas y siglas

AEOI	Intercambio Automático de Información
AIN	Análisis de impacto en el negocio
AML	Anti-lavado de dinero
BCM	Gestión de la continuidad del negocio
BEPS	Erosión de la base imponible y traslado de beneficios
CCTV	Circuito cerrado de televisión
CDP	Política de escritorio limpio
CMDB	Base de datos de gestión de configuraciones
CoE	Consejo de Europa
COS	Centro de Operaciones de Seguridad
CRS	Estándar Común de Reporte
CSTI	Continuidad de los servicios de tecnologías de la información
DLP	Prevención de pérdida de datos
DMZ	Zona desmilitarizada
DR	Recuperación ante desastres
EOI	Intercambio de información
EOIR	Intercambio de información previa petición
ETR	Intercambio de información sobre resoluciones fiscales
Foro Global	Foro Global sobre Transparencia e Intercambio de Información con Fines Fiscales
GSI	Gestión de la seguridad de la información
IF	Institución financiera
MAAC	Convención sobre Asistencia Administrativa Mutua en Materia Fiscal, modificada por el Protocolo de 2010
MCAA	Acuerdo Multilateral de Autoridades Competentes
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OSI	Oficial de seguridad de la información
PCO	Plan de continuidad de las operaciones
PDCA	*Plan; Do; Check; Act*
PRD	Plan de recuperación ante desastres
PUA	Política de uso aceptable
RE	Requisito específico
RP	Requisito principal
SIEM	Gestión de eventos e información de seguridad
SLA	Acuerdos de Nivel de Servicio (*Service Level Agreements*)
TI	Tecnologías de la información

Prefacio

Maria José Garde
Presidenta
del Foro Global

Zayda Manatta
Jefa de la Secretaría
del Foro Global

La confidencialidad y la seguridad de la información resultan esenciales en las relaciones entre las administraciones tributarias y los contribuyentes de todo el mundo. Sustentan también el intercambio de información tributaria entre los gobiernos, que constituye uno de los pilares del sistema tributario internacional y de los esfuerzos multilaterales contra la evasión y la elusión fiscal.

La comunidad internacional no habría adoptado el *Estándar para el Intercambio Automático de Información sobre Cuentas Financieras*, que hizo posible una mejora sin precedentes del cumplimiento de las obligaciones tributarias a escala mundial, de no ser por las rigurosas exigencias que prevé en materia de confidencialidad y gestión de la seguridad de la información (GSI).

El Foro Global sobre Transparencia e Intercambio de Información con Fines Fiscales (el Foro Global) viene trabajando desde 2014 en el seguimiento, la revisión inter pares y el apoyo a los miembros en la aplicación del Estándar AEOI. La comprobación y el apoyo del cumplimiento de los requisitos de confidencialidad han ocupado un lugar primordial en esa labor.

Los países miembros en su conjunto han tomado nota de la importancia que las administraciones tributarias de todo el mundo atribuyen a la GSI. A través del proceso de revisión y apoyo multilateral se ha obtenido una visión de conjunto de las disposiciones sobre confidencialidad y buenas prácticas de GSI que existen en las distintas jurisdicciones miembros, así como de la forma en que sus administraciones tributarias incorporan a su actividad los estándares de seguridad internacionales.

En consonancia con nuestra ambición de hacer extensivas las ventajas del AEOI a un número creciente de países en desarrollo, esta guía práctica sobre Confidencialidad y GSI ha sido concebida para orientar sobre las buenas prácticas clave de GSI que constituyen el eje de los estándares del Foro Global en este ámbito.

Confiamos en que todas las administraciones tributarias, y en particular las de los países en desarrollo que aspiran a adoptar el Estándar AEOI y otras formas de intercambio, aprovechen estas orientaciones para continuar fortaleciendo el manejo de la información intercambiada y de otros tipos de datos.

Acerca de esta guía práctica

La finalidad de esta guía práctica sobre confidencialidad y GSI (en adelante, la "guía") es ayudar a los países interesados en participar en el intercambio automático de información (AEOI, por sus siglas en inglés), asegurando que cumplan con las buenas prácticas y estándares en materia de confidencialidad y protección de datos. Ofrece orientación general sobre la adopción de un marco jurídico y un sistema de GSI que garanticen la confidencialidad de la información sobre los contribuyentes, incluida la que se intercambia en virtud de acuerdos internacionales (en adelante, la "información intercambiada"), en línea con los requisitos contemplados en el Estándar para el Intercambio Automático de Información sobre Cuentas Financieras, el denominado "Estándar AEOI".[1] La adopción de un marco de buenas prácticas de GSI reviste interés también para otros tipos de intercambio, como el intercambio de información previa petición, el intercambio espontáneo de información y el intercambio de informes país por país con arreglo a los criterios de la Acción 13 del estándar contra la erosión de la base imponible y el traslado de beneficios (BEPS, siglas en inglés de *Base Erosion and Profit Shifting*).

La guía se compone de las 4 partes siguientes:

- La Parte 1 pone en contexto la participación de los países en desarrollo en el AEOI y presenta los estándares sobre confidencialidad y GSI a los que se refieren los "requisitos principales" de los Términos de Referencia del Foro Global sobre revisiones inter pares de la confidencialidad y la protección de datos en relación con el Estándar AEOI.
- La Parte 2 contiene orientación para ayudar a las jurisdicciones a garantizar que su marco jurídico en materia de confidencialidad de la información sobre los contribuyentes es adecuado para proteger la confidencialidad y el uso adecuado de la información intercambiada en virtud de un acuerdo de intercambio de información.
- La Parte 3 contiene orientación para ayudar a las administraciones tributarias de países en desarrollo a implementar los elementos básicos de un marco de GSI que observe los estándares y mejores prácticas reconocidos a nivel internacional, de conformidad con el Estándar AEOI. Esta sección se subdivide a su vez en seis ámbitos clave de GSI ("requisitos específicos") en torno a los cuales se articulan las exigencias formuladas por el Foro Global.
- La Parte 4 ofrece orientación para ayudar a las jurisdicciones y administraciones tributarias a garantizar que se adopten medidas y procedimientos de cumplimiento efectivos para abordar las violaciones de la confidencialidad.

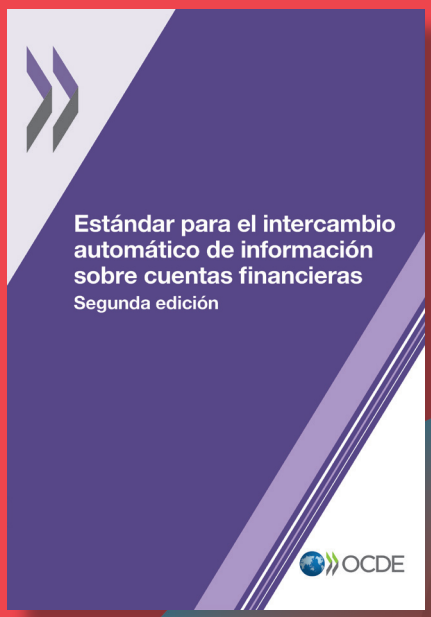
Los Anexos contienen un glosario con los principales conceptos utilizados en esta guía práctica, así como otros recursos útiles.

1. www.oecd.org/tax/exchange-of-tax-information/estandar-para-el-intercambio-automatico-de-informacion-sobre-cuentas-financieras-segunda-edicion-9789264268074-es.htm

Cláusula de responsabilidad

Esta guía práctica no pretende recoger de forma exhaustiva los elementos de los estándares de GSI reconocidos internacionalmente. Su contenido tampoco refleja necesariamente todas las formas posibles en que una jurisdicción puede gestionar la confidencialidad y la seguridad de la información de manera consistente con esos estándares. Esta guía práctica está diseñada solamente como una guía general sobre cómo introducir los elementos de un marco de confidencialidad y GSI adaptado a las administraciones tributarias que participan en el intercambio de información a escala internacional. Son las propias jurisdicciones a las que en última instancia les corresponde establecer marcos jurídicos y de GSI adaptados a sus circunstancias, todo ello en función de los riesgos concretos en materia de confidencialidad y seguridad de la información que cada una de ellas enfrente.

1. Introducción



LA CONFIDENCIALIDAD Y LA PROTECCIÓN DE DATOS COMO PILARES DEL INTERCAMBIO DE INFORMACIÓN TRIBUTARIA

Los contribuyentes valoran la equidad sistémica que proporcionan la transparencia y el intercambio de información (EOI, por sus siglas en inglés) para fines fiscales. Al mismo tiempo, esperan que los gobiernos que intercambian información personal de los contribuyentes la traten con el máximo cuidado. Por ello, el Estándar para el Intercambio Automático de Información sobre Cuentas Financieras (Estándar AEOI, por sus siglas en inglés),[2] partiendo del Estándar para el Intercambio de Información previa Petición (Estándar EOIR, por sus siglas en inglés),[3] exige que las distintas jurisdicciones prevean obligaciones de confidencialidad y protección de datos. Esta exigencia debe traducirse en la existencia de un marco jurídico que garantice la confidencialidad y el uso adecuado de la información intercambiada y un sistema de GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente.

Poco después de la elaboración del Estándar AEOI en 2014, el Foro Global lo adoptó e instauró un proceso para hacer posible su aplicación en todo el mundo mediante compromisos políticos colectivos orientados a su puesta en práctica dentro de los plazos acordados. Se instó a todos los miembros del Foro Global, excepto a los países en desarrollo en los que no existieran centros financieros, a asumir el compromiso de implementar el estándar y comenzar a intercambiar información en 2017 o 2018 con todos los socios apropiados que estuvieran interesados (entendiendo por tales las jurisdicciones interesadas en recibir información que cumplieran las exigencias previstas de confidencialidad y protección de datos). El Foro Global desarrolló igualmente un mecanismo de revisión inter pares del AEOI para apoyar, hacer seguimiento y evaluar la aplicación del Estándar AEOI.

En este contexto, el Foro Global estableció un procedimiento específico para evaluar si las jurisdicciones comprometidas con el AEOI cumplen las exigencias en materia de confidencialidad y protección de datos como condición previa para recibir datos. Estas evaluaciones corren a cargo de un grupo de expertos integrado por funcionarios con experiencia en GSI procedentes de las administraciones tributarias de los países pares (coordinados por la Secretaría del Foro

2. Véase el comentario a la sección 5, relativa a la confidencialidad y la protección de datos, del Modelo de Acuerdo entre Autoridades Competentes recogido en el Estándar AEOI: https://read.oecd-ilibrary.org/taxation/estandar-para-el-intercambio-automatico-de-informacion-sobre-cuentas-financieras-segunda-edicion_9789264268074-es#page30

3. www.oecd.org/tax/transparency/documents/global-forum-handbook-2016.pdf

Global). Las evaluaciones de confidencialidad constan de las fases siguientes:

- una evaluación previa al intercambio antes de que se reciban datos por vez primera (iniciada en 2015); y
- una evaluación posterior al intercambio que valora las medidas de seguridad pertinentes a los datos del AEOI tras su recepción, cuando ya estén siendo utilizados (iniciada en 2019).
- un proceso específico de evaluación previa y posterior al intercambio para las jurisdicciones no recíprocas, reflejando el hecho de que envían datos pero no los reciben.

Cuando se detectan deficiencias, se pide a las jurisdicciones que introduzcan mejoras antes de otorgarles una calificación satisfactoria que les permita comenzar a recibir información. En caso necesario, la Secretaría del Foro Global presta asistencia técnica para ayudar con la introducción de esas mejoras.

Como la posibilidad de que los datos de administraciones tributarias sean vulnerados no se puede descartar por completo, los procesos del Foro Global incluyen un mecanismo de respuesta para hacer frente a las violaciones de datos. Este proceso reevalúa si las medidas de seguridad que han sido vulneradas en la jurisdicción siguen siendo adecuadas para su propósito, y se entablan contactos multilaterales con objeto de informar a todas las partes interesadas afectadas.

ASEGURANDO QUE LOS PAÍSES EN DESARROLLO TAMBIÉN SE BENEFICIEN DEL AEOI

A los miembros del Foro Global que son países en desarrollo sin un centro financiero no se les exigió que aplicaran el Estándar AEOI e iniciaran los intercambios en 2018. Aunque en principio se espera que estas jurisdicciones se comprometan con el Estándar como parte de las obligaciones derivadas de su condición de miembros, se les anima a llevarlo a efecto dentro de plazos prácticos que ellos mismos juzguen viables (para lo que podrán contar con el apoyo de la Secretaría del Foro Global).

No obstante, el Foro Global aspira a que las ventajas del AEOI se hagan plenamente extensivas a todos los países en desarrollo que son miembros, con objeto de mejorar el cumplimiento de las obligaciones tributarias y de movilizar ingresos internos para el desarrollo. Por ello, la Secretaría ha instaurado un programa de creación de capacidades y asistencia técnica con el que ayuda a los países en desarrollo a evaluar su grado de preparación para el AEOI, siendo la confidencialidad y la protección de datos el pilar fundamental del apoyo que se presta en este marco. Además de ayudar a los miembros a implantar los elementos legislativos y administrativos del AEOI, este programa tiene por objetivo ayudarles a prepararse para cumplir las exigencias del Estándar AEOI y para la evaluación de confidencialidad del Foro Global. Este programa está descrito en el Plan de Acción del Foro Global para la participación de los países en desarrollo en el AEOI.[4]

El programa prevé la realización de un análisis de brechas de las administraciones tributarias en materia de GSI con respecto a los requerimientos de confidencialidad y protección de datos del AEOI, así como prestar orientación técnica y asistencia a proyectos para corregir esas deficiencias. Este programa de ayuda está disponible bajo demanda de los países miembros interesados, y requiere que dichos países asuman el compromiso político firme de elaborar una planificación realista para su participación en el AEOI y llevarla a efecto en los plazos establecidos.

UNA GUÍA PRÁCTICA PARA APOYAR LA CONFIDENCIALIDAD Y LA PROTECCIÓN DE DATOS DE LAS ADMINISTRACIONES TRIBUTARIAS DE PAÍSES EN DESARROLLO

Si bien la Secretaría del Foro Global proporciona apoyo personalizado en GSI a países miembros que lo soliciten individualmente, también ha elaborado esta guía práctica para ayudar a las administraciones tributarias de todos los países en desarrollo a adoptar o mejorar los elementos clave de su marco de GSI, así como a gestionar de forma segura la información que se intercambia en virtud de acuerdos internacionales en materia tributaria.

La estructura de esta guía se ajusta a la de los requisitos de confidencialidad y protección de datos del Estándar AEOI, plasmados y detallados en los Términos de Referencia para las evaluaciones, y al cuestionario de evaluación.[5] Esto simplificará la tarea de las administraciones tributarias que están introduciendo mejoras necesarias en sus sistemas de GSI, al tiempo que las prepara de manera sistemática para su evaluación de la confidencialidad en el marco de AEOI que lleva a cabo el Foro Global.

4. www.oecd.org/tax/transparency/documents/plan-of-action-AEOI-and-developing-countries.pdf

5. Los Términos de Referencia pueden consultarse en www.oecd.org/tax/transparency/documents/confidentiality-data-safeguards-assessments-tor.pdf. El cuestionario de evaluación de la confidencialidad y la protección de datos lo proporciona la Secretaría al personal autorizado de las jurisdicciones que lo soliciten.

EL ESTÁNDAR AEOI Y LOS REQUISITOS PRINCIPALES Y ESPECÍFICOS DE EVALUACIÓN DEL FORO GLOBAL

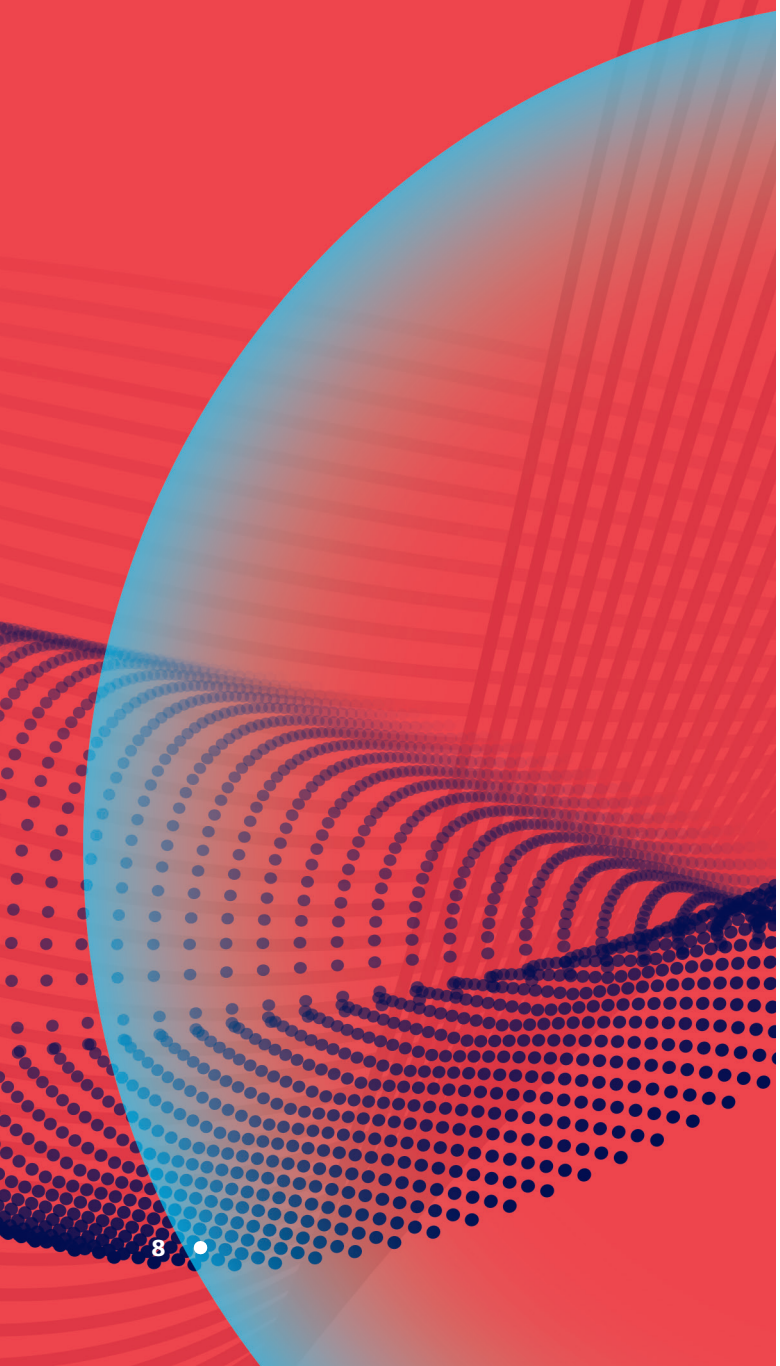
El Estándar AEOI exige que las jurisdicciones preserven la confidencialidad de la información intercambiada y la protejan debidamente, así como que dicha información sea utilizada con arreglo al acuerdo que sirvió de base para el intercambio. Esta exigencia se recoge como requisito principal (RP) 3 en los Términos de Referencia sobre el proceso de revisión inter pares del estándar AEOI.[6] El RP 3 se descompone en tres elementos esenciales (RPs 1 a 3), que a su vez se desdoblan en requisitos específicos (RE), tal como se aprecia en la Tabla 1. Esta guía práctica ofrece orientación sobre cada uno de estos RPs y REs.

Tabla 1. **Requisitos principales y requisitos específicos de las evaluaciones de confidencialidad**

RP 3.1 Las jurisdicciones deben contar con un marco jurídico que garantice la confidencialidad y el uso adecuado de la información intercambiada	RP 3.2 Las jurisdicciones deben contar con un marco GSI que se ajuste a los estándares y mejores prácticas reconocidos internacionalmente	RP 3.3 Las jurisdicciones deben contar con medidas y procedimientos de cumplimiento con los que abordar las violaciones de confidencialidad
• RE 3.1.1 El marco juridico de las jurisdicciones debe incluir disposiciones suficientes para proteger la confidencialidad de la información de los contribuyentes, incluyendo la información intercambiada, y establecer que únicamente se podrá revelar y utilizar esa información en determinadas circunstancias bien delimitadas, siendo esas circunstancias consistentes, en lo que respecta a la información intercambiada, con lo dispuesto en el instrumento internacional de intercambio (bilateral o multilateral) en virtud del cual se intercambió la información	• RE 3.2.1 Los organismos relevantes deben contar con un sistema de gestión de la seguridad de la información adecuado • RE 3.2.2 Los organismos relevantes deben tener controles adecuados de recursos humanos • RE 3.2.3 Los organismos relevantes deben contar con controles de acceso adecuados, ya sea el acceso físico o lógico • RE 3.2.4 Los organismos relevantes deben contar con una seguridad adecuada de los sistemas de TI • RE 3.2.5 Los organismos relevantes deben proteger la información de forma apropiada • RE 3.2.6 Los organismos relevantes deben contar con un sistema adecuado de gestión de las operaciones, que incluya la gestión de incidentes , la gestión del cambio, supervisión y auditoría	• RE 3.3.1 Las jurisdicciones deben imponer multas y/o sanciones adecuadas por la divulgación o el uso indebidos de la información • RE 3.3.2 Las jurisdicciones deben aplicar procedimientos adecuados para abordar incumplimientos presuntos o reales, incluida la aplicación efectiva de multas o sanciones

6. www.oecd.org/tax/transparency/documents/AEOI-terms-of-reference.pdf. Los RPs 1 y 2 de las revisiones inter pares del estándar AEOI hacen referencia a la obtención y el intercambio efectivos de información en relación con el Estándar AEOI. El RP 1 requiere que las jurisdicciones garanticen que todas las instituciones financieras que reportan información apliquen procedimientos de diligencia debida de conformidad con el Estándar Común de Reporte (CRS) para revisar las cuentas financieras que administran y para recabar y reportar la información requerida. El RP 2 requiere que las jurisdicciones intercambien la información con todos los socios apropiados interesados, dentro de los plazos previstos y con garantías de que su obtención, selección, preparación, validación y transmisión se ajustan al Estándar AEOI.

2. Marco jurídico que garantice la confidencialidad y el uso adecuado de la información intercambiada (Requisito Principal 3.1)



REQUERIMIENTOS DE LOS ACUERDOS INTERNACIONALES SOBRE INTERCAMBIO DE INFORMACIÓN

Una asistencia mutua efectiva en materia tributaria requiere que cada jurisdicción tenga la seguridad de que la otra tratará con la debida confidencialidad la información que reciba en el curso de la cooperación entre ambas.

De ahí que los acuerdos internacionales sobre intercambio de información contengan disposiciones relativas a la confidencialidad y a la obligación de los Estados Contratantes, es decir, las jurisdicciones participantes en el intercambio, de preservar el secreto o la confidencialidad de la información intercambiada con arreglo a los mismos criterios que aplican a la información recabada en virtud de su legislación nacional. Los participantes en el intercambio pueden suspender el EOI si no existen garantías suficientes o si se ha producido una violación de la confidencialidad y no tienen la seguridad de que la situación se haya resuelto de manera apropiada.

En el Recuadro 1 se recogen extractos de varias disposiciones modelo de intercambio internacional relativas a la confidencialidad, sobre las que se basan la mayoría de los instrumentos internacionales vigentes. Las jurisdicciones deben procurar incluir disposiciones equivalentes en los nuevos acuerdos de EOI celebrados con sus socios.

De estas obligaciones internacionales se deriva la necesidad de proteger la confidencialidad de la información sobre los contribuyentes, incluida la que haya sido objeto de intercambio, a través de un marco jurídico interno que sea efectivamente aplicable y que sirva de base para las medidas prácticas adoptadas en cada jurisdicción para garantizar la confidencialidad.

En ausencia de un marco de estas características, ni los participantes en el intercambio de información ni los propios contribuyentes podrán confiar en la protección de la confidencialidad ni en que las violaciones de la misma vayan a ser debidamente investigadas y sancionadas, aun cuando se hayan adoptado prácticas rigurosas de GSI.

En este contexto, el RP 3.1 requiere que los países cuenten con un marco jurídico que garantice la confidencialidad y el uso adecuado de la información intercambiada bajo un acuerdo internacional de intercambio de información.

Recuadro 1. **Disposiciones sobre confidencialidad de los modelos de acuerdo internacional sobre intercambio de información y la MAAC**

Artículo 26(2) del Modelo de Convenio Tributario sobre la Renta y sobre el Patrimonio[7]

"La información recibida por un Estado Contratante en virtud del apartado 1 se mantendrá en secreto al igual que la información obtenida conforme a la legislación interna de ese Estado y solo se desvelará a las personas o autoridades (incluidos los órganos jurisdiccionales y administrativos) encargadas de la liquidación o recaudación de los impuestos a los que hace referencia el párrafo 1, de su aplicación efectiva o de la persecución del incumplimiento relativo a los mismos, de la resolución de los recursos referentes a tales impuestos o de la supervisión de las funciones anteriores. Dichas personas o autoridades solo utilizarán esta información para estos fines. Podrán desvelar la información en las audiencias públicas de los tribunales o en las sentencias judiciales. No obstante, la información recibida por un Estado contratante podrá utilizarse para otros fines cuando, conforme la legislación de ambos Estados, pueda utilizarse para dichos otros fines y la autoridad competente del Estado emisor autorice dicho uso."

Artículo 8 del Modelo de Acuerdo sobre intercambio de información en materia tributaria[8]

"Toda información recibida por una Parte contratante al amparo del presente Acuerdo se tratará como confidencial y sólo podrá comunicarse a las personas o autoridades (incluidos los tribunales y órganos administrativos) bajo la jurisdicción de la Parte contratante encargadas de la gestión o recaudación de los impuestos comprendidos en el presente Acuerdo, de los procedimientos declarativos o ejecutivos relativos a dichos impuestos o de la resolución de los recursos relativos a los mismos. Dichas personas o autoridades sólo utilizarán esa información para dichos fines. Podrán revelar la información en procedimientos judiciales públicos o en las sentencias judiciales. La información no podrá comunicarse a ninguna otra persona, entidad, autoridad o a cualquier otra jurisdicción sin el expreso consentimiento por escrito de la autoridad competente de la Parte requerida."

Artículo 26(2) de la Convención modelo de las Naciones Unidas sobre la doble tributación entre países desarrollados y países en desarrollo[9]

"Cualquier información recibida con arreglo al párrafo 1 por un Estado contratante se considerará secreta, de la misma forma que la información obtenida en virtud de la legislación interna de ese Estado, y se revelará solo a las personas o autoridades (inclusive tribunales y órganos administrativos) que participen en la estimación de la base imponible o la recaudación, o la decisión de recursos en relación con los impuestos a que se hace referencia en el párrafo 1, o en la supervisión de esas personas o autoridades. Esas personas o autoridades utilizarán la información exclusivamente para esos fines, pero podrán revelarla en actuaciones de tribunales públicos o decisiones judiciales. No obstante, la información recibida por un Estado contratante podrá utilizarse para otros fines cuando dicha información pueda utilizarse para otros fines con arreglo a la legislación de los dos Estados y la autoridad competente del Estado emisor autorice dicho uso."

Artículo 22 (Secreto) de la MAAC[10]

1. Cualquier información obtenida por una Parte de conformidad con esta Convención deberá mantenerse como secreta y deberá protegerse de la misma manera que la información obtenida con base en la legislación interna de esa Parte y, en la medida en que se requiera para asegurar el nivel necesario de protección de datos personales, de conformidad con las salvaguardas que puedan especificarse por la Parte que proporciona la información, según lo requiera su legislación interna.

2. Dicha información, en cualquier caso, podrá ser revelada únicamente a las personas o autoridades (incluidos los tribunales y órganos administrativos o de supervisión) encargadas de la determinación, recaudación o cobro de los impuestos de esa Parte, de los procedimientos declarativos o ejecutivos relativos a dichos impuestos o de la resolución de los recursos relativos a los mismos o de la supervisión de lo anterior. Únicamente estas personas o autoridades podrán utilizar la información, y sólo para los fines señalados. No obstante, lo dispuesto en el párrafo 1, dichas personas o autoridades podrán revelar la información en las audiencias públicas de los tribunales o en las sentencias judiciales relacionadas con dichos impuestos.

3. [...]

4. Sin perjuicio de lo dispuesto en los párrafos 1, 2 y 3 la información que reciba una Parte podrá ser utilizada para otros efectos cuando ello sea factible de conformidad con la legislación de la Parte que otorgue la información y la autoridad competente de esa Parte autorice dicho uso. La información que una Parte otorgue a otra Parte puede transmitirse por esta última a una tercera Parte, previa autorización de la autoridad competente de la Parte mencionada en primer lugar.

7. www.oecd-ilibrary.org/taxation/modelo-de-convenio-tributario-sobre-la-renta-y-sobre-el-patrimonio-version-abreviada-2017_765324dd-es

8. www.oecd.org/ctp/exchange-of-tax-information/37975122.pdf

9. www.un-ilibrary.org/content/books/9789210474047

10. www.oecd.org/ctp/exchange-of-tax-information/ESP-Amended-Convention.pdf

Marco jurídico que garantice la confidencialidad y el uso adecuado de la información intercambiada (Requisito Principal 3.1)

Los acuerdos internacionales de intercambio de información contienen también disposiciones que limitan a quién puede revelarse la información intercambiada y los fines para los que puede utilizarse esta (véase el Recuadro 1). Por lo general, esta revelación se limita a las personas o autoridades (incluidos los tribunales y órganos administrativos) que intervienen en la/el:

- Evaluación
- Recaudación
- Cumplimiento
- Enjuiciamiento, y
- Determinación de apelaciones

en relación con los impuestos sobre los que puede intercambiarse información con arreglo al acuerdo aplicable.

La información intercambiada puede comunicarse también al contribuyente, su representante o a un testigo. También puede revelarse a las autoridades gubernamentales o judiciales encargadas de resolver si la información puede comunicarse al contribuyente, su representante o a testigos. Los tribunales y los órganos administrativos que intervengan en los asuntos tributarios mencionados arriba pueden revelar la información en las sesiones o en las decisiones judiciales. Una vez que la información se utiliza en procedimientos judiciales públicos o en decisiones judiciales y, por lo tanto, se hace pública, es claro que desde ese momento dicha información puede ser citada de los expedientes o decisiones judiciales para otros fines, incluso como posible prueba. Pero esto no significa que las personas y autoridades antes mencionadas estén autorizadas a proporcionar, previa solicitud, información adicional recibida. Si uno o ambos socios de intercambio se oponen a que los tribunales hagan pública la información de esta manera, o una vez que la información se ha hecho pública de esta manera, o a que la información se utilice para otros fines, porque este no es el procedimiento normal bajo sus leyes internas, deben indicarlo expresamente en su acuerdo de intercambio.

En resumen, los acuerdos que regulan el intercambio de información en materia tributaria generalmente autorizan la divulgación y el uso de la información intercambiada para fines tributarios.

No obstante, socios de intercambio pueden acordar que se permita también la divulgación y el uso de la información intercambiada para otros fines, por ejemplo, para colaborar en la investigación y enjuiciamiento de delitos de lavado de dinero o financiación del terrorismo. En tales casos, esos otros fines deberán ser conformes con la legislación interna de cada uno de los socios de intercambio, y la jurisdicción que reciba la información deberá buscar la autorización de la autoridad competente de la jurisdicción que proporciona la información para divulgarla y utilizarla para fines no tributarios. La Convención Multilateral de Asistencia Administrativa Mutua en Materia Fiscal (MAAC), entre otros, contempla esta posibilidad (véase el Recuadro 1).

En este contexto, por autoridad o autoridades competentes se entiende la(s) persona(s) o autoridad(es) de gobierno designada(s) por una jurisdicción como competentes para el intercambio de información en virtud de un acuerdo internacional en la materia.

REQUISITO ESPECÍFICO 3.1.1: UN MARCO JURÍDICO QUE GARANTICE LA CONFIDENCIALIDAD Y EL USO ADECUADO DE LA INFORMACIÓN INTERCAMBIADA

En línea con los requisitos de confidencialidad establecidos en los acuerdos internacionales sobre intercambio de información, el requisito específico (RE) 3.1.1 establece que el marco jurídico interno de cada jurisdicción ha de contener disposiciones adecuadas para proteger la confidencialidad de la información sobre los contribuyentes, incluida la información intercambiada, y establecer que únicamente se podrá revelar y utilizar esa información en determinadas circunstancias bien delimitadas, que deberán ser conformes, en lo referente a la información intercambiada, con lo dispuesto en el instrumento internacional de intercambio aplicable (bilateral o multilateral) en virtud del cual se efectuó el intercambio.

El RE 3.1.1 plantea por tanto dos aspectos esenciales:

- Debe existir un marco jurídico que garantice la confidencialidad de la información sobre los contribuyentes en general, y la información intercambiada debe estar comprendida en su ámbito de protección.
- Ese marco jurídico debe garantizar la revelación y utilización de la información intercambiada en determinadas circunstancias y de manera conforme con lo dispuesto en el acuerdo internacional sobre intercambio de información en virtud del cual se produjo ese intercambio.

Un marco jurídico que proteja la confidencialidad de la información relativa a los contribuyentes, incluida la información intercambiada

La legislación nacional de la jurisdicción ha de garantizar la confidencialidad o el secreto de la información sobre los contribuyentes, entendiendo por tal la información relativa a sus ingresos, gastos, cuentas, obligaciones tributarias, cuestiones personales, asuntos de negocios u otros aspectos relevantes que una

administración tributaria pueda manejar en el ejercicio de sus funciones.

Los estándares sobre confidencialidad pueden estar recogidos en leyes, regulaciones secundarias o ejecutivas o guías administrativas. Sea cual sea el instrumento legal utilizado, estos deben ser jurídicamente vinculantes y aplicables.

En particular, la legislación nacional:

- Establecerá el carácter confidencial o secreto de la información sobre los contribuyentes utilizada por la administración tributaria;
- Obligará a todos los miembros del personal (permanentes, temporales o contratistas) a preservar el secreto absoluto y la confidencialidad de la información sobre los contribuyentes que manejen en el curso de su trabajo;

Recuadro 2. **Ejemplos del alcance de las disposiciones sobre confidencialidad**

La legislación nacional de la jurisdicción A contiene normas sobre confidencialidad aplicables a la información sobre los contribuyentes dispersas en distintas leyes. La Ley del Impuesto sobre la Renta impone a todo el personal de la administración tributaria (incluidos los contratistas) la obligación general de preservar la confidencialidad de toda la información tributaria que maneje en el ejercicio de sus funciones. Además, la Ley de Secretos Oficiales prohíbe a los funcionarios públicos y a los contratistas, o a quienes hubieran ejercido con anterioridad esos cargos, revelar información secreta.

La Ley de Empleo Público de la jurisdicción B impone la obligación de preservar la confidencialidad a todos los funcionarios públicos (incluido el personal temporal y los contratistas proveedores de servicios a las autoridades públicas). El Código de Conducta de los funcionarios públicos establece la confidencialidad de toda información a que tengan acceso en el curso de su trabajo. En lo referente al intercambio de información, la Ley de Cooperación Tributaria Internacional se aplica expresamente a todo el personal y a los contratistas que intervengan en cualquier aspecto del intercambio de información (entre ellos, los proveedores de servicios de TI), incluyéndolos en el ámbito de aplicación de las disposiciones generales sobre confidencialidad de la información tributaria.

- Garantizará que la obligación de preservar la confidencialidad o el secreto sea exigible a los miembros del personal durante todos su periodo de servicio y después de su cese, traslado a otra función, jubilación, o de la expiración del contrato, o de cualquier otra circunstancia similar que ponga fin a su contacto con la información sobre los contribuyentes (este aspecto se detalla en el RE 3.2.2 sobre los mecanismos de control de los recursos humanos);
- Preverá la imposición de multas o sanciones para prevenir o sancionar las violaciones de la confidencialidad (los aspectos relativos a las multas y sanciones se detallan en el RE 3.3.1).

Los estándares sobre confidencialidad pueden estar recogidos en leyes tributarias o en leyes de índole más general (por ejemplo, las disposiciones legales sobre la función pública o sobre las obligaciones de los funcionarios de servicio civil), en leyes sobre protección de la esfera privada y los datos personales y/u otras leyes (véanse los ejemplos del Recuadro 2).

En algunas jurisdicciones, las disposiciones generales sobre confidencialidad de la información tributaria pueden tener un alcance tan amplio que abarque la información intercambiada. Un ejemplo sería una disposición recogida en una ley tributaria que imponga la obligación de preservar la confidencialidad o el secreto a los funcionarios públicos o personas contratadas por la administración tributaria con respecto a cualquier información sobre los contribuyentes que puedan manejar en el curso de su trabajo, con independencia de cuál sea la fuente de la información (de fuente nacional o de EOI) y con independencia de que el contribuyente tenga su residencia fiscal en ese o en otro país.

Sin embargo, cuando las disposiciones generales no garanticen la cobertura de la información intercambiada, las jurisdicciones tendrán que aprobar disposiciones específicas que garanticen que la protección jurídica de la confidencialidad sea aplicable a esa información.

Revelación y uso adecuados de la información intercambiada de manera conforme con los acuerdos internacionales sobre intercambio de información

Son muchas las jurisdicciones cuya legislación nacional permite compartir información sobre contribuyentes con autoridades no tributarias. Por ejemplo, no es infrecuente que la ley autorice la revelación de ciertos datos de los contribuyentes a alguna de las autoridades siguientes:

Marco jurídico que garantice la confidencialidad y el uso adecuado de la información intercambiada (Requisito Principal 3.1)

- Órganos de investigación y encargados del cumplimiento de la ley, tales como organismos anticorrupción o autoridades encargadas de la lucha contra el lavado de dinero (AML, siglas en inglés de *anti-money laundering*) o las autoridades aduaneras;
- Autoridades de la seguridad social, para fines relacionados con la administración de prestaciones sociales;
- Miembros del público general en ciertos casos, en aplicación de las normas de libertad de información.

Teniendo en cuenta que los acuerdos internacionales de intercambio suelen ser más restrictivos en cuanto a las circunstancias en que puede revelarse y utilizarse la información, según se describe en esta guía, las jurisdicciones deben asegurarse de que las obligaciones previstas en sus acuerdos de intercambio entren en vigor y tengan carácter vinculante en su legislación interna, de manera que la información intercambiada únicamente se revele y utilice en la forma acordada con los socios en el intercambio.

Las jurisdicciones dan efecto a sus obligaciones internacionales (incluidas las relativas a la confidencialidad) por distintas vías (véanse los ejemplos del Recuadro 3). Una posibilidad es modificar la legislación interna para garantizar que las obligaciones derivadas de acuerdos internacionales sean respetadas bajo las leyes domésticas. En algunas jurisdicciones, las obligaciones jurídicas internacionales prevalecen sobre las leyes domésticas en caso de conflicto en virtud de estatutos de jerarquía normativa o de la constitución. En otras jurisdicciones, las obligaciones derivadas de acuerdos internacionales son implementadas de tal forma que, en caso de conflicto con la ley interna, prevalezca el acuerdo. Algunos países combinan ambos enfoques.

Las jurisdicciones pueden completar sus normas jurídicas sobre revelación y utilización de la información intercambiada con instrucciones sobre cómo proceder a su revelación y utilización para fines no tributarios, cuando sea permitido hacerlo. En esas instrucciones puede especificarse que será necesario solicitar la autorización de la autoridad competente del socio de intercambio que ha proporcionado la información, así como garantizar que la revelación y utilización se hagan de manera conforme con las leyes de ambas partes.

Recuadro 3. **Ejemplos de leyes que dan efecto a los acuerdos internacionales de intercambio de información**

En la jurisdicción A, cuando existen inconsistencias entre la ley doméstica y los acuerdos internacionales, las leyes por las que se incorporan estos a la ley interna especifican que los acuerdos prevalecen.

En la jurisdicción B, existen leyes que establecen que cualquier restricción sobre el uso de la información intercambiada que haya sido acordada con una jurisdicción extranjera o impuesta por esta, será aplicable aun cuando sea contraria a la legislación interna.

3. Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

LA NECESIDAD DE UN MARCO DE GSI

Para que las garantías legales previstas en los acuerdos internacionales y en la legislación interna resulten efectivas, se requieren prácticas y procedimientos que las lleven a efecto. De ahí que el RP 3.2 exija que las jurisdicciones cuenten con un marco de Gestión de la Seguridad de la Información (GSI) que se ajuste a los estándares y mejores prácticas reconocidos internacionalmente y garantice la protección de la información intercambiada.

Un marco GSI es un conjunto de acuerdos de gobernanza, políticas, procedimientos, prácticas y controles de seguridad. Un control de seguridad es una medida específica dirigida a mitigar o eliminar un riesgo para la seguridad: puede ser un procedimiento, un equipo o un programa informático, u otro.

El Estándar AEOI requiere la existencia de un marco completo de GSI debido a la naturaleza sensible, los grandes volúmenes y los medios electrónicos a través de los cuales se intercambia la información. Los sistemas de las administraciones tributarias pueden recibir miles de registros financieros que deben ser manejados por toda una serie de procesos de negocio, sistemas de IT y personas. Estos factores elevan considerablemente los riesgos para la seguridad, incluido el acceso no autorizado a la información por el personal o por un ciberataque específico, que pueden llevar a violaciones de la confidencialidad si no se adoptan medidas adecuadas de mitigación.

Los distintos mecanismos de control que, como parte del marco de GSI, se aplican a esos procesos, sistemas y personas tienden a reducir los riesgos y las amenazas a la información y crean una “cultura de cuidado” dentro de la administración tributaria.

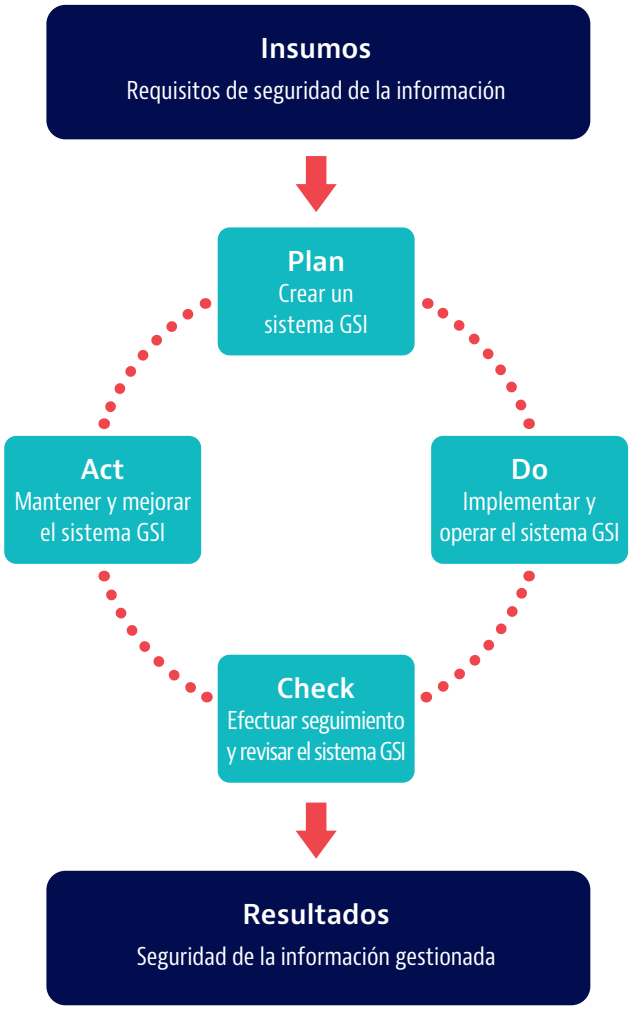
ESTÁNDARES Y MEJORES PRÁCTICAS RECONOCIDOS INTERNACIONALMENTE

Por estándares y mejores prácticas de GSI reconocidas internacionalmente se entienden estándares como los de la serie ISO/IEC 27000, publicada conjuntamente por la Organización Internacional de Normalización (ISO, por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés), u otros estándares equivalentes. Las administraciones tributarias a nivel mundial aplican diferentes estándares nacionales o internacionales y no existe un único estándar de GSI universalmente aceptado; no obstante, la serie ISO/IEC 27000 es la más citada en los trabajos del Foro Global.

La serie ISO/IEC 27000, pese a su complejo contenido, puede representarse de forma simplificada como un

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

FIGURA 1. **El ciclo PDCA en la Gestión de la Seguridad de la Información**



proceso continuado e iterativo de mejora, ampliamente reconocido, expresado con el acrónimo "PDCA" ("*Plan; Do; Check; Act*"). El ciclo PDCA subraya que la seguridad de la información es una práctica en mejora continua y que las amenazas para la seguridad evolucionan constantemente.

El ciclo PDCA requiere desarrollar e implementar un marco y un plan de seguridad de la información, aplicar los mecanismos de control de la seguridad según lo planeado, verificar que el plan funciona debidamente y mejorar continuamente el plan y los controles, reforzando las actividades que funcionan debidamente y modificando las que no lo hacen (véase la Figura 1).

UN MARCO DE GSI PARA EL INTERCAMBIO DE INFORMACIÓN TRIBUTARIA

El Estándar AEOI y las evaluaciones de confidencialidad requieren que las administraciones tributarias estén en condiciones de demostrar que sus prácticas se ajustan a los estándares de la serie ISO/IEC 27000 o que disponen de un sistema equivalente de seguridad de la información[11] , así como que la información sobre los contribuyentes recibida en virtud de un acuerdo internacional se encuentra protegida por ese sistema.

Los estándares de la serie ISO/IEC 27000 están concebidas de forma amplia y no se refieren específicamente a las administraciones tributarias. Fueron desarrollados para permitir que cualquier tipo de organización empresarial pueda aplicar un marco de GSI adecuado y demostrar su acreditación de seguridad a otras organizaciones.

Partiendo de esta base, en el curso de las evaluaciones de la confidencialidad bajo AEOI, el panel de expertos del Foro Global se basó en los estándares de la serie ISO/IEC 27000 para elaborar una visión global de los riesgos para la seguridad de la información en las administraciones tributarias y de las mejores prácticas de control empleadas por las administraciones tributarias de todo el mundo para mitigar esos riesgos.

Con objeto de optimizar los estándares internacionales para los fines de la administración tributaria y el intercambio de información, los requerimientos de GSI recogidos en RP 3.2 fueron organizados en seis encabezados (REs 3.2.1 a 3.2.6) que se ajustan en líneas generales al modo en que las administraciones tributarias organizan normalmente sus arreglos de GSI, utilizando el ciclo PDCA como guía general.

- El RE general o "integral" 3.2.1 se corresponde con las fases 'Plan' y 'Act' del PDCA. Establece que las administraciones tributarias u otras autoridades responsables del intercambio de información tributaria ("organizaciones relevantes") deberán tener un marco global de GSI que incluya una política de GSI, un sistema de gestión del riesgo y un marco de gestión de la continuidad del negocio.
- Los REs 3.2.2 a 3.2.5 se corresponden con la fase 'Do' del PDCA:
  - El RE 3.2.2 hace referencia a los controles de seguridad aplicados a los recursos humanos (personal interno y contratistas externos). Requiere que se informe a los recursos humanos sobre su obligación de preservar la confidencialidad y la seguridad de la información tributaria, se verifiquen debidamente sus antecedentes, se les impartan la formación y la sensibilización

11. Basado en otras buenas prácticas internacionales, como NIST SP 800-53, CSF. Otras normas internacionales que pueden utilizarse dentro de sus ámbitos propios son los Objetivos de control para la información y tecnologías afines (COBIT), el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO), la Biblioteca de infraestructura de tecnologías de información (ITIL), etc.

necesarias y se asegure que dejan de tener acceso a la información protegida al finalizar su relación laboral.

- El RE 3.2.3 hace referencia a los controles de seguridad para gestionar el acceso a sistemas de información ("acceso lógico") y a las instalaciones ("acceso físico"), de forma que la información se gestione con el principio de "necesidad de saber" (*need to know principle*, en inglés).

- El RE 3.2.4 hace referencia a los controles de seguridad para proteger los sistemas de TI, lo que comprende la infraestructura, redes, aplicaciones, estaciones de trabajo o *workstations* y dispositivos.

- El RE 3.2.5 hace referencia a los controles de seguridad que protegen la información o los datos en sí mismos, incluidos los procedimientos aplicados para clasificar la información y asegurar un nivel de protección acorde con el nivel de clasificación de confidencialidad y sensibilidad de los datos (por ejemplo, medios seguros de almacenamiento físico para la información en papel o cifrado de datos para la información digital).

- El RE 3.2.6 se corresponde con la fase 'Check' del PDCA. Requiere que se efectúe un seguimiento de la aplicación efectiva de los controles de seguridad (fase 'Do'), el cual deberá ir acompañado de una serie de actividades de registro del acceso a los sistemas y datos físicos y digitales y de su utilización. El RE 3.2.6 también requiere que se recabe información de otras fuentes, como de reportes de incidentes de seguridad o actividades de auditoría, para saber si los controles de seguridad están funcionando efectivamente en la práctica. Por último, requiere que se incorporen controles de seguridad en los procesos de cambio, y que exista algún tipo de función de auditoría interna y externa.

Los REs estructuran el contenido del RP 3.2 en esta guía, tal como indicado en la Tabla 2.

Como ayuda para aquellas administraciones tributarias que ya estén aplicando los estándares de la serie ISO/IEC 27000 o estándares equivalentes, en la Figura 2 se proporciona un mapeo general del RP 3.2 (sistema GSI) con el estándar ISO/IEC 27001.

PASOS CLAVE PARA LA IMPLEMENTACIÓN DE UN MARCO DE GSI

Como el objetivo de esta guía es ayudar a las administraciones tributarias de países en desarrollo a desarrollar su marco de GSI en línea con los estándares y mejores prácticas internacionales, en esta sección se ofrece una visión global de los pasos generales que son esenciales para adoptar ese marco. Posiblemente sea necesario reiterar este proceso a medida que el marco de GSI de la administración tributaria del país en desarrollo alcanza madurez.

Paso 1: Delimitar el alcance del marco de GSI

Las jurisdicciones pueden considerar dos enfoques para que el alcance de su marco de GSI les permita participar en el intercambio de información, en función del grado de madurez y la complejidad de las operaciones, sistemas de TI y controles de la seguridad de sus administraciones tributarias, y de las modalidades de intercambio de información en que estas participen (por ejemplo, intercambio automático (recíproco o no recíproco), previa petición o EOI espontáneo). Este aspecto se recoge en el RE 3.2.1.1 referido al ciclo de vida de la información:

- Desarrollar un marco de GSI que cubra la totalidad de las actividades de la administración tributaria y aplicarlo a la información intercambiada, o

- Desarrollar un marco de GSI centrado inicialmente en un perímetro seguro dedicado exclusivamente a las operaciones que manejan información intercambiada.

Tabla 2. **Estructura del RP 3.2 (marco GSI)**

Plan, Act	RE 3.2.1 Las organizaciones relevantes deben contar con un sistema de GSI global adecuado.	
Do	RE 3.2.2 Las organizaciones relevantes deben contar con controles adecuados de los recursos humanos.	RE 3.2.3 Las organizaciones relevantes deben contar con controles adecuados de acceso, tanto físico como lógico.
	RE 3.2.4 Las organizaciones relevantes deben contar con seguridad adecuada de los sistemas de TI.	RE 3.2.5 Las organizaciones relevantes deben proteger la información de forma adecuada.
Check	RE 3.2.6 Las organizaciones relevantes deben contar con un marco adecuado de gestión de las operaciones que incluya la gestión de incidentes, gestión del cambio, seguimiento y auditoría.	

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Paso 2: Definir una política de GSI

Una política de GSI documenta el compromiso de la alta dirección con una seguridad de la información sólida, incluida la información intercambiada. La política de GSI establece los principios rectores y los principales procesos, procedimientos y controles de seguridad de la información de la administración tributaria. Asigna las responsabilidades de alto nivel, compromete los recursos de la administración tributaria para la implementación y establece revisiones periódicas de la política. Como resultado de esas revisiones, pueden introducirse mejoras en la política de GSI que reflejen la madurez del marco de seguridad de la información de la administración tributaria.

Paso 3: Identificar los riesgos para la seguridad

La adopción de un marco y una política de GSI rigurosos comienza por la identificación sistemática de los riesgos para la seguridad de la información en poder de la administración tributaria. Por riesgo se entiende un escenario en la que una posible amenaza aprovecha una vulnerabilidad existente en un activo determinado. Se necesita, en particular, una percepción clara de cuáles son los activos clave implicados en el AEOI, además de una evaluación crítica de las amenazas y la vulnerabilidad relacionadas con esos activos.

Se debe llevar a cabo una evaluación del riesgo aplicando una metodología que permita identificar todos los riesgos que se derivan de las distintas amenazas y vulnerabilidades, para evaluar el impacto de esos riesgos y determinar qué controles de tratamiento se aplicarán a esos riesgos, es decir, cuáles son los controles necesarios para tratar los riesgos identificados en función de su impacto estimado. La gestión del riesgo para la seguridad de la información se aborda en detalle en el RE 3.2.1.4.

Paso 4: Establecer políticas, procesos y procedimientos específicos en los ámbitos relevantes

Una vez identificados los riesgos y decididos los controles que se usarán para tratarlos, la administración tributaria debe reflejar y documentar los controles que aplicará en las políticas, procesos y procedimientos de los ámbitos pertinentes. En el Recuadro 4 se ofrece una lista no exhaustiva de ejemplos de políticas de seguridad que pueden utilizarse.

Paso 5: Formar al personal

Todo el personal involucrado en GSI (y en el intercambio de información) debe recibir formación acerca de las políticas, procesos, procedimientos y controles establecidos para hacer frente a los riesgos para la seguridad, a fin de garantizar su debida aplicación.

Paso 6: Verificar la adopción efectiva del sistema de GSI

La administración tributaria debe verificar periódicamente si su personal está aplicando efectivamente el sistema de

FIGURA 2. **Mapeo general del RP 3.2 (marco GSI) con el estándar ISO/IEC 27001**

GSI, entendiendo por tal el conjunto de políticas, procesos, procedimientos y controles de seguridad en ámbitos específicos para implementar el marco de GSI (véase la definición de la Tabla 3 y la discusión en el RE 3.2.1.3), y si esos controles están surtiendo efecto en la práctica.

Las siguientes secciones de esta guía contienen recomendaciones para la aplicación de cada uno de los REs (REs 3.2.1 a RE 3.2.6) de un marco de GSI que se ajuste a los estándares internacionalmente reconocidos.

REQUISITO ESPECÍFICO 3.2.1: UN MARCO DE GSI INTEGRAL

El RE 3.2.1 establece que las administraciones tributarias deben definir un planteamiento global de GSI que incluya la estrategia, las políticas y la gestión del riesgo, es decir, definir las estructuras organizativas y los objetivos y principios generales de seguridad de la información que componen el marco de GSI. Este RE se corresponde con las fases 'Plan' y 'Act' del ciclo PDCA y constituye el requisito "integral" para la aplicación del sistema de GSI (término que alude, como se ha indicado ya, al conjunto de políticas, procesos, procedimientos y controles en ámbitos específicos que permiten implementar el marco de GSI). Un marco de GSI insuficiente puede resultar en problemas para abordar de manera efectiva los riesgos para la seguridad de la información.

El RE 3.2.1 se subdivide a su vez en seis RE:

- **RE 3.2.1.1**:como primer paso para garantizar la existencia de un sistema de GSI riguroso para el intercambio de información, es preciso que la administración tributaria tenga un entendimiento claro del ciclo de vida de la información intercambiada que maneja y que se comprometa a salvaguardar su confidencialidad y uso adecuado.
- **RE 3.2.1.2**: Tanto si el marco de GSI elaborado por una administración tributaria abarca todas sus operaciones como si abarca únicamente a las que manejan información intercambiada, su alta dirección debe estar plenamente comprometida con el marco general de seguridad. Ese compromiso suele expresarse en un documento escrito sobre la política de GSI.
- **RE 3.2.1.3**: La administración tributaria debe garantizar también que el marco de GSI esté integrado con los procesos de negocio relevantes y esté apoyado por medidas operativas y sistemas de GSI adecuados.
- **RE 3.2.1.4**: Un sistema de GSI sólido debe basarse en los riesgos y amenazas a que está expuesta la administración tributaria, a fin de evitar el uso inadecuado de recursos escasos y valiosos.
- **RE 3.2.1.5**: La administración tributaria debe definir y gestionar los escenarios de riesgo que podrían afectar la continuidad de sus procesos del negocio.

Recuadro 4. **Lista no exhaustiva de políticas de seguridad en distintos ámbitos**

Una política es una declaración documentada de una administración tributaria en relación con la implementación de procesos, procedimientos y controles en un ámbito determinado, como por ejemplo:

- Política de continuidad del negocio (RE 3.2.1.5)
- Política de seguridad de los recursos humanos (RE 3.2.2)
- Política de gestión de accesos (RE 3.2.3):
  - Política de acceso físico (REs 3.2.3.1 y 3.2.3.2)
  - Política de acceso lógico (REs 3.2.3.3 y 3.2.3.4)
- Política de seguridad de TI (RE 3.2.4.2):
  - Política de protección frente a *malware*
  - Política de registro y seguimiento
- Política de gestión de activos (RE 3.2.4.3)
- Política de clasificación de la información (RE 3.2.5)
- Política de "escritorio limpio/despejado" (RE 3.2.5)
- Política de criptografía (RE 3.2.5)
- Política de gestión del cambio (RE 3.2.6.5)
- Política de gestión de incidentes (RE 3.2.6.6)

En la Tabla 3 se definen los principales conceptos utilizados en el RE 3.2.1.

RE 3.2.1.1. Conocer bien el ciclo de vida de la información intercambiada y comprometerse a garantizar su confidencialidad y un uso adecuado

La finalidad de las evaluaciones de la confidencialidad es determinar si una administración tributaria está en condiciones de recibir un tipo específico de información sobre los contribuyentes, es decir, los datos intercambiados en aplicación del Estándar AEOI. De ahí que el RE 3.2.1 haga referencia en primer lugar a las expectativas que tienen las administraciones tributarias con respecto a la gestión de los distintos tipos de datos que comúnmente se intercambian con otras administraciones tributarias, de conformidad con los acuerdos internacionales de intercambio de información.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Tabla 3. **Glosario de principales conceptos**

Concepto	Descripción
Activo	Todo elemento de valor involucrado en el desarrollo de procesos y en la generación de resultados. Los activos pueden ser información, personas, servicios, equipos, sistemas, etc.
Gestión de la continuidad del negocio	Proceso de gestión dirigido a asegurar la continuidad de las operaciones en el escenario de un evento que altere su curso normal.
Seguridad de la información	Se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información.
Riesgo para la seguridad de la información	Posibilidad de que una amenaza determinada explote vulnerabilidades de un activo o un grupo de activos, causando un perjuicio a la organización.
Marco GSI	Un marco de GSI comprende las estructuras organizativas y los principios generales sobre seguridad de la información, que guían a las administraciones tributarias para alcanzar sus objetivos en GSI, siguiendo un enfoque basado en riesgos. La responsabilidad última sobre el marco GSI debe recaer en los funcionarios de mayor jerarquía dentro de la administración tributaria.
Política GSI	Una política de GSI expresa la postura de la administración tributaria sobre la forma en cómo plantea la seguridad de la información. La política de GSI debe establecer el alcance del sistema de GSI y los objetivos generales de gestión de la seguridad de la información a los que habrán de ajustarse todas las demás políticas específicas.
Sistema GSI	Por sistema de GSI se entiende el conjunto de políticas, procedimientos y controles en ámbitos específicos que permiten implementar el marco de GSI. La responsabilidad última sobre el sistema de GSI debe recaer en los funcionarios de seguridad con mayor jerarquía dentro de la administración tributaria.
Nomenclaturas	Reglas que establecen cómo debe designarse la información para que sea claramente identificable.
Política	Una política es una declaración documentada de la administración tributaria en relación con la implementación de procesos, procedimientos y controles en un ámbito determinado. Una política responde a la pregunta "¿qué se debe hacer?". Debe existir una jerarquía entre las políticas. Por ejemplo, una política sobre identificación y autenticación para el acceso a los sistemas de TI estará subordinada a la política global sobre la gestión del acceso. También debe existir una política de GSI general en la que se enumeren los principios generales de seguridad aplicables a todas las políticas.
Prácticas o controles	Un control o una práctica es una medida específica utilizada para gestionar el riesgo para la seguridad de la información (es decir, para mitigar o eliminar el riesgo). Los controles pueden ser procesos y procedimientos, así como programas, herramientas, técnicas, tecnologías y dispositivos. En ocasiones, los controles también se denominan como salvaguardas o contramedidas en relación con un riesgo identificado.
Procedimiento	Un procedimiento es una serie documentada de pasos y actividades para implementar políticas de seguridad. Un procedimiento responde a la pregunta "¿cómo se debe hacer y quién lo hace?". El término procedimiento suele aparecer asociado al término proceso – procesos y procedimientos –, porque un procedimiento suele ser una representación más detallada de cada uno de los pasos de un proceso. Con frecuencia, puede haber más de un procedimiento para cada paso de un proceso. Por ejemplo, un proceso puede referirse a la presentación de una declaración de impuestos; pero como pueden existir distintas formas de realizar esa presentación, existirán procedimientos diferentes para cada forma de presentación.
Proceso	Un proceso es una secuencia repetible de acciones con un resultado medible. El concepto de proceso es crucial en la GSI. Medir los resultados y actuar en función de ellos constituye la base para mejorar los procesos y la seguridad. Un proceso puede ser de cualquier tipo, desde un proceso tributario, como la presentación y la evaluación de declaraciones de impuestos, hasta la actualización de programas informáticos. Toda acción que no forme parte de un proceso determinado representa por definición un riesgo para la seguridad, ya que no hay garantía de repetibilidad ni de que se midan y mejoren sus resultados.
Mitigación del riesgo	Consiste en adoptar activamente medidas para reducir el impacto o la probabilidad de que se produzca un riesgo.
Vulnerabilidad	Deficiencia en el diseño o en la naturaleza de un activo o debilidad derivada de la falta de mantenimiento de un activo.

El enfoque propuesto en el RE 3.2.1.1 es el del ciclo de vida. El RE 3.2.1.1 se ocupa principalmente de garantizar que los datos en poder de las administraciones tributarias, incluida la información intercambiada, se encuentren protegidos durante todo su ciclo de vida, entendiendo por tal los distintos procesos y sistemas de manejo, almacenamiento y utilización por los que pasan los datos desde el momento en que se reciben en una administración tributaria y hasta su eliminación (véase la Figura 3).

El enfoque del ciclo de vida de la información también se aborda en el RE 3.2.5, que trata de los controles necesarios para proteger todos los tipos de información que maneja una administración tributaria. No obstante, a efectos de las evaluaciones de confidencialidad, el RE 3.2.1.1 se centra exclusivamente en la categoría de la información intercambiada, que está sujeta a controles confidencialidad específicos impuestos por acuerdos internacionales de intercambio de información.

FIGURA 3. **Ciclo de vida de la información intercambiada**

Durante cada una de las fases del ciclo de vida de la información, las administraciones tributarias deben implementar controles de seguridad específicos, con un entendimiento claro de qué sistemas de TI, departamentos, instalaciones y personal de las distintas áreas de la administración tributaria intervendrán a lo largo de ese ciclo.

La selección de los controles que se implementarán durante ese ciclo de vida dependerá en gran medida de la forma en que se practique el intercambio de información y de los riesgos al EOI identificados por la administración tributaria. A lo largo de esta guía se describen distintos controles, y las administraciones tributarias deberán aplicarlos de la forma que les sea relevante y que se adapte mejor a sus circunstancias. Se recomienda documentar estos controles del ciclo de vida para garantizar su aplicación consistente.

Los controles del ciclo de vida de la información incluyen los siguientes:

- La nomenclatura y las clasificaciones de la confidencialidad utilizadas para identificar claramente la información intercambiada, entendiendo por tal no solo la que se intercambie bajo el Estándar AEOI, sino también la intercambiada previa petición y de forma espontánea, así como otros tipos de información relevantes, como los Reportes País-por-País y las resoluciones en materia tributaria intercambiadas bajo los estándares de transparencia en el ámbito BEPS.
- Los arreglos de almacenamiento, es decir, dónde y cómo se almacena la información, así como una visión general de los controles empleados para protegerla.
- Los procesos para el uso de la información para los fines autorizados y para prevenir el acceso no autorizado.
- Los arreglos de registro para asegurar que se mantengan registros apropiados del acceso a los datos.
- Los arreglos para el archivo y eliminación de la información cuando deje de necesitarse o expire su período de retención (si lo hubiera).

La Tabla 4 muestra un ejemplo simplificado de un enfoque de controles a lo largo del ciclo de vida de la información intercambiada bajo los estándares AEOI y EOIR.

El enfoque predeterminado del Foro Global al realizar evaluaciones de confidencialidad es que las administraciones tributarias aplican a la información intercambiada los mismos controles de seguridad que utilizan para sus operaciones en general, con controles adicionales específicos para la información intercambiada según corresponda.

No obstante, para los países en desarrollo la implantación de un sistema de GSI en todas las operaciones de la administración tributaria puede estar aún por concluir y representar un costoso esfuerzo a largo plazo. Por ello, es posible que a las administraciones con menor experiencia en materia de GSI y TI no les baste con introducir mejoras de los controles generales de la seguridad en el conjunto de la organización para poder participar en las iniciativas AEOI en los plazos previstos en sus compromisos internacionales y acuerdos de intercambio.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Tabla 4. **Ejemplo de controles generales durante el ciclo de vida de la información intercambiada mediante AEOI y EOIR**

Fase del ciclo de vida	Datos AEOI	Datos EOIR
Arreglos de acceso y registro	Se establecen y aplican controles para que únicamente tengan acceso los usuarios autorizados. Todos los accesos a la base de datos de AEOI se registran y guardan.	Se establecen y aplican controles para que únicamente tengan acceso los usuarios autorizados. Todos los accesos a la base de datos de EOIR o a los gabinetes o sala de archivo donde se guarden los datos de EOIR se registran y guardan.
Archivo y eliminación de la información	Los datos AEOI se eliminan de forma segura cuando ya no se necesitan. Si los datos ya no se necesitan pero no ha expirado su plazo de retención, se archivan en condiciones seguras hasta que expire ese plazo y puedan eliminarse.	Los datos EOIR se eliminan en condiciones seguras cuando ya no se necesitan. Si los datos ya no se necesitan pero no ha expirado su plazo de conservación, se archivan en condiciones seguras hasta que expire ese plazo y puedan eliminarse.
Clasificación y etiquetado	Los datos AEOI son clasificados como confidenciales y etiquetados en consonancia.	Los datos EOIR son clasificados como confidenciales y etiquetados en consonancia.
Manejo y utilización	Los datos AEOI se utilizan exclusivamente cuando lo requieran las operaciones tributarias y de conformidad con los acuerdos de intercambio.	Los datos EOIR se utilizan exclusivamente cuando lo requieran las operaciones tributarias y de conformidad con los acuerdos de intercambio.
Arreglos de almacenamiento	Los datos AEOI se segregan de las bases de datos que contienen otro tipo de información.	Los datos EOIR recibidos en formato digital se segregan de las bases de datos que contienen otro tipo de información. Los datos EOIR recibidos en papel se almacenan de forma segura en gabinetes cerrados o en salas de archivo a los que únicamente tiene acceso el personal autorizado.

Por ello, las administraciones tributarias de los países en desarrollo pueden considerar dar prioridad al desarrollo de controles rigurosos del ciclo de vida de la información intercambiada, elaborando un marco de GSI centrado inicialmente en un 'perímetro seguro' dentro del cual se llevan a cabo las actividades relacionadas con el intercambio de información, tales como el cotejo de datos, el análisis de riesgos, la selección de casos y la auditoría (véase el Recuadro 5).

El Foro Global puede proporcionar a las jurisdicciones que lo soliciten orientación detallada sobre cómo implementar un perímetro seguro.

RE 3.2.1.2. Política de GSI, liderazgo y compromiso y marco organizativo

El RE 3.2.1.2 requiere que las administraciones tributarias gestionen la seguridad de la información por medio de un documento de política de GSI que forme parte de un marco global de seguridad con funciones y responsabilidades claramente definidas, cuente con el respaldo de la alta gerencia y se mantenga actualizado.

Este RE se refiere a la importancia fundamental que reviste el liderazgo estratégico para garantizar la efectividad de la GSI. Un elemento clave es el compromiso de los alta gerencia de la administración tributaria con la seguridad de la información y su apoyo inequívoco a la asignación de recursos y fondos para la planificación y ejecución de la GSI.

Si los altos cargos otorgan prioridad a la seguridad de la información y demuestran su compromiso personal con la consecución de los objetivos del sistema de GSI, el resto del personal de todos los niveles de la administración tributaria seguirá su ejemplo.

Por el contrario, si los responsables establecen que los objetivos en materia de seguridad pueden sacrificarse, entonces la seguridad será comprometida. Aunque la concepción de un enfoque de GSI constituye un esfuerzo colectivo organizado y dirigido por los especialistas en operaciones tributarias, es importante que la alta gerencia marque el rumbo general.

Los elementos clave del liderazgo y compromiso con la GSI en la administración tributaria son:

- Objetivos GSI
- Política GSI
- Definición clara de las funciones, responsabilidades y autoridades respecto del sistema de GSI

Recuadro 5. **Un perímetro seguro para la información intercambiada**

¿Qué es un perímetro seguro?

Por perímetro seguro se entiende un entorno físico y/o virtual altamente seguro dentro de una administración tributaria (y, por tanto, adecuadamente protegido de acuerdo con los estándares relevantes) que permitiría a las jurisdicciones recibir, proteger y manejar la información intercambiada de forma automática, espontánea o previa petición, mientras que se realizan esfuerzos de más largo plazo para implementar los estándares internacionales de GSI en el conjunto de la administración tributaria. Se trata de un enfoque táctico que puede implementarse a un menor costo y en plazos más breves que si se implementaran los controles de seguridad necesarios en todas las operaciones.

Un perímetro seguro implica que las administraciones tributarias gestionan y controlan el ciclo de vida de la información intercambiada manteniendo un alto grado de separación entre esta y los demás procesos, tecnología, personal y conjuntos de datos que ya se utilizan en las operaciones tributarias internas. En principio, requeriría contar con una unidad organizativa segura dentro de la administración, en la que puedan adoptarse mecanismos de control de la seguridad más estrictos para cumplir con las estrictas demandas de los acuerdos de intercambio, de los socios de intercambio y de los estándares del Foro Global (por ejemplo, una oficina situada en el edificio de la sede central o un edificio propio).

En la práctica, significa que la administración tributaria únicamente manejaría y utilizaría los datos recibidos de sus socios de intercambio dentro de ese perímetro seguro. Tendrían que asignarse los recursos tecnológicos, físicos y humanos necesarios para procesar la información intercambiada dentro de ese perímetro, así como para realizar dentro del perímetro el cotejo de datos, evaluaciones de riesgo, revisiones, auditorías y otras actividades de cumplimiento.

¿Cómo implementar un perímetro seguro?

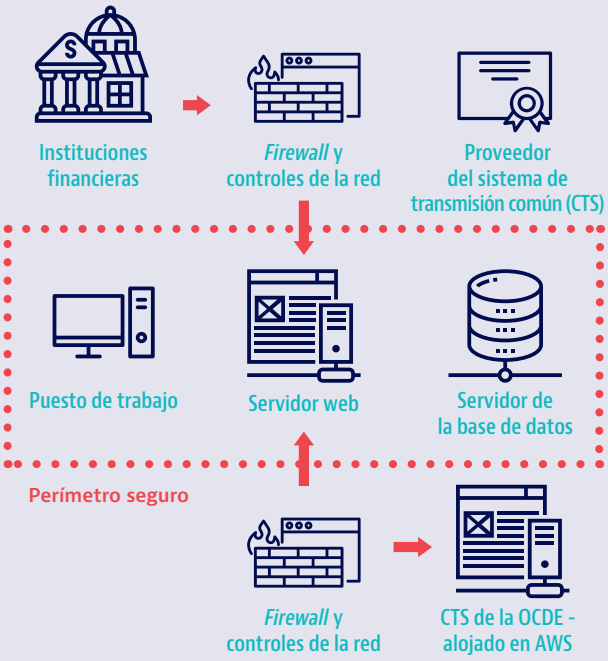
A la hora de decidir la implementación de un perímetro seguro, la administración tributaria debería empezar estudiando su mejor encaje posible dentro de las estructuras operativas que ya existen. Por ejemplo, si una administración tributaria tiene ya una unidad organizativa interna relativamente más segura para llevar a cabo las operaciones especialmente delicadas (por ejemplo, una unidad de contribuyentes con grandes fortunas o un edificio especialmente seguro situado en la capital), sería posible asignar a esa unidad el manejo y la utilización de la información intercambiada.

Otra opción sería analizar cómo el trabajo relativo a la información intercambiada se asigna a las operaciones que se vienen desarrollando ya. Por ejemplo, si existe una única unidad organizativa que se ocupa de los grandes contribuyentes y fortunas, puede ser recomendable integrar el perímetro seguro en esa unidad, ya que con toda probabilidad esos serán los contribuyentes a los que haga referencia la información que se reciba de los socios de intercambio.

Algunos de los elementos clave para la implementación de un perímetro seguro incluyen:

- Instalación de uno o varios ordenadores utilizados en exclusiva para acceder a la información recibida mediante el EOI.
- Controles especiales de seguridad para el acceso físico a las dependencias, tales como tornos de acceso activados mediante tarjeta, circuito cerrado de televisión en esa área (CCTV), acceso limitado a una sola persona en cada momento, alarmas, etc.
- Medidas adecuadas de formación y sensibilización del personal que vaya a trabajar con la información intercambiada dentro del perímetro seguro, por ejemplo, los inspectores fiscales.
- Establecimiento de una estructura, una política y unos procesos globales de gobernanza de GSI aplicables al perímetro seguro que cuenten con el respaldo de los máximos responsables de la administración tributaria.
- Adquisición, producción y entrega de unos controles mínimos de TI para los sistemas empleados para procesar y utilizar la información intercambiada, incluidos los siguientes: documento de diseño del sistema y plan de controles, controles gateway, segmentación de la red interna, listas blancas, gestión y autenticación del acceso, limitación del acceso del personal y del acceso a ordenadores, registro centralizado de las auditorías, gestión del cambio, cifrado de las comunicaciones, gestión del riesgo y exploración de vulnerabilidad.

A continuación se ofrece, con fines exclusivamente ilustrativos, un ejemplo de la arquitectura de red de un perímetro seguro.



Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Objetivos GSI

Las administraciones tributarias tienen que definir claramente los objetivos del sistema de GSI y de lo que se espera conseguir. En función del grado de madurez o la escala de las operaciones de la administración tributaria, la planificación y fijación de objetivos puede llevarse a cabo a distintos niveles. Los objetivos de GSI pueden ser definidos como parte de la planificación estratégica de la administración tributaria, como parte de la estrategia de TI o, idealmente, como parte de una estrategia específica de seguridad de la información.

Con independencia de cómo se definan los objetivos de GSI, estos deben ser apoyados mediante el compromiso de recursos y fondos para su consecución y con una atribución clara de las responsabilidades respecto de cada uno de los objetivos y actividades.

Los objetivos clave de GSI de las administraciones tributarias deberían ser:

- Proteger la información sensible que posean sobre los contribuyentes y otros activos de información relevantes, de manera consistente con las normas internas sobre confidencialidad de la información y protección de datos y con los compromisos de confidencialidad derivados de los tratados internacionales.
- Mitigar los riesgos para la seguridad de la información mediante controles de seguridad y medidas de acceso proporcionales a esos riesgos, permitiendo al mismo tiempo que los usuarios (el personal) tengan acceso a la información que necesiten para el correcto desempeño de sus funciones.
- Establecer la obligación del personal de informar sobre incidentes de seguridad, fomentando un ambiente de trabajo abierto y positivo en el que los miembros del personal se muestren dispuestos a reconocer sus errores y a participar en el esfuerzo colectivo por mejorar constantemente la seguridad de la información (PDCA).
- Establecer sistemas de reporte e instrumentos efectivos de medición y revisión (con datos precisos y seguros) para verificar si se están alcanzando los objetivos y si los controles que les sirven de apoyo funcionan en la práctica.

Política de GSI

La manera en que los objetivos de GSI se comunican al personal de la administración tributaria es ante todo a través de una política global de GSI.

Recuadro 6. **Ejemplo de la estructura general de una política de GSI**

Una política de GSI puede tener distinto niveles de detalle, pero en general podría tener la estructura siguiente:

- Declaración de propósito: por qué existe una política de GSI.
- Descripción de la audiencia objetivo: quiénes tienen que leerlo y a quiénes se aplica. Puede tratarse de audiencias internas y externas, por ejemplo, personal de la administración tributaria y proveedores de servicios de TI.
- Estrategia de la organización respecto a los objetivos y principios de GSI: proteger la confidencialidad e integridad de la información, asegurando al mismo tiempo que se garantiza su disponibilidad para el personal que la necesite en el desempeño de sus funciones.
- Panorama general de las áreas clave y los principios de seguridad, con referencias generales a las políticas específicas. Aunque la política de GSI establece el marco global de la seguridad de la información, deberá exponer como mínimo el criterio que se seguirá en las áreas siguientes:
  - Seguridad de TI.
  - Seguridad física.
  - Seguridad en materia de recursos humanos
  - Gestión de la continuidad de las operaciones del negocio.
- Funciones y responsabilidades clave, que incluyan arreglos sobre mecanismos de reporte, procesos de escalamiento y medición de resultados.
- Autoridad competente de la revisión: quién aprueba y revisa la política de GSI y con qué periodicidad.

Habitualmente las administraciones tributarias tienen políticas específicas para diferentes materias, como por ejemplo para la gestión de los recursos humanos, el acceso físico a las instalaciones y el acceso lógico a los sistemas de TI, la utilización de los equipos de TI o las vulnerabilidades. Estas políticas específicas suelen ser gestionadas por diferentes áreas organizativas dentro de la administración tributaria, lo que puede conducir a una falta de coherencia entre políticas.

Por lo tanto, es una buena práctica establecer una política global de GSI que refleje la forma en que la administración tributaria concibe la seguridad de la información. La política de GSI debería definir el alcance del sistema de GSI y los objetivos generales de gestión de la seguridad de la información (esbozados en la sección anterior) a los que han de ajustarse las demás políticas específicas.

La política de GSI debe reflejar también el compromiso de la alta dirección de asignar los recursos necesarios para la consecución de sus objetivos de seguridad. En el Recuadro 6 se ofrece un ejemplo de la estructura general de una política GSI.

La alta gerencia de la administración tributaria debe asegurarse de que el personal (incluidos los contratistas externos) esté informado de la política de GSI y de su contenido, para lo cual se recomienda llevar a cabo un programa integral de comunicación y formación. La formación y la sensibilización en cuestiones de seguridad se abordan en detalle en el RE 3.2.2, referido a los mecanismos de control en el ámbito de los recursos humanos.

Principales funciones y responsabilidades en materia de GSI

Por medio de la política GSI, la alta gerencia de la administración tributaria debe asignar responsabilidades claras en materia de GSI a todo el personal comprendido en el ámbito de aplicación de la misma, y al menos a las siguientes personas o grupos:

- Persona clave responsable de la seguridad de la información.
- Alta dirección de las áreas comprendidas en la política GSI.
- Jefe del departamento de TI.
- Personal del departamento de TI.
- Auditoría interna

La persona clave responsable de la seguridad de la información suele denominarse Oficial de Seguridad de la Información (OSI), pero puede recibir una denominación diferente en función de la estructura organizativa y la cultura de la administración tributaria.

En general, es aconsejable que el OSI tenga una línea de reporte directa a los alta gerencia de la administración tributaria, así como que forme parte del departamento de TI. El motivo es que el OSI debería ser responsable de los controles y políticas en ámbitos de seguridad diversos, en toda una serie de procesos que no solo pertenecen al área de las TI (seguridad física, recursos humanos, auditoría interna, etc.). El Recuadro 7 contiene un esbozo de las competencias y funciones recomendadas para el OSI.

Conviene delimitar claramente las funciones y responsabilidades entre el personal de TI y el personal de la seguridad de la información. Además, deben establecerse líneas claras de comunicación entre ellos. El personal de TI debería centrarse en la implementación y funcionamiento efectivos de los sistemas de TI y la integración de los aspectos de seguridad en su desarrollo, según lo definido en las políticas. Las administraciones tributarias deben documentar con claridad en un organigrama las líneas jerárquicas y las líneas de reporte entre el personal de TI y el personal de seguridad.

Recuadro 7. **Competencias y funciones del Oficial de Seguridad de la Información**

¿Qué cualificaciones y experiencia debe poseer?

El OSI debe poseer una combinación de habilidades técnicas y organizativas, un conocimiento claro del área de la seguridad de la información y tener experiencia en diversos ámbitos de la seguridad. El OSI debe ser una persona habituada a la discusión de cuestiones técnicas y debe comprender las exigencias operativas, regulatorias y jurídicas asociadas a la seguridad.

Las cualificaciones específicas del OSI pueden depender de la escala de las operaciones de la administración tributaria, pero el requisito clave más importante es su creencia en la importancia de garantizar la seguridad y de comunicarla a los demás.

En las administraciones tributarias más pequeñas, el OSI puede ser una persona de la propia administración tributaria con sólidos conocimientos de seguridad y de TI. En las administraciones tributarias de mayores dimensiones puede ser necesario contar con equipos de múltiples especialistas para cada área del negocio, en cuyo caso el OSI podría requerir un conjunto de competencias que tal vez no se encuentren disponibles dentro de la propia administración tributaria.

¿Dónde debería situarse el puesto de OSI dentro de la estructura de la organización? ¿Cómo debe gestionarse?

Como principal encargado de la seguridad, el OSI debería tener contacto directo con la jefatura de la administración tributaria. Sus funciones pueden esbozarse en Términos de Referencia o descripción del puesto de trabajo aprobado por la jefatura de la administración tributaria, en el que se determine, entre otros aspectos, cuáles son los principales resultados en materia de seguridad que deben lograrse, qué tipo de informes debe presentar y con qué periodicidad.

En función del tamaño de la administración tributaria, el OSI puede apoyarse en un equipo propio para el desempeño de las funciones y actividades comprendidas en su ámbito de competencia.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

RE 3.2.1.3. Sistema GSI

El RE 3.2.1.3 requiere que las administraciones tributarias aborden la seguridad de la información por medio de medidas operativas adecuadas y como parte integrante de la gestión de las operaciones de negocio relevantes. En resumen, esto significa tener un sistema de GSI integrado con las operaciones del negocio.

Tal y como se indica en la Tabla 3, el marco de GSI se refiere a las estructuras organizativas y los principios generales sobre seguridad de la información que guían a las administraciones tributarias para alcanzar sus objetivos de GSI, mientras que el sistema de GSI es el conjunto de políticas, procedimientos y controles en ámbitos específicos que se requieren para implementar el marco de GSI.

Tanto el tamaño de la administración tributaria como la complejidad de sus operaciones y el grado de madurez de sus sistemas de TI son factores que influirán en el grado de detalle del sistema de GSI (véase la Figura 4).

FIGURA 4. **Componentes del marco de GSI y del sistema de GSI**

Los componentes del sistema de GSI deben desarrollarse tomando como base las evaluaciones de la gestión de riesgos llevadas a cabo por la administración tributaria. La gestión de riesgos se examina en detalle en el RE 3.2.1.4.

El sistema de GSI puede representarse en un documento general (como un manual) que contenga los distintos grupos de políticas, procedimientos y controles relativos a un ámbito específico. Las administraciones tributarias pueden tomar como ejemplo esta estructura para su documento sobre el sistema GSI:

- Introducción.
- Ámbito de aplicación del sistema GSI.
- Organigrama, funciones y responsabilidades, y procedimientos de reporte entre las partes interesadas.
- Política de GSI.
- Principales procesos de GSI.
- Enfoque seguido para la gestión de riesgos, junto con los riesgos identificados.

Recuadro 8. **Ejemplo de política de un ámbito específico de la seguridad en el contexto del marco y el sistema de GSI**

Marco de GSI. Objetivo: Proteger información sensible sobre los contribuyentes y otros activos de información relevantes.

Sistema y política de GSI. Política para la protección de los datos de AEOI en poder de la administración tributaria, en consonancia con la evaluación de riesgos efectuada respecto de ese activo de información. Todos los accesos a los sistemas y bases de datos de AEOI se someten a un estricto control por medio del empleo de contraseñas complejas.

Aplicación de una política de contraseñas como control. En el directorio activo, la política de grupo para el sistema en que está archivada la información de AEOI se configura del siguiente modo: las contraseñas deben tener un mínimo de 15 caracteres y deben cambiarse cada 180 días. No se puede repetir ninguna de las 10 últimas contraseñas, y no pueden revelarse en ninguna forma y por ningún medio. Se instruye al personal acerca del uso de las contraseñas.

Aplicación de una política de contraseñas como procedimiento. El OSI es el responsable de garantizar que la política de contraseñas se aplica y se hace cumplir en todos los sistemas y bases de datos de AEOI. Cuando se desarrollen sistemas, se consultará al OSI para garantizar la correcta aplicación de esta política. El OSI coordinará con los especialistas de TI (normalmente administradores de sistemas) para cerciorarse de que la política se esté aplicando y funcione correctamente. En caso de que la política no se esté aplicando en forma adecuada, se adoptarán medidas correctoras (por ejemplo, mejorar las instrucciones impartidas al personal.). El OSI realizará comprobaciones ocasionales para asegurarse de que el personal comprende la política y la aplica correctamente. El OSI colaborará estrechamente con aquellos trabajando en operaciones de seguridad para establecer si los controles operativos, tales como registros, seguimiento o gestión de incidentes, están detectando problemas o deficiencias en la aplicación de la política de contraseñas.

- Políticas previstas en un determinado ámbito de la seguridad para hacer frente a los riesgos identificados (con referencia a procedimientos y controles específicos). Existen varios ámbitos generales de seguridad de la información y, para fines de las evaluaciones de la confidencialidad, las administraciones tributarias deben abordar los siguientes en sus sistemas de GSI:
  - Recursos humanos (RE. 3.2.2)
  - Gestión del acceso (RE 3.2.3)
  - Seguridad de las TI (RE 3.2.4)
  - Protección de la información (RE 3.2.5), y
  - Gestión de las operaciones (RE 3.2.6).
- Enfoque para el control de las políticas documentadas del sistema de GSI.
- Enfoque para la auditoría interna del sistema de GSI.
- Periodicidad de revisión del sistema de GSI.

En el Recuadro 8 se muestra un ejemplo simplificado de cómo una política en un ámbito específico de la seguridad puede organizarse en el contexto del marco y el sistema de GSI.

RE 3.2.1.4. Gestión de riesgos para la seguridad de la información

Como los recursos humanos y financieros de las administraciones tributarias son limitados, una buena práctica consiste en diseñar el sistema GSI tomando como base una evaluación de los riesgos para la seguridad a que está expuesta la administración tributaria, a fin de asignar de forma eficiente esos recursos limitados.

El RE 3.2.1.4 requiere que las administraciones tributarias gestionen de manera sistemática los riesgos para la seguridad de la información a que están expuestas, teniendo en cuenta las amenazas, las vulnerabilidades y los impactos.

Bajo los estándares internacionales sobre gestión de riesgos, como ISO31000 e ISO27005[12], los riesgos para la seguridad de la información pueden definirse como el "potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos, causando un perjuicio a la organización".

12. www.iso.org/iso-31000-risk-management.html y www.iso.org/standard/75281.html.

Las administraciones tributarias deben disponer de un proceso riguroso y exhaustivo de gestión del riesgo, reflejado en una metodología de gestión de riesgo. En esta deben esbozarse las fases del proceso de gestión del riesgo, las responsabilidades específicas respecto de cada una de ellas y los criterios empleados para evaluar los riesgos.

Las administraciones tributarias pueden tener una metodología específica de gestión del riesgo para el sistema de GSI o bien optar por una metodología que ya estén siguiendo en otros ámbitos de su actividad y aplicarla al sistema de GSI. Si eligen esta última vía, es importante adaptar los criterios a la seguridad de la información.

En general, la metodología de gestión del riesgo para la seguridad de la información sigue las fases indicadas en la Tabla 5. No obstante, los detalles de la misma tienen únicamente fines referenciales y se alienta a las administraciones tributarias a que utilicen la metodología que mejor se adapte a sus respectivas organizaciones.

La gestión del riesgo es un proceso continuo, por lo que los riesgos deben revisarse y evaluarse a intervalos regulares. Especial importancia reviste el seguimiento periódico de la efectividad de los controles de mitigación del riesgo. Cuando se produzca un escenario de riesgo, las administraciones tributarias deberán iniciar el procedimiento de gestión de incidentes, descrito en detalle en el RE 3.2.6.6.

Es crucial que el personal de la administración tributaria tenga conocimiento de los principales riesgos para la seguridad de la información y que estos se comuniquen como parte de un programa de sensibilización o de otras actividades formativas llevadas a cabo por la administración tributaria.

Las administraciones tributarias pueden documentar el resultado del ejercicio de evaluación del riesgo en un registro de riesgos u otra herramienta que utilicen en apoyo de sus actividades de evaluación del riesgo. En la Tabla 6 figura un modelo de registro de riesgos con ejemplos de los grupos de activos "recursos humanos" y "activos de información", basado en la metodología esbozada en la Tabla 5.

Este registro de riesgos es solo para fines ilustrativos. Las administraciones tributarias pueden optar por crear registros de riesgos diferentes para cada grupo de activos, para áreas TI o no TI, o bien utilizar un registro centralizado. Se recomienda seguir el criterio que mejor se adapte a la organización propia.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Tabla 5. **Modelo de metodología de gestión del riesgo basada en las pautas de la serie ISO27000**

Fase	Descripción	Resultado
1. Identificación de activos	Elaborar un inventario de los principales activos de la organización identificando a su titular. El titular de un activo es la persona responsable de su gestión y utilización. Los activos pueden ser muy diversos según el alcance de la evaluación. Por ejemplo, en una evaluación integral del riesgo para AEOI únicamente se considerarán como activos los procesos de negocio y los sistemas relacionados con el AEOI. Si la evaluación de riesgos se refiere únicamente a los sistemas de TI, se identificarán como activos los componentes específicos de los sistemas de TI (equipos y programas informáticos).	**Categorías de activos pueden incluir:** • Procesos de negocio • Recursos humanos • Activos de información • Imagen y reputación • Programas informáticos • Equipos informáticos • Otros activos físicos • Servicios sub-contratados • Servicios de apoyo interno
2. Valoración de los activos	Llevar a cabo una valoración de los activos en función de su importancia para la administración tributaria y para la consecución de sus objetivos de seguridad de la información.	**Posible valoración de los activos:** **1.** Muy poco importante **2.** Poco importante **3.** Medianamente importante **4.** Bastante importante **5.** Muy importante
3. Determinación de escenarios de riesgo	Esta fase puede dividirse en: • Identificación de amenazas y vulnerabilidades de los activos, o posibles escenarios de riesgo. • Evaluación de la probabilidad de que se produzca el escenario de riesgo.	**Probabilidad de que suceda un escenario de riesgo:** **1.** Rara probabilidad de que suceda **2.** Poco probable que suceda **3.** Posibilidad moderada de que suceda **4.** Es probable que suceda **5.** Es casi seguro que sucederá
4. Evaluación del impacto	Evaluar el impacto sobre la confidencialidad, la integridad y la disponibilidad de la información y/o sobre los objetivos de seguridad, en caso de que se produzca el escenario de riesgo.	**Valores de impacto propuestos:** **0.** Ningún impacto **1.** Escaso impacto **2.** Mediano impacto **3.** Gran impacto
5. Valoración del riesgo	Valorar el riesgo. Se puede utilizar una fórmula sencilla que tome en consideración el valor del activo, la probabilidad de que se produzca el escenario de riesgo y el valor del impacto.	**Fórmula de valoración del riesgo:** valor del activo * probabilidad de escenario de riesgo * valor del impacto
6. Definición del nivel de riesgo aceptable	Definir el nivel de riesgo aceptable sobre la base de la importancia de los activos, los requisitos legales internos o las obligaciones derivadas de los tratados. Por riesgo aceptable se entiende un riesgo cuyas consecuencias, en caso de materializarse, están dispuestos a asumir los responsables de la administración tributaria. Usualmente, en el caso de estos riesgos el coste de poner en práctica un control de mitigación pesa más que los beneficios de adoptar ese control. No obstante, aun cuando se defina un riesgo como "aceptable", siempre debe efectuarse un seguimiento del mismo, ya que los riesgos pueden cambiar y evolucionar. Si cambiaran las exigencias del negocio o los recursos disponibles, podría modificarse la decisión sobre el carácter aceptable de los riesgos.	Esta decisión habrá de documentarse y revisarse a intervalos regulares.
7. Tratamiento del riesgo	Identificar los controles adecuados de tratamiento del riesgo.	**Opciones de tratamiento del riesgo:** • Aceptación del riesgo: no se adopta control específico alguno, por ejemplo, no se aplica ningún cifrado a determinados datos cuando no se están utilizando. No obstante, se efectúa un seguimiento del riesgo. • Mitigación del riesgo: se aplican controles para reducir la probabilidad de que el riesgo ocurra, por ejemplo, uso de firewalls y cifrado para proteger una base de datos. • Evitación del riesgo: el servicio o aplicación afectados por el impacto son completamente inhabilitados, reduciendo con ello la probabilidad a cero, por ejemplo, no conectando un sistema a Internet para evitar ataques de piratería. • Transferencia del riesgo: un riesgo determinado pasa a ser gestionado por otra entidad (por ejemplo, un ciberseguro para accesos no autorizados a los datos). Esta opción únicamente se recomienda para mitigar el impacto económico de un riesgo, por lo que debería utilizarse en casos muy limitados.
8. Seguimiento y reevaluación del riesgo	Sobre la base del seguimiento periódico de la aplicación de controles, la auditoría interna y otros procesos de revisión, actualizar el proceso de gestión del riesgo y sus resultados.	El intervalo recomendado para las revisiones es de un año, o cuando se produzca un cambio importante en el entorno.

Tabla 6. **Modelo de estructura de un registro de riesgos**

Grupo de activos	Activo	Valor del activo (1-5)	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia (1-5)	Valor del impacto (0-3)	Valoración del riesgo (valor del activo* probabilidad* impacto)	Controles elegidos si se requiere tratamiento
Recursos humanos	Responsable de la administración tributaria	4	No está disponible para adoptar una decisión clave	Cambio constante de autoridades	4	3	48	Mitigar: Delegación de la autoridad.
	Personal esencial de TI	5	El administrador del sistema no está disponible para aplicar un parche de emergencia	Existe un único administrador del sistema en el departamento de TI	3	3	45	Mitigar: Crear un equipo de tres administradores del sistema.
Activos de información	Datos nacionales sobre los contribuyentes y datos de AEOI (en formato digital)	5	Acceso no autorizado a los datos con revelación de información confidencial	Vulnerabilidades del sistema	3	5	75	Mitigar: tests de penetración, cifrado de datos en tránsito, controles de firewalls, copia de seguridad de los datos, todos los accesos a la base de datos son registrados y guardados, acceso exclusivamente en caso necesario.
	Información intercambiada mantenida en papel	5	Una persona no autorizada accede a la sala de archivo y revela información confidencial	La sala de archivo no es lo bastante segura	3	5	75	Mitigar: Únicamente puede acceder a la sala de archivo el personal autorizado, utilizando un código de acceso. Todos los accesos a la sala de archivo son registrados y guardados.

RE 3.2.1.5. Gestión de la continuidad de las operaciones

El RE 3.2.1.5 requiere que las administraciones tributarias dispongan de medidas adecuadas para gestionar y mantener la continuidad de sus operaciones. Esto se refiere a cómo la administración tributaria asegura que puede continuar desarrollando sus principales procesos de negocio, como la recaudación de impuestos y el AEOI, en el escenario de que se produzca un evento que altere su normal funcionamiento. Ese evento puede ser un desastre natural, una pandemia, un chantaje informático (*ramsomware attack*) o un incidente técnico que deje inoperativos los sistemas de TI.

La continuidad de las operaciones y su planificación (Plan de continuidad de las operaciones - PCO) guardan una estrecha relación con el proceso de gestión del riesgo. La continuidad de las operaciones es un proceso de gestión que incluye la identificación de escenarios de riesgo, la evaluación de su impacto, la elaboración de un PCO para asegurar la continuidad de las operaciones si se materializa el escenario de riesgo, la prueba y revisión del PCO y la formación del personal acerca del mismo, como se muestra en la Figura 5. A continuación se esbozan las fases típicas del PCO.

Fase 1: Identificación de escenarios de riesgo para la continuidad de las operaciones

Los altos directivos y representantes clave de las áreas involucradas (como los departamentos de TI, seguridad física o recursos humanos) deben identificar conjuntamente los escenarios probables de riesgo que podrían alterar las operaciones de la administración tributaria. Escenarios de riesgo pueden incluir desastres naturales, pandemias o catástrofes técnicas que pudieran tener como resultado alguna combinación de los siguientes elementos:

- Indisponibilidad del personal.

- Indisponibilidad de las instalaciones físicas.
- Indisponibilidad de los sistemas de tecnología de la información y las comunicaciones.

FIGURA 5. **Proceso de gestión de la continuidad de las operaciones**

Fase 2: Evaluación del impacto de los escenarios de riesgo en las operaciones

Las administraciones tributarias deben evaluar y documentar el impacto potencial de cada uno de los escenarios de riesgo en la continuidad de las operaciones, por ejemplo, cómo repercutiría una situación de riesgo determinada en las operaciones de AEOI o en los procesos de recaudación tributaria. El impacto puede expresarse en términos cualitativos (como la posibilidad de que la administración tributaria no pueda intercambiar información en el plazo previsto) o cuantitativos (como el importe de los tributos no recaudados en el plazo previsto).

Fase 3: Elaboración de la estrategia y el PCO

Las administraciones tributarias deben definir una estrategia para responder y superar el impacto en las operaciones si se materializa un escenario de riesgo. Cada PCO debe comprender tres fases principales (véase el ejemplo de la estructura de un PCO en el Recuadro 9):

- Respuesta inmediata, dando prioridad a la seguridad del personal, si fuera necesario.

Recuadro 9. **Ejemplo de estructura de un PCO**

1. Prioridades de recuperación. Operaciones esenciales cuya recuperación sea prioritaria y que deban ser trasladadas a una ubicación alternativa.
2. Estrategia de traslado y ubicación alternativa. La ubicación alternativa está indicada para el caso de que se produzca una catástrofe o perturbación que impida la continuidad de las operaciones en la ubicación original de la administración tributaria. Esta estrategia puede incluir ubicaciones de corto y largo plazo, en función de la gravedad de la perturbación.
3. Copia de seguridad de la información crítica en formato digital y en papel.
4. Fases de la recuperación:
   - **a.** Ocurrencia de la catástrofe.
   - **b.** Activación del PCO.
   - **c.** Traslado a ubicación alternativa.
   - **d.** Recuperación, es decir, actividades o tareas específicas para restablecer las operaciones habituales y las críticas.
   - **e.** Retorno al funcionamiento normal.
5. Plan de restablecimiento: los equipos de recuperación y de TI mantienen, controlan y comprueban periódicamente todos los registros que son vitales para la continuidad de las operaciones y que resultarían afectados por las perturbaciones o catástrofes en las instalaciones. Estos equipos realizan periódicamente copias de seguridad y almacenan los archivos críticos en una ubicación situada en otro lugar.
6. Equipo de recuperación. Funciones y responsabilidades. Datos de contacto.

- Habilitar el restablecimiento de las funciones centrales. Para tal fin, el PCO debe identificar:
  - Los sistemas clave y el orden de prioridad para su restablecimiento.
  - El personal o proveedores críticos involucrados y sus datos de contacto personales (dirección de correo electrónico, teléfono particular).
  - La información, documentos en papel y/o copias de seguridad o discos duros externos críticos que deban trasladarse a una ubicación de seguridad.
  - La persona que tomará la decisión de retornar al funcionamiento normal.

Recuadro 10. **Ejemplo de PCO de una administración tributaria**

El PCO de la administración tributaria de la jurisdicción A contiene todas los pasos detallados que deben aplicarse para garantizar que la administración tributaria pueda recuperarse de una perturbación importante de su funcionamiento normal. En la elaboración del PCO se han tenido en cuenta los principales escenarios de riesgo, si bien el carácter general del plan lo hace aplicable a la mayoría de las amenazas.

En el PCO se indican todos los actores que deben intervenir de producirse una emergencia que perturbe el funcionamiento, y sus datos de contacto se actualizan de inmediato ante cualquier cambio de forma que se les pueda localizar sin demora.

El PCO enumera todo los sistemas críticos de TI y el orden de prioridad para su recuperación. El PCO establece que todos los sistemas críticos de TI deben recuperarse en un plazo de 24 a 48 horas, y que el retorno al funcionamiento normal no debe tomar más de una semana. La administración tributaria dispone de un sitio de procesamiento alternativo por si hubiera que reubicar las operaciones.

El personal recibe formación anual acerca del PCO, que está publicado en la intranet de la administración tributaria.

La administración tributaria realiza simulacros teóricos de aplicación del PCO dos veces al año y un simulacro práctico como mínimo una vez al año. Su finalidad es evaluar la preparación y los conocimientos del personal en relación con el plan, para tener la certeza de que todos los miembros del personal conocen las funciones que tienen que asumir en caso de emergencia y detectar posibles brechas en el PCO. A raíz de estos simulacros se introducen las mejoras necesarias en el PCO.

- Procedimiento y fases para el retorno al funcionamiento normal.

El PCO se revisará periódicamente para reflejar posibles cambios en las situaciones de riesgo, actualizar la designación del personal clave y sus datos de contacto, reflejar posibles cambios en el tipo de información que se posee o en el sistema de TI, etc.

Fase 4: Pruebas y formación en relación con el PCO y revisión del plan

El PCO deberá ponerse a prueba por lo menos una vez al año por medio de ensayos o simulacros que abarquen todos sus aspectos. Su finalidad primordial es verificar que el personal sabe lo que tiene que hacer en caso de emergencia conforme a lo establecido en el PCO. Los resultados de las pruebas del PCO serán comunicados y utilizados para mejorar el plan.

Reviste la máxima importancia que el personal reciba formación sobre el PCO. Deben realizarse sesiones periódicas de sensibilización para todos los miembros del personal implicados en esta área. En el recuadro 11 se recoge un ejemplo de ensayo del PCO y de formación sobre el mismo.

La gestión de escenarios de indisponibilidad de los sistemas de tecnología de la información y las comunicaciones suele ser competencia del departamento de TI. Este aspecto se aborda en detalle en el RE 3.2.4.5, relativo a la continuidad de los servicios de TI bajo Acuerdos de Nivel de Servicio.

REQUISITO ESPECÍFICO 3.2.2: CONTROL DE LOS RECURSOS HUMANOS

Los controles de los recursos humanos son las políticas y procedimientos jurídicos y administrativos aplicables a la gestión de los recursos humanos de la administración tributaria (por lo general, personal propio y contratistas), con vistas a garantizar que respetan y protegen la confidencialidad de la información tributaria.

El personal tienen acceso a información sensible sobre los contribuyentes, así como a la política y la actuación de la administración tributaria, por ejemplo, en el curso de inspecciones fiscales, análisis de riesgos o investigaciones. El personal tiene también una relación estrecha con todas las fases del ciclo de vida de la información intercambiada.

Por ello, las administraciones tributarias deben establecer controles a lo largo del ciclo de vida de la relación laboral, a fin de asegurar que se pueda confiar en el personal, así como en terceras partes o contratistas externos, para garantizar la confidencialidad. La confianza entre un empleador y su personal se basa en un primer examen realizado durante la fase de contratación (a menudo seguido de un periodo de prueba) y en los años de su relación empleador-empleado.

Esta sección se divide en cuatro secciones: una breve descripción del ciclo de vida de la relación laboral, seguida de las actividades y procesos a desarrollarse en cada una de las tres fases principales de ese ciclo (contratación, empleo y terminación).

Estas tres fases se describen de forma detallada junto con los controles específicos que podrían aplicarse. En la Tabla 7 se proporcionan definiciones de los principales conceptos utilizados en el RE 3.2.2.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Tabla 7. **Glosario de principales conceptos**

Concepto	Descripción
Sensibilización	La sensibilización consiste en exponer periódicamente a los empleados a mensajes de seguridad que les alertan de amenazas y riesgos en materia de TI o de otras amenazas y riesgos para la seguridad; estos mensajes suelen comunicarse a todos los empleados a la vez, tanto en una determinada área de trabajo como en el conjunto de la administración tributaria, e incluso a terceros externos.
Acuerdo de no divulgación	Declaraciones o contratos formales en los que se establecen las reglas para la no divulgación de información confidencial a terceros.
Phishing	Tipo de estafa online que consiste en el envío de mensajes fraudulentos de correo electrónico que aparentan proceder de una fuente legítima y engañan al destinatario para que envíe información confidencial, como sus credenciales de acceso a los sistemas.
Ingeniería social	Consiste en explotar de forma malintencionada la confianza del personal para obtener información que puede utilizarse en beneficio propio. Esta actividad se conoce también como "piratería de personas".
Formación	Medidas dirigidas a que el personal de la administración tributaria (empleados y contratistas) adquiera y desarrolle los conocimientos, aptitudes y competencias clave necesarias para integrar la confidencialidad y la seguridad en los procesos tributarios.

Ciclo de vida del personal

El RE 3.2.2, siguiendo los estándares internacionales, requiere que las administraciones tributarias cuenten con distintas políticas y procedimientos (denominados controles) para las tres fases del ciclo de vida de la relación laboral: controles relativos a la fase de contratación (REs 3.2.2.1 y 3.2.2.2), controles relativos al desarrollo de la relación laboral (REs 3.2.2.3 y 3.2.2.4), y controles relativos a la terminación de la relación laboral (RE 3.2.2.5). En la Figura 6 se indican los más importantes.

Tipos de personal de las administraciones tributarias

Los controles a lo largo del ciclo de vida de la relación laboral deben aplicarse a todo el personal (término que en sentido amplio comprende a los empleados, tanto permanentes como temporales, y a los proveedores de servicios y contratistas externos). El personal de la administración tributaria no está integrado por una sola clase de empleados, sino que suelen coexistir las categorías descritas en la Tabla 8.

Pueden existir otras categorías, dependiendo del contexto particular de cada jurisdicción y de su legislación laboral.

Las administraciones tributarias deben tomar en consideración todas sus categorías de personal cuando evalúen los distintos tipos de procesos aplicables a lo largo del ciclo de vida de su relación laboral. Por ejemplo, deben establecer controles adecuados respecto de terceras partes contratadas para desempeñar funciones delicadas (como la administración de sistemas que contengan información intercambiada) e impartir formación específica para cada función en materia de protección de la confidencialidad a todo el personal que gestione o maneje información sensible sobre los contribuyentes, sea cual sea su modalidad de contratación.

Los controles específicos de seguridad aplicables a los terceros contratistas se cubren en más detalle en el RE 3.2.4.4, relativo a la gestión de la prestación de servicios por proveedores.

Los controles que se apliquen pueden depender también de cómo esté organizada la función de recursos humanos

FIGURA 6. **Ciclo de vida de la relación laboral y controles para garantizar la confidencialidad**

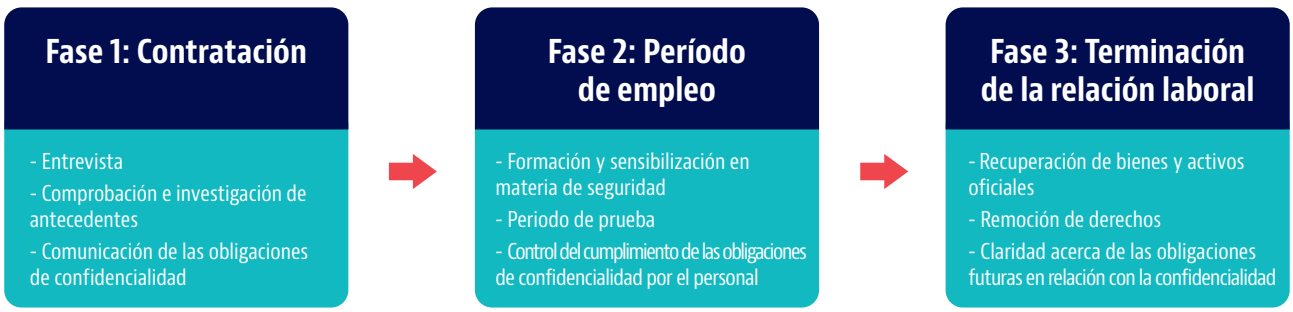


Tabla 8. **Clases de personal de la administración tributaria**

Clase	Descripción
Empleado	Por lo general, personas contratadas por tiempo indefinido o por una duración determinada pero prorrogable.
Personal temporal	Por lo general, personas contratadas por una duración determinada para un fin específico (por ejemplo, servicios de consultoría).
Funcionario / servidor público	Persona a la que se concede un puesto permanente en la administración pública, normalmente un puesto vitalicio.
Contratistas externos	En esta categoría pueden darse dos tipos de relación contractual: ● Contratistas externos contratados para prestar un servicio específico, como puede ser el suministro de un determinado sistema de TI o la limpieza de las instalaciones. ● Contratistas que desempeñan una función específica, por ejemplo una función de corta duración o una función para la que no se dispone de empleados cualificados. Por ejemplo, un experto contratado para impartir in situ un curso de formación para el personal sobre el uso de un sistema especializado.

en cada administración tributaria. Los recursos humanos no constituyen una función de la administración tributaria per se, sino más bien una función genérica de la que la administración tributaria se sirve. Por ello, la gestión de los recursos humanos no siempre se lleva a cabo dentro de la propia administración tributaria, sino que en algunas jurisdicciones puede haber un único departamento de recursos humanos para todo el Ministerio de Hacienda o para todo el sector público; igualmente cabe que una categoría de personal se gestione de forma centralizada (como los servidores públicos), mientras que otras no consideradas función pública sean gestionadas por la propia administración tributaria.

Al margen de cuál sea su estructura organizativa, las jurisdicciones deben poder identificar dónde está ubicada la función de gestión de los recursos humanos dentro de su sistema general de gobierno, así como su vinculación a la administración tributaria. De este modo podrán evaluar lo que debe hacer cada organismo o departamento competente para garantizar que en las distintas políticas y procedimientos se apliquen controles proporcionales a la sensibilidad de la función de la administración tributaria.

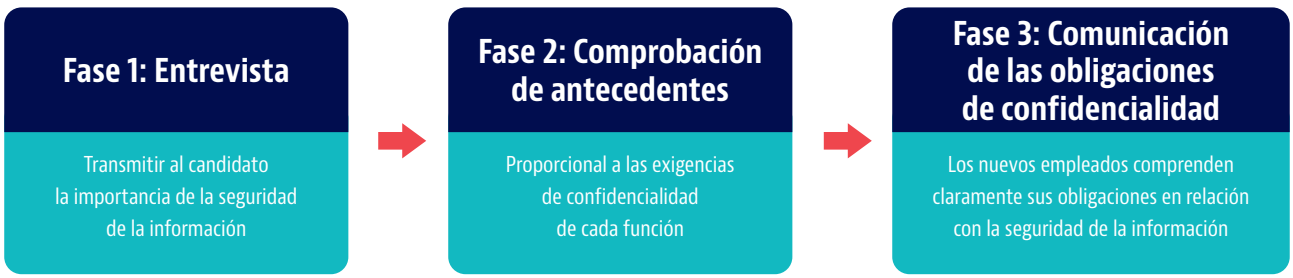
Los siguientes apartados ofrecen orientación sobre controles habituales en cada una de las tres fases de la relación laboral.

REs 3.2.2.1 y 3.2.2.2. Fase 1: Controles durante la contratación

Esta sección trata sobre los controles de seguridad durante el proceso de contratación de personal. Consisten en verificaciones y medidas dirigidas a garantizar que podrá confiarse a los futuros miembros del personal el manejo de información confidencial. Los controles deben ser consistentes con las leyes y regulaciones relevantes de cada jurisdicción (por ejemplo, el código tributario o las regulaciones sobre el servicio civil) y proporcionales a las necesidades operativas, la clasificación y sensibilidad de la información a la que tendrán acceso y los riesgos percibidos.

En primer lugar, el RE 3.2.2.1 requiere que las administraciones

FIGURA 7. **El proceso de contratación**



tributarias se aseguren de que las funciones y responsabilidades de los empleados y contratistas en materia de seguridad estén bien definidas y documentadas y se comuniquen claramente en las condiciones de contratación, revisándose periódicamente de conformidad con la política de GSI (incluidos los acuerdos de confidencialidad y de no revelación). Este aspecto se analiza más adelante.

En segundo lugar, el RE 3.2.2.2 requiere que las administraciones tributarias lleven a cabo verificaciones de los antecedentes de cada candidato, empleado y contratista por medio de una investigación adecuada, de acuerdo con las mejores prácticas aceptadas y los riesgos percibidos. Este aspecto se refiere al proceso de contratación, que puede segmentarse en tres fases, cada una de ellas con sus propios controles relativos a la confidencialidad (véase la Figura 7).

Fase 1: Entrevista

Durante el proceso de entrevistas se transmitirá a los potenciales candidatos la importancia de la confidencialidad y la protección de la seguridad de la información. Por ejemplo, el formulario de contratación puede llevar la clasificación de seguridad correspondiente, indicando al futuro miembro del personal el nivel de confidencialidad que implicará su función. También puede explicarse a los candidatos preseleccionados para una entrevista cuáles serán, en caso de resultar seleccionados para el puesto, sus obligaciones de confidencialidad y las consecuencias (administrativas y penales) de un eventual incumplimiento.

Tabla 9. **Tipos de verificaciones de antecedentes durante el proceso de contratación**

Comprobación de antecedentes	Descripción
Verificación de las pruebas aportadas por los candidatos	Consiste en verificar la experiencia profesional, las titulaciones educativas y técnicas, las referencias, etc. proporcionadas por los candidatos. Si un candidato suministra información falsa no cumplirá los estándares de probidad necesarios que requiere un puesto de trabajo en la administración tributaria. No obstante, podría no ser necesario llevar a cabo comprobaciones de todas las titulaciones y referencias aportadas. Comprobaciones por muestreo en base a ciertos criterios convenidos en función del riesgo o comprobaciones completas de todos los candidatos en algunos ámbitos pueden ser suficientes para asegurarse de que las candidaturas sean aceptables.
Comprobación de antecedentes penales	Normalmente, junto con la información relativa a la candidatura se exige una comprobación de antecedentes penales. En algunas jurisdicciones se considera que tener antecedentes penales es totalmente incompatible con asumir un empleo en la administración tributaria. Si tener antecedentes penales no es un impedimento para una administración tributaria al contratar personal, podría ser necesaria la aplicación de ciertos criterios restrictivos, entre los que pueden incluirse la gravedad del delito, el tiempo transcurrido desde la comisión del delito, etc. Asimismo, las administraciones tributarias podrán adoptar medidas compensatorias cuando contraten a candidatos con antecedentes penales como, por ejemplo, estableciendo períodos de prueba o introducción (con criterios para la salida del empleado) durante los cuales esas personas estarían sometidas a una supervisión especial. En relación con delitos cometidos durante el desarrollo de la relación laboral, las jurisdicciones deberían dejar en claro al futuro personal que debe comunicar cualquier acusación de naturaleza penal que le afecte y que ello podría conllevar ciertas consecuencias (como el despido).
Comprobación del historial financiero	Otro tipo de comprobación puede consistir en la divulgación de los antecedentes financieros, en particular para las personas que ocupan puestos directivos. Aunque esta comprobación puede ser importante para la labor de la administración tributaria, su aplicación puede variar en función del contexto concreto de cada jurisdicción, p.ej. si se percibe la corrupción como un problema especial. En algunas jurisdicciones, puede llevarse a cabo como parte de una revisión más amplia de los asuntos de quienes necesitan autorización para trabajar con la información más delicada (véase a continuación el apartado dedicado a la investigación).
Investigación	Algunas jurisdicciones disponen de servicios de investigación o autorización a nivel de departamento o intergubernamentales (a menudo integrados en los servicios de seguridad nacional), que llevan a cabo distintos tipos de comprobaciones de idoneidad con el fin de adquirir un conocimiento adecuado de los antecedentes y el carácter de los candidatos. Estas comprobaciones se realizan por lo común antes de que esas personas comiencen a trabajar en un puesto que conlleve el acceso a información clasificada, y pueden variar en función del nivel de clasificación de dicha información (p.ej. protegida, secreta, de alto secreto). Es común que cierto personal de la administración tributaria maneje datos clasificados como muy confidenciales tal como sucede, por ejemplo, con los registros financieros y comerciales de grandes contribuyentes o de personas que ostentan un cargo político. Esta investigación multinivel ayuda a las agencias gubernamentales y a su personal que trabaja con información con distintos niveles de seguridad. La investigación puede incluir: comprobación de la identidad, condenas penales y delitos menores, análisis positivos de drogas, calificación crediticia, quiebra, ingresos de los últimos 5 años, problemas de ludopatía, etc. En el caso de una investigación más profunda, la lista puede incluir entrevistas al personal, así como a una muestra de otros familiares, amigos y asociados.

Fase 2: Comprobación de antecedentes

Esta fase se refiere a la aplicación de verificaciones de antecedentes, investigaciones de antecedentes u otras medidas de verificación adecuadas a todos los candidatos, incluidos empleados permanentes y temporales, contratistas, etc. La comprobación de los antecedentes puede implicar distintos niveles de escrutinio, y suele ser proporcional al tipo de rol y a sus requisitos de confidencialidad (véase la Tabla 9).

Aunque estas comprobaciones y verificaciones se presentan como aplicables al inicio de la relación laboral, también es importante que se actualicen periódicamente, y es posible que algunas de ellas tengan que repetirse a lo largo de la relación laboral en determinadas circunstancias. Por ejemplo, cuando exista un cambio importante en la función del empleado o se traslade a un puesto más sensible, con acceso a información más sensible o clasificada como muy confidencial. La investigación, en particular cuando se trate de una autorización superior a la de nivel básico, tendrá normalmente una duración limitada e incluirá un proceso dirigido a revisar los niveles de investigación y actualizar las autorizaciones.

En caso de contratistas externos, las administraciones tributarias también deben llevar a cabo comprobaciones y verificaciones de antecedentes. No obstante, las administraciones tributarias pueden decidir delegarlas en el propio contratista, de modo tal que será éste quien lleve a cabo las comprobaciones de su propio personal y se asegure de que todos sus empleados cumplan con las políticas de seguridad de la administración tributaria. En tal caso, la administración tributaria debe asegurarse de que el tercero realiza las comprobaciones de antecedentes y cumple debidamente las condiciones de su contrato. Los controles de terceros contratistas también se abordan en el RE 3.2.4.4, relativo a la gestión de la prestación de servicios por parte de proveedores. En caso de contratistas a largo plazo, las administraciones tributarias podrían exigir la actualización regular de la comprobación de antecedentes del contratista o de su personal (p.ej. según los intervalos mínimos establecidos en la ley o en la política relativa al personal general). El recuadro 11 ofrece algunos ejemplos de controles en la contratación.

Recuadro 11. **Ejemplo de controles en la contratación**

La administración tributaria de la Jurisdicción A aplica controles de verificación de antecedentes en relación con todo su personal. Durante el proceso de contratación, se obtiene un certificado del Ministerio de Interior para confirmar que no se han impuesto sanciones penales y que la persona no está sometida a procedimiento penal alguno. Además, se solicita una prueba de la formación educativa del candidato. Se consulta a antiguos empleadores.

Cuando la persona debe acceder a información clasificada, tal como la información obtenida a través del EOI, los controles también incluyen un proceso de investigación y autorización de seguridad que investiga los asuntos financieros, la nacionalidad, la salud mental y otra información personal relevante del candidato. Si el candidato ya ha trabajado para la administración tributaria, se tienen en cuenta factores como una conducta adecuada en el manejo de la información y los documentos y su conducta en general a lo largo de toda su relación laboral.

Si la administración tributaria tiene que encargar a contratistas el manejo de la información obtenida a través del EOI, o el suministro de software, hardware o servicios, el personal de dichos contratistas también sería sometido a las mismas comprobaciones de antecedentes, investigaciones y autorizaciones de seguridad que se aplican al personal regular, en función de los riesgos percibidos y del tipo de servicio que deba prestarse. También debería someterse a revisión la propia empresa, a fin de supervisar cuestiones de cualquier tipo ligadas a su reputación.

Fase 3: Comunicación de funciones y obligaciones en materia de confidencialidad en el momento de la contratación

Tal como se describe en el RE 3.2.2.1, el nuevo personal debe recibir una imagen clara de sus obligaciones en el marco de su contratación, incorporación y cumplimiento de su relación laboral. Las funciones y responsabilidades en materia de confidencialidad y seguridad de la información deben ser documentadas y comunicadas de forma clara a todas las nuevas incorporaciones y a los miembros del personal, por ejemplo, a través de:

- Las disposiciones sobre secreto fiscal en la legislación aplicable, p.ej. el Código Tributario o el Estatuto de la Función Pública.
- La política de GSI y otros documentos en materia de GSI.
- Contratos, términos y condiciones de la relación laboral u otros instrumentos de nombramiento firmados por el nuevo personal.
- Acuerdos o declaraciones de confidencialidad y no divulgación como, por ejemplo, la inclusión de una cláusula de confidencialidad en los contratos del personal que trabaje en la unidad de EOI.

Las administraciones tributarias también deben verificar que los nuevos empleados hayan comprendido efectivamente sus obligaciones y se comprometan a ajustar su actuación a las políticas de confidencialidad y seguridad. A tal fin, deben adoptarse procesos y

Recuadro 12. **Ejemplo de comunicación de obligaciones de confidencialidad en el momento de la contratación**

El personal recién contratado de la administración tributaria de la Jurisdicción B firma un acuerdo de confidencialidad y no divulgación que forma parte de los términos y condiciones de su contrato de trabajo. En dicho acuerdo se les informa expresamente de lo siguiente:

- El acceso a los sistemas de información solo debe usarse para actividades laborales adecuadas.
- El uso por su parte de los sistemas de información puede ser y será supervisado.
- El uso inadecuado puede dar lugar a investigaciones de carácter administrativo y, en su caso, penal.

Asimismo, se entrega a los recién incorporados una copia de la parte del Código Tributario aplicable en materia de obligaciones de secreto fiscal.

Un representante del departamento de recursos humanos y el director del departamento de contratación organizan una breve reunión introductoria para los recién incorporados que incluye una explicación de la interpretación práctica de la legislación y de los requisitos de confidencialidad y no divulgación. Esta formación introductoria concluye con un breve cuestionario.

Una vez finalizado el programa introductorio, los recién incorporados participan en una ceremonia oficial en la que juran respetar la confidencialidad, jurando mantenerla incluso con posterioridad a la extinción de su relación laboral.

procedimientos que permitan determinar la eficacia de la comunicación, con independencia del instrumento o los medios de comunicación utilizados. Por ejemplo, las administraciones tributarias pueden comunicar al personal las políticas de confidencialidad, así como evaluar en qué medida las han comprendido, a través de programas introductorios de cumplimiento obligatorio que incluyan evaluaciones y comentarios de los empleados entrenados durante la primera semana de la relación laboral. El recuadro 12 ofrece un ejemplo de comunicación en el momento de la contratación.

Contratistas externos

Algunos servicios pueden ser prestados por contratistas externos como, por ejemplo, los servicios de tecnologías de la información (TI), mantenimiento de impresoras, servicios de limpieza o contratistas contratados para aportar competencias específicas como análisis de datos, entre otras. Los contratistas y su personal deben comprender las políticas de confidencialidad de la administración tributaria y comprometerse a cumplirlas.

Las relaciones con contratistas se regirán normalmente por contratos y/o Acuerdos de Nivel de Servicio (SLA, siglas en inglés de *Service Level Agreement*), que se analizan de forma más pormenorizada en el RE 3.2.4.4, relativo a la gestión de la prestación de servicios por parte de proveedores:

- Los **contratos** son acuerdos exigibles que definen las funciones y responsabilidades de las partes.
- Los **SLA** son acuerdos en los que las administraciones tributarias establecen un nivel mínimo del servicio que se espera que cumpla el contratista externo. Los SLA se centran en medidas y parámetros de cumplimiento para asegurar que el contratista presta el servicio bajo los estándares de calidad acordados.

Con independencia del tipo de acuerdo que se utilice, éste debe contener requisitos explícitos para la protección de la confidencialidad y la seguridad de la información, que incluirán, como mínimo, los siguientes:

- **Acceso**. El acceso a los sistemas de la administración tributaria debe permitirse en función de la "necesidad de saber" y ser proporcional al alcance de los servicios encomendados al contratista (véase el RE 3.2.3 para más detalles relativos a la gestión del acceso).
- **Comunicación de incidencias**. Los contratistas deben comunicar todos los incidentes de seguridad de la información al OSI tan pronto como sea posible después de que se produzcan o descubran. Deben habilitarse procesos de escalamiento de incidencias a superiores en casos de vulneración de la confidencialidad (véase el RE 3.2.6.6 para más detalles relativos a la gestión de incidencias).

RE 3.2.2.3 y RE 3.2.2.4. Fase 2: Controles relativos a la relación continua entre el empleador y el empleado

Esta sección tiene por objeto garantizar que, durante la relación laboral, el personal reciba orientación periódica relativa a requisitos organizacionales en materia de confidencialidad y aplique en la práctica las políticas y procedimientos de seguridad. Esto puede lograrse mediante una combinación de formación y sensibilización, y aplicando mecanismos que fomenten y refuercen el cumplimiento.

Por lo tanto, el RE 3.2.2.3 requiere que las administraciones tributarias se aseguren de que los empleados y contratistas reciban formación y sensibilización periódica y actualizada en materia de seguridad, y que quienes ocupan puestos sensibles reciban orientación adicional relevante para el manejo

de material más sensible. Según el RE 3.2.2.4, las administraciones tributarias deben asegurarse de que los empleados apliquen las políticas y procedimientos de seguridad.

Formación y sensibilización en materia de seguridad

Aunque la formación y sensibilización persiguen objetivos similares y conexos, son conceptos distintos (véase la Figura 8).

Las necesidades de formación y sensibilización, su contenido y frecuencia deben identificarse y definirse tanto en los niveles directivos de la administración tributaria (p. ej. OSI, directivos de las divisiones tributarias, departamentos de recursos humanos y de informática) como en el ámbito de la relación entre el supervisor y el empleado.

Formación

La formación en materia de confidencialidad y seguridad debe integrarse en los requisitos y políticas institucionales relativos al desarrollo profesional del personal. La formación es un proceso que comienza antes del propio acto de formación, cuando se identifican las necesidades formativas, y se extiende hasta la aplicación efectiva de los conocimientos adquiridos por el personal en sus tareas cotidianas. Debe impartirse de manera periódica a fin de garantizar que el personal se encuentre informado con respecto a los desarrollos más recientes.

En función de cómo gestione una administración tributaria su función formativa y de desarrollo profesional, los encargados de impartir la formación en materia de confidencialidad y seguridad pueden variar. En cualquier caso, es una buena práctica asegurarse de la implicación y participación de los departamentos responsables de recursos humanos, informática y seguridad en el desarrollo de los contenidos de la formación y en su impartición.

Pueden impartirse varias categorías distintas de formación en materia de seguridad, que incluyen:

- **Formación básica en materia de seguridad**, conforme a la cual se comunica a todo el personal la política de GSI y otras políticas organizacionales fundamentales relativas a los procesos de confidencialidad y seguridad, tales como el Código Tributario, la política de seguridad física, etc. Este tipo de formación puede integrarse en la formación introductoria analizada anteriormente en el contexto de los controles relativos al proceso de contratación.
- **Formación adaptada al puesto**, ajustada a las necesidades de cada puesto. Por ejemplo, se espera que el personal de la unidad de EOI reciba formación especial relativa a los procesos de manejo de la información intercambiada, según lo dispuesto en el manual de EOI o en un procedimiento similar, y que esté especialmente sensibilizado con los requisitos de los tratados en cuanto al manejo y uso de información recibida de autoridades competentes extranjeras. Además, el personal directivo o con responsabilidades relevantes (p. ej. el OSI) podría recibir formación ad hoc relacionada con las necesidades particulares de su puesto como, por ejemplo, formación certificada en operaciones de seguridad, seguridad cibernética, gestión de accesos, etc.
- **Formación no asociada a un puesto específico**, sino al entorno en que trabaja el personal. Algunos ejemplos son la seguridad en las instalaciones de la oficina (p. ej. portátiles, ordenadores de escritorio), los riesgos asociados a las tecnologías de Internet, etc.
- **Formación basada en el cambio de funciones como**, por ejemplo, cuando un miembro del personal es ascendido a un nuevo puesto.

Sensibilización

Las campañas de sensibilización pueden incluir:

- **Mensajes relativos a riesgos y amenazas informáticas** como, por ejemplo, advertir al personal de los peligros de abrir enlaces en correos electrónicos de fuentes

FIGURA 8. **Definición de formación y sensibilización**

Formación	La formación consiste en la adquisición y desarrollo por el personal de los conocimientos, capacidades y competencias básicas que son necesarios para incorporar la confidencialidad y la seguridad a los procesos tributarios.
Sensibilización	La sensibilización consiste en la exposición periódica del personal a mensajes que les adviertan de riesgos y amenazas en materia de seguridad, ya sean relacionados con las tecnologías de la información u otros. Los mensajes suelen comunicarse al mismo tiempo a todo el personal, o al menos a los que pertenecen a grupos o áreas de trabajo definidos (incluido el personal externo, según proceda).

desconocidas, o de *phishing o ataques de spear phishing*,[13], que pueden tratar de obtener información que podría utilizarse con el fin de poner en peligro los datos de la administración tributaria mediante la ejecución de descargas maliciosas como ransomware y spyware.

- **Mensajes relativos a riesgos y amenazas a la seguridad física** como, por ejemplo, recordar al personal la importancia de comunicar siempre la pérdida de credenciales con fotografías identificativas.

Las campañas de sensibilización no deben centrarse únicamente en ayudar al personal a evitar ser víctima de ataques informáticos o de otro tipo, sino también en instruirlos acerca de sus responsabilidades como funcionarios de la administración tributaria (p. ej. comunicar siempre los ataques de *phishing* al departamento responsable y/o al OSI, a fin de que puedan adoptar medidas preventivas o correctivas adecuadas).

Tal como con la formación, sería una buena práctica implicar a los departamentos responsables de recursos humanos, informática y seguridad en el desarrollo y ejecución de campañas de sensibilización. El recuadro 13 ofrece un ejemplo de formación y sensibilización en materia de seguridad dentro de una administración tributaria.

Asegurarse de que el personal aplica efectivamente las políticas y procedimientos de seguridad

El personal debe aplicar políticas de seguridad en su labor cotidiana y cuando utiliza sistemas y procesos que involucran información confidencial. Por lo tanto, los cargos directivos necesitan medios para evaluar el nivel de cumplimiento de las obligaciones de seguridad por parte del personal. Estos medios pueden incluir:

- La inclusión de la seguridad de la información como parte de los acuerdos u objetivos de rendimiento de los empleados, y el tratamiento de este tema en las reuniones sobre gestión del rendimiento que se celebren entre el superior y sus subordinados.
- La definición clara de los objetivos de los eventos de formación y las campañas de sensibilización en materia de seguridad, en cuanto a las necesidades de confidencialidad que cubren, y el seguimiento de los resultados mediante encuestas o cuestionarios, reuniones de equipo y comentarios y valoraciones del personal a los cargos directivos.

El rol del supervisor es esencial, pues es quien puede persuadir con más éxito al personal para que lleve a cabo la formación necesaria y puede verificar que el

13. Los ataques de *phishing* se envían a muchos destinatarios. Los ataques de *spear phishing* se dirigen a un solo individuo.

Recuadro 13. **Ejemplo de formación y sensibilización en materia de seguridad**

Todo el personal de la administración tributaria de la Jurisdicción C recibe formación obligatoria en materia de seguridad de la información al menos una vez cada dos años, de conformidad con lo establecido en la política de GSI. La formación es impartida por el Instituto de Estudios Fiscales, que es parte de la administración tributaria. Sus contenidos son elaborados por el OSI junto con el director del Departamento de Informática y el Instituto, y son actualizados periódicamente de acuerdo a los desarrollos en el entorno de seguridad y en base a los comentarios y valoraciones de los asistentes y los cargos directivos. La formación cubre la confidencialidad en relación con los procesos tributarios, así como cuestiones más amplias tales como los riesgos derivados del uso de la tecnología y los medios sociales y los riesgos físicos.

También se dispone de un sistema de aprendizaje a distancia en las siguientes materias:

- Legislación en materia de secreto tributario, política de GSI y Código de Conducta.
- Protección contra las amenazas informáticas, de Internet, de ingeniería social y de *phishing*.
- Clasificación, conservación y gestión de la información.
- Comunicación de incidentes de seguridad y gestión de vulneraciones de datos.

Los módulos del aprendizaje a distancia incluyen cuestionarios al final de cada sección, a fin de comprobar que el personal entiende los requisitos básicos antes de que puedan proceder a finalizar la formación en línea. Cada cuestionario requiere contestar correctamente el 90% de las preguntas. El OSI y los jefes de línea verifican que todo el personal haya concluido con éxito la formación y reciben comentarios y valoraciones a través de reuniones con el personal.

El personal recibe mensajes de correo electrónico diarios del departamento de informática relativos a la protección de la información y los sistemas de información frente a amenazas internas y externas, con ejemplos relativos a correos electrónicos maliciosos, administración de contraseñas, políticas de escritorio y de pantalla limpios, ingeniería social y bulos en Internet. Estos mensajes también están disponibles en la intranet.

La administración tributaria exige a los contratistas que formen a su personal en seguridad de la información bajo los SLA. El cumplimiento de este requisito es supervisado anualmente por el equipo de Auditoría Interna de la administración tributaria.

Recuadro 14. **Ejemplo de ejecución y evaluación del cumplimiento de las políticas de confidencialidad**

El personal de la administración tributaria de la Jurisdicción A es recordado periódicamente de su obligación de proteger la confidencialidad de la información tributaria, a través de ventanas emergentes, anuncios en la intranet y eventos de formación. Los procedimientos disciplinarios se publican en la intranet. El acceso y la divulgación de información no autorizados se califican como falta grave.

Todo el personal que desempeñe funciones asociadas a la gestión de la información del contribuyente está obligado a incluir entre sus objetivos anuales, como mínimo, un objetivo en materia de seguridad de la información.

Auditoría Interna realiza continuos controles de auditoría, tales como la revisión de los registros de auditoría de los accesos al sistema, a fin de comprobar si ha habido algún acceso no autorizado a información por parte del personal. Los resultados de estas auditorías se comunican a los superiores inmediatos y al OSI.

Cuando se entablan acciones administrativas o penales contra el personal por el incumplimiento de obligaciones de confidencialidad, tales procedimientos se pondrán en conocimiento del personal a través de reuniones con los empleados y en la intranet, como medida disuasoria.

personal ha comprendido bien la formación y que la aplica en su labor cotidiana.

Los procedimientos y sanciones disciplinarios por incumplimiento también son esenciales para asegurarse de que el personal aplica las políticas de confidencialidad y seguridad. Dichos procedimientos deben comunicarse y recordarse al personal en todas las fases del ciclo de vida de la relación laboral.

Las sanciones podrían ser administrativas, civiles o penales, en función de la gravedad de la infracción. El marco legal nacional debe permitir la imposición de sanciones (este aspecto se cubre en detalle en el RP 3.3, que analiza las disposiciones y procesos de cumplimiento para hacer frente a las violaciones de la confidencialidad).

Las administraciones tributarias deben demostrar de forma clara su voluntad de aplicar sanciones cuando la conducta esté por debajo de los estándares requeridos, y cuando la protección de la información se vea comprometida. Es esencial que el personal vea que se recompensa el buen comportamiento y desempeño en materia de seguridad de la información y que, en cambio, las malas prácticas serán perseguidas y sancionadas según proceda. El recuadro 14 ofrece un ejemplo de ejecución y evaluación del cumplimiento de las políticas de confidencialidad.

RE 3.2.2.5. Fase 3: Controles relacionados al término de la relación laboral

Este RE requiere que las administraciones tributarias dispongan de políticas y procesos de recursos humanos relativos al cese de la relación laboral que protejan la información sensible. Esto se refiere a procedimientos definidos relativos a la extinción del contrato de trabajo, ya sea por jubilación, renuncia o despido de todo tipo de personal, incluidos los contratistas. Algunas administraciones tributarias pueden considerar también que un cambio de puesto equivale a una extinción de la relación laboral anterior, en cuyo caso podrán aplicarse los controles descritos en esta sección, según proceda.

Los controles deben garantizar que se mantiene la confidencialidad de la información después de la extinción de la relación laboral, y alcanzan fundamentalmente a los siguientes aspectos (véase el recuadro 15 a modo de ejemplo).

Recuperación de bienes o activos de la administración

Debe existir un proceso para comprobar que todos los bienes oficiales (p. ej. credenciales identificativas, portátiles, teléfonos móviles, USBs, etc.) han sido devueltos por el personal saliente (este proceso está ligado al RE 3.2.4.3, relativo a la gestión de activos).

Los superiores inmediatos y/o las áreas encargadas de la gestión de activos o recursos humanos deben encargarse de dicho proceso. El proceso puede llevarse a cabo, por ejemplo, a través de una lista de verificación firmada por el personal saliente, a veces en el marco de una "reunión de salida".

Supresión de derechos

La supresión de derechos se refiere a la oportuna revocación de todos los permisos de acceso, ya sean físicos (acceso a edificios, oficinas) o lógicos (acceso a sistemas). El proceso de establecimiento de los requisitos de acceso físico y de concesión y revocación de acceso lógico se describe de forma pormenorizada en el RE 3.2.3, relativo a la gestión de accesos.

El personal normalmente tiene derechos de acceso a espacios privados de trabajo de la administración tributaria, y algunos de sus miembros podrían tener derechos especiales de acceso a espacios en los que el acceso está sometido a controles más estrictos (p. ej. centros de datos o archivos). El acceso a estas áreas puede habilitarse a través de identificaciones con fotografía, pases electrónicos, identificación biométrica,

códigos de seguridad, etc., en función de los requisitos de seguridad física de cada instalación.

Para el personal saliente, todos dichos permisos de acceso deben revocarse y se les debe solicitar que entreguen sus credenciales con fotografías identificativas, así como desactivarse su identificación biométrica y códigos de seguridad, etc. En este proceso intervienen normalmente los gerentes de línea, la gerencia de seguridad física y/o recursos humanos.

Las administraciones tributarias deben aplicar también procesos para la oportuna revocación del acceso lógico a los sistemas. Este proceso es fundamental para la seguridad de la información, pues una causa muy importante de vulneración de datos es la piratería de derechos de acceso no utilizados.

El uso de derechos de acceso lógico debe controlarse, por tanto, de manera estricta. La supresión de derechos de acceso debe organizarse con anterioridad al último día en que su uso sea necesario, y los derechos deben ser revocados al finalizar ese último día. La responsabilidad de la revocación del acceso lógico debe recaer en los altos directivos responsables del proceso de negocio tributario o la aplicación relevantes, con la asistencia técnica del departamento de Informática, pues son esos directivos los encargados de determinar los criterios de acceso y aprobar los derechos de acceso al sistema.

Cuando un miembro del personal sea despedido o suspendido como consecuencia de conducta indebida, el proceso debe posibilitar la revocación inmediata de todos los derechos (físicos y lógicos) cuando se realice una solicitud adecuada (p. ej. de directivos o superiores inmediatos, o del departamento de investigaciones).

Claridad de las obligaciones futuras

El personal de la administración tributaria adquiere mucho conocimiento sobre información sensible relativa a los contribuyentes y sus asuntos fiscales. Su deber de confidencialidad debe mantenerse con posterioridad a la extinción de la relación laboral. Debe informarse de forma clara al personal saliente acerca de dicha obligación, que deberá registrarse en un documento oficial firmado por el miembro del personal y un supervisor competente (p. ej. en el documento que también cubre la devolución de activos).

REQUISITO ESPECÍFICO 3.2.3: CONTROLES DE ACCESO, INCLUIDO EL ACCESO FÍSICO Y LÓGICO

El RE 3.2.3 consiste en proteger la confidencialidad garantizando que solo los usuarios que tengan una razón de negocio legítima para acceder a la información están autorizados a hacerlo.

Recuadro 15. **Ejemplo de controles al finalizar la relación laboral**

En la administración tributaria de la Jurisdicción B, el departamento de Informática revoca de manera automática los accesos al sistema del personal saliente en base a la fecha de extinción del contrato de trabajo proporcionada por el departamento de recursos humanos. Cuando proceda, tal como sucede en casos de conducta indebida, el acceso se suprime en una fecha anterior.

El último día de trabajo se realiza una entrevista de salida. En ella estarán presentes el supervisor de la persona saliente, un representante del departamento de recursos humanos y un representante del departamento de gestión de la seguridad física. La persona saliente debe firmar un documento en el que declare que ha devuelto todos los bienes y activos de la administración, y que está sujeta a un deber de secreto vitalicio en relación con toda la información confidencial obtenida durante su relación laboral con la administración tributaria. Dicho documento también afirma que el incumplimiento de las disposiciones sobre confidencialidad se sancionará con arreglo a la legislación civil o penal, y recomienda al personal saliente que evite colocarse en una posición que pudiera plantear conflictos de intereses con respecto al mantenimiento de obligaciones de confidencialidad.

También como parte de la entrevista de salida, se revisa una lista de verificación a fin de comprobar la recuperación de todos los bienes de la administración y la supresión de todos los derechos. Esta lista de verificación incluye:

- Recogida del pase del miembro del personal, tokens de seguridad y llaves que hayan sido entregadas para el acceso tanto informático como físico a información clasificada.
- Recogida del ordenador portátil y el teléfono móvil de trabajo.
- Recogida de todos los activos y materiales con información clasificada que les hayan sido entregados para desempeñar su trabajo.
- Verificación de la revocación del acceso a las aplicaciones informáticas e instalaciones de las oficinas de acceso restringido.
- Verificación de la desactivación de la cuenta de correo electrónico de la persona saliente.
- Comunicación de la salida a partes interesadas pertinentes (compañeros, etc.).

De acuerdo con los estándares internacionales en materia de GSI, las administraciones tributarias deben disponer de políticas generales de gestión del acceso que engloben todos los accesos (contempladas en los RE 3.2.3.1, respecto del acceso físico, y el RE 3.2.3.3, en relación con el acceso lógico (TI)).

Tabla 10. **Glosario de principales conceptos**

Concepto	Descripción
Controles de acceso	Controles de seguridad que garantizan que el acceso a la información, los espacios físicos y los sistemas esté basado en la necesidad de saber y los derechos mínimos.
Gestión del acceso	Políticas, procesos y procedimientos, de los que son responsables los cargos directivos y no únicamente la función informática de la administración tributaria, que rigen el acceso físico y lógico, así como los procesos efectivos para la concesión y la auditoría del acceso lógico y para la identificación y autenticación de los usuarios.
Concesión de acceso	Otorgamiento efectivo del acceso a información a través de la creación de cuentas de usuario, administración de contraseñas y de la asignación a los usuarios de derechos de acceso específicos y autorizaciones.
Autenticación	Cuando un usuario accede a los sistemas informáticos, el proceso de autenticación asegura y confirma la identidad de dicho usuario de manera irrefutable.
Autorización	Una vez se haya autenticado a un usuario en un sistema, el usuario estará autorizado a acceder a los recursos según los principios de necesidad de saber y de mínimo privilegio.
Identificación	Un proceso utilizado en los sistemas informáticos para identificar únicamente a los usuarios que disponen de un derecho de acceso.
Mínimo privilegio	Principio de gestión del acceso que establece que el acceso legítimo debe restringirse a las funciones específicas mínimas que el usuario necesita para desempeñar sus tareas.
Usuario legítimo	Usuario que obtiene un derecho de acceso específico en base a los principios de necesidad de saber y de mínimo privilegio.
Acceso lógico	Un acceso a sistemas mediante procesos de identificación, autenticación y autorización.
Necesidad de saber	Principio de gestión del acceso que establece que solo debe acceder a la información del contribuyente el personal con un fin de negocio legítimo para ello.
Acceso físico	Un acceso a zonas específicas de las instalaciones.

Por tanto, las administraciones tributarias deben disponer de mecanismos que permitan la adecuada aplicación y administración de dichas políticas, es decir, que protejan de manera adecuada los espacios físicos y la definición de perímetros interiores y exteriores (RE 3.2.3.2) y de mecanismos para permitir de manera eficaz el acceso lógico conforme determinen los responsables del negocio de cada área, y no únicamente el departamento de informática (RE 3.2.3.4).

Esta sección ofrece orientación acerca de la definición de políticas y su implementación. La Tabla 10 contiene las definiciones de los principales conceptos comprendidos en el RE 3.2.3.

Este RE se divide en tres partes:

- Principios generales de la gestión del acceso.
- Orientación sobre seguridad física en las instalaciones de la administración tributaria (RE 3.2.3.1 y RE 3.2.3.2).
- Orientación para implantar una política y controles de acceso lógico (RE 3.2.3.3 y RE 3.2.3.4).

La presente sección no tiene por objeto analizar exhaustivamente el tema de la gestión del acceso. Se limita a destacar aspectos genéricos que pueden aplicarse a todas las administraciones tributarias y se consideran esenciales para la gestión del acceso en el marco de una administración tributaria.

Principios generales de la gestión del acceso

Los estándares internacionales en materia de gestión del acceso se rigen por dos principios, que deben aplicarse sin excepción (véase la Figura 9).

- **Los accesos deben controlarse en base al principio de necesidad de saber**, lo que significa que solo debe acceder a la información del contribuyente el personal que tenga una razón de negocio legítima para hacerlo. Este principio comprende un principio adicional, denominado de mínimo privilegio, bajo el cual el acceso legítimo debe restringirse a las funciones específicas que los usuarios necesitan para desempeñar sus tareas. La aplicación de estos principios garantiza a los contribuyentes la protección de sus derechos de privacidad y, por ende, una comunicación abierta con las autoridades fiscales.

- **Los accesos (físicos y lógicos) deben registrarse**, identificando a las personas individuales que han accedido a las instalaciones o a la información, el momento y la duración del acceso y los detalles de las acciones realizadas. La aplicación de este principio facilita el rastreo de las acciones de las personas pertinentes y, a su vez, desincentiva fuertemente las acciones ilícitas o indebidas.

FIGURA 9. **Principios de la gestión del acceso**

La Tabla 11 indica los tipos de usuarios que pueden acceder de manera legítima a información en el marco de la administración tributaria.

REs 3.2.3.1 y 3.2.3.2. Seguridad del acceso físico

En la presente sección se abordan las políticas de seguridad del acceso físico en cada una de las distintas instalaciones en las que las administraciones tributarias operan, así como los procedimientos y controles para garantizar su eficacia.

Convirtiendo la seguridad física en política(s)

El acceso físico a los edificios de la administración tributaria debe articularse a través de una o varias políticas de seguridad física avaladas por la alta dirección. Por lo tanto, el RE 3.2.3.1 requiere que las administraciones tributarias tengan una política de control del acceso físico de la que es responsable la alta dirección. El RE 3.2.3.2 requiere que las administraciones tributarias protejan de manera adecuada las instalaciones físicas y definan de manera apropiada perímetros de seguridad interiores y exteriores.

Las políticas deben ser consistentes con el tamaño y la complejidad de la administración tributaria, así como orientar a los responsables de gestionar la seguridad física en cada uno de los distintos lugares en que opera la administración.

Las políticas de seguridad física pueden formularse en términos de diseño de seguridad de las oficinas físicas, requerimientos de los usuarios y los controles específicos que se aplican para gestionar el acceso.

Diseño de la seguridad de las oficinas físicas

Las políticas deben definir la variedad de lugares, instalaciones y oficinas en los que la administración

Tabla 11. **Categorías de usuarios legítimos**

Usuario	Descripción
Personal de la administración tributaria	Personal que, como consecuencia del puesto que ocupa, está directamente implicado en el manejo de información de los contribuyentes. Puede incluir personal de la unidad de EOI y ciertas divisiones de cumplimiento encargadas de actividades de análisis de riesgos e inspección que utilicen información intercambiada como, por ejemplo, división de grandes empresas e internacional, división de cumplimiento en jurisdicciones offshore o división de personas físicas con un patrimonio neto elevado.
Contratistas externos de TI	El personal de los proveedores de TI que gestionan servicios por encargo de la administración tributaria, como los encargados de administrar los sistemas y bases de datos que contienen información relativa a los contribuyentes, incluida la información intercambiada, y que también han sido sometidos a una comprobación de antecedentes y procesos de investigación adecuados.
Autoridades supervisoras	Los tribunales, órganos administrativos y órganos de control que participan en la evaluación, recaudación, ejecución, enjuiciamiento y resolución de apelaciones en relación con los impuestos, incluyendo con respecto a información intercambiada bajo un acuerdo internacional. Algunos países han implantado sistemas de portales de información jurídica a través de los cuales se comparten datos con autoridades de supervisión específicas y autorizadas.
Contribuyentes y agentes	La información también puede divulgarse a los contribuyentes interesados y sus representantes autorizados (p. ej. agentes). Las tecnologías modernas permiten a las jurisdicciones introducir mecanismos de autogestión para el contribuyente, bajo los cuales los contribuyentes no solo presentan por sí mismos sus declaraciones de impuestos, sino que además gestionan sus pagos y otros aspectos de sus asuntos fiscales.

tributaria opera, así como determinar sus necesidades de seguridad física en base a los distintos tipos de usuarios que necesitarán acceder a cada una de esas instalaciones.

La principal consideración de diseño a la hora de formular políticas de seguridad física debe ser proteger la información de quienes no necesitan acceder a ella. A tal efecto, deben tenerse en cuenta las siguientes buenas prácticas internacionales:

- Disponer las instalaciones de tal manera que permitan la separación entre usuarios "de confianza" (empleados, contratistas), que tienen derechos de acceso a partes más restringidas o interiores de las instalaciones, y el resto de los usuarios.
- Organizar espacialmente el edificio y las instalaciones de manera que puedan cumplirse los principios de necesidad de saber y mínimo privilegio, así como permitir la separación física de zonas de trabajo más sensibles o en las que se realicen actividades críticas (p. ej. centros de datos o donde se trate información tributaria especialmente sensible, con acceso únicamente de quienes dispongan de niveles más altos de autorización en base a los niveles más altos de confianza, como la unidad de EOI).

Tipos de usuarios y sus requisitos

Todos los diferentes tipos de usuarios con niveles diferentes de derechos de acceso deben tener sus propios requisitos y controles para garantizar que solo accedan a instalaciones respecto de las cuales tengan un propósito legítimo.

La definición de los requisitos de los usuarios requiere valorar quién necesita acceder, a qué y por qué. Las principales categorías de usuarios pueden incluir:

- Personal de la administración tributaria con derecho de acceso a zonas privadas de los edificios.
- Personal con acceso a edificios en los que el acceso está sometido a controles más estrictos como, por ejemplo, los centros de datos.
- Personal de otros departamentos gubernamentales.
- Contratistas de TI y de otros sectores que presten sus servicios, p. ej. personal de limpieza.
- Contribuyentes y representantes tributarios que acudan para tratar asuntos tributarios, o el público en general.

Si la administración tributaria se ubica en instalaciones de las que no es propietaria, es posible que el edificio cuente con otros tipos de usuarios particulares con requisitos de seguridad propios.

Controles para gestionar el acceso físico

Las políticas deben incluir un conjunto estructurado de controles de seguridad física que deben aplicarse dentro de la administración tributaria. Para garantizar que estos controles cumplan los estándares de buenas prácticas, deben estar basados en riesgos y vinculados a las consideraciones de diseño físico y requerimientos de los usuarios.

Tabla 12. **Ejemplo de matriz de seguridad física**

Instalaciones	Tipos de usuarios	Controles
Entrada principal	Personal de la administración tributaria, contratistas informáticos	CCTV en tiempo real, personal de seguridad, revisión de efectos personales.
	Otras autoridades gubernamentales	
	Contribuyentes	
Oficinas internas	Personal de la administración tributaria, contratistas informáticos	Pases electrónicos con fotografía identificativa, torniquetes, CCTV.
	Otras autoridades gubernamentales	Pases provisionales con identificación, torniquetes, CCTV. Acompañamiento en todo momento por el personal de la administración tributaria.
Unidad de EOI / Archivos	Personal de la unidad de EOI	Pases electrónicos con fotografía identificativa, torniquetes, CCTV, sistema de detección de intrusos y alarma, cerraduras con teclado, acceso multifactor a dispositivos informáticos.
Centro de datos	Administradores informáticos	Pases electrónicos con fotografía identificativa, torniquetes, CCTV, sistema de detección de intrusos y alarma, cerraduras con teclado, acceso multifactor a dispositivos informáticos, aire acondicionado, protección contra incendios.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Recuadro 16. Buenas prácticas internacionales en el diseño de controles de seguridad física

Los controles de seguridad física deben estructurarse de manera lógica. Un enfoque lógico utilizaría un enfoque "de afuera hacia adentro" que comenzaría por el control más externo cuando una persona se aproxima al edificio, y trabajando hacia el interior hacia el puesto de trabajo de los usuarios. Este enfoque debe tener en cuenta lo siguiente:

- ¿Cuál es el perímetro más externo? ¿Es el terreno que rodea el edificio, incluidos los aparcamientos? ¿Está controlado el acceso a la zona de aparcamiento y, en caso afirmativo, de qué manera? ¿El terreno está cercado con puertas de acceso y éstas están vigiladas? ¿Existen sistemas de control secundarios tales como CCTV y se supervisan en tiempo real?
- ¿Existe un inventario adecuado de los distintos lugares (p. ej. puertas, puertas en caso de incendios) a través de los cuales los usuarios pueden acceder al edificio o abandonarlo? ¿Existen indicaciones claras en cada tipo de puerta sobre cómo debe usarse y por quién? (p. ej. acceso del personal, acceso de contribuyentes o de ambos, salida de emergencia, punto de acceso para entregas).
- La mayoría de los edificios tendrán una zona de acceso, a menudo un lugar en el que el personal se mezcle con otras personas. ¿Cómo consiguen acceder los distintos usuarios del edificio? ¿Necesitan un pase electrónico? ¿Cómo se emiten y controlan los pases (electrónicos o de otro tipo)? ¿Incluyen una fotografía? Si no incluyen una fotografía, ¿existen otros modos de comprobar que el portador es el legítimo usuario?
- ¿Cuáles son los controles en otras áreas comunes del edificio, tales como los mostradores de atención al público?
- ¿Cómo se accede a las zonas de acceso restringido de un edificio, por ejemplo, insertando un pase electrónico? ¿Deben pasar los usuarios por un torniquete de altura completa (esto es, un control que limita el acceso a las personas de una en una)? Si no hay torniquetes de altura completa, ¿existen controles secundarios, como personal de seguridad? ¿O cámaras de CCTV? Si hay cámaras de CCTV, ¿se supervisan en tiempo real?
- Dentro de las zonas de acceso restringido de un edificio, ¿cómo puede saber el personal si otra persona tiene derecho a estar ahí?
- ¿Cuáles son las normas correspondientes a la gestión de la seguridad física en cada zona de trabajo dentro de los edificios?
- ¿Cuáles son los controles en zonas en las que se realizan las operaciones más sensibles? (p. ej. centros de datos, archivos)
- ¿Qué tipo de controles se aplican normalmente dentro del edificio? Por ejemplo, ¿se usan cámaras de CCTV y, en caso afirmativo, con qué fines? ¿Y cómo se supervisan? Es importante advertir que las cámaras de CCTV no deben colocarse de manera que puedan verse los escritorios, las pantallas de los ordenadores, los archivos, etcétera, ni nada que pueda provocar que la información del contribuyente sea grabada por el sistema de CCTV.
- ¿Existe un espacio público alrededor del edificio (edificios adyacentes, viviendas) que pudiera usarse para vulnerar la confidencialidad, y qué controles se aplican a este respecto?

¿Un enfoque alternativo?

Otro enfoque podría ser dividir la lista de control en:

- Controles básicos que constituyan el grupo de controles mínimos.
- Todos los controles adicionales o reforzados que se apliquen en respuesta a un riesgo o problema específico.

Puede elaborarse una lista completa de controles como, por ejemplo, en forma de matriz que incluya las distintas zonas del edificio o los distintos tipos de accesos, los tipos de usuarios y sus derechos de acceso, y los controles relevantes. La Tabla 12 muestra un ejemplo simplificado de una matriz de seguridad física, y los recuadros 16 y 17 ofrecen una orientación más pormenorizada, así como ejemplos de las estrategias a considerar en el diseño de controles de seguridad física.

Comprobación de los controles de seguridad física

Debe haber un sistema que permita comprobar si los controles de seguridad previstos en la política se aplican de manera correcta y eficaz en la práctica.

Las mejoras de los controles deben basarse en comprobaciones previas realizadas de conformidad con los planes de comprobación. A su vez, los planes de comprobación deben readaptarse cuando sea necesario, a partir de las conclusiones del plan vigente.

En general, cuando se evalúen o comprueben los controles de seguridad física, deben tenerse en cuenta los siguientes aspectos:

- Las evaluaciones de la seguridad física deben actualizarse periódicamente y basarse en las conclusiones y lecciones aprendidas de anteriores evaluaciones y/o incidentes, aplicando una combinación de comprobaciones aleatorias y basadas en riesgos.

Recuadro 17. **Ejemplo de evaluación de los controles de seguridad física**

La división de Gestión de la Seguridad Física de la administración tributaria de la Jurisdicción A comprueba al menos una vez al mes que los controles físicos funcionen. Esto incluye comprobaciones técnicas de las cerraduras, alarmas y cámaras de vigilancia. Cada tres años un proveedor de servicios externo audita la seguridad física.

Todos los fallos del sistema de control de accesos se reportan a la división de Gestión de la Seguridad Física. Si existe evidencia de acceso indebido a las instalaciones, se inicia una investigación dirigida a determinar si se han causado daños materiales (p. ej. bienes robados o dañados) o se ha producido una posible violación de datos (en papel o digital). Los resultados y conclusiones de la investigación se documentan y utilizan para subsanar el fallo en los controles que causó el incidente.

Los centros de datos están vigilados y disponen de un sistema de control de acceso electrónico que requiere identificación biométrica. Los reportes que contienen los registros de acceso al centro de datos se revisan quincenalmente. Los centros de datos disponen de sistemas propios de CCTV.

- Los incidentes y eventos relacionados con la seguridad física deben comunicarse de inmediato a los administradores del edificio, y registrarse y documentarse (los controles de gestión de incidentes se describen con mayor detalle en el RE 3.2.6.6). Si los incidentes no se comunican y registran debidamente, podría obtenerse una falsa impresión de que el sistema funciona. Pueden existir distintos tipos de incidentes, en función de los distintos niveles de gravedad e impacto, tales como que los empleados pierdan su pase de seguridad, los intentos de acceso indebido a los edificios, la circulación de personas de una zona a otra sin insertar pase de seguridad alguno, el robo de material de oficina, etc. El personal debe estar concienciado de la importancia de reportar un incidente, y el formato de reporte debe contener los detalles del incidente a fin de que puedan adoptarse medidas adecuadas.
- Las evaluaciones de los controles de sitios críticos (p. ej. centros de datos, unidad de EOI, archivos) deben tener en cuenta la posibilidad de usar controles adicionales acordes a la clasificación de la información que se trata en esas oficinas (véase el RE 3.2.5.1 sobre protección de la información) y evaluaciones de riesgos institucionales (véase el RE 3.2.1.4 sobre gestión del riesgo).

REs 3.2.3.3 y 3.2.3.4. Acceso lógico

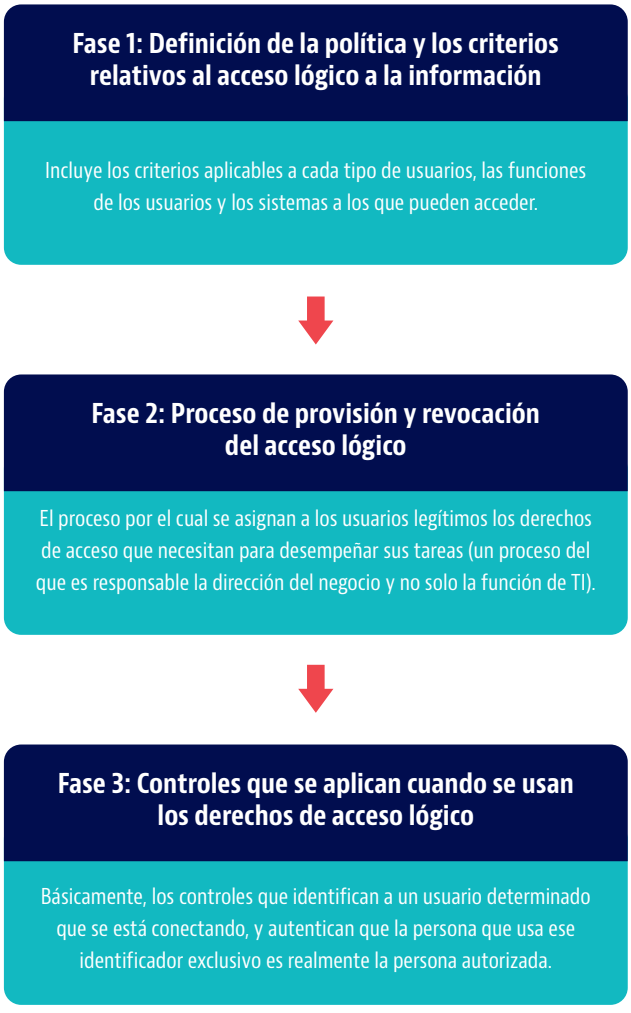
En esta sección se aborda el enfoque general de diseño y comprobación de controles adecuados de acceso lógico (TI) a datos conservados por medios electrónicos en distintos sistemas informáticos.

El RE 3.2.3.3 requiere que las administraciones tributarias tengan una política de control de acceso lógico de la que sea responsable la alta dirección y que se base en los principios de necesidad de saber y mínimo privilegio. El RE 3.2.3.4 requiere que las administraciones tributarias adopten políticas, procesos y procedimientos, de los que sea responsable la alta dirección y no solo la función de TI de la organización, que regulen el acceso lógico, y procedimientos eficaces para la provisión y la auditoría del acceso lógico y para la identificación y autenticación de los usuarios.

Fase de gestión del acceso lógico

Los requisitos están reflejados en términos generales en tres fases de gestión del acceso lógico, tal como muestra la Figura 10.

FIGURA 10. **Fases de gestión del acceso lógico**



Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Tabla 13. **Definición de la política y los criterios relativos al acceso lógico a la información**

Consideraciones que orientan la definición	Quién define los criterios relativos al acceso al sistema de información
• La política en materia de acceso lógico debe reflejar los principios de necesidad de saber y mínimo privilegio, esto es, establecer que los usuarios solo deben tener los derechos de acceso que necesiten para hacer su trabajo o desempeñar sus funciones y que el acceso legítimo debe restringirse a las funciones específicas que los usuarios necesiten. • En la medida en que los tipos de funciones de los usuarios sean diferentes en función de los distintos procesos tributarios, deberán adoptarse controles adecuados para garantizar la coherencia entre los criterios de todos los sistemas. • Los derechos de acceso pueden variar en función del lugar donde se conserven los datos: centros de datos en las instalaciones de la administración tributaria, centros de datos externalizados o en la "nube". [14] [15] • Pueden haber derechos de acceso y políticas en materia de uso de aplicaciones informáticas tales como el correo electrónico y navegadores de Internet para fines no profesionales. • Pueden haber derechos de acceso relativos al trabajo fuera del entorno de oficina, especialmente de acceso seguro a datos confidenciales cuando se trabaja desde fuera de las Redes de Área Local (*Local Area Networks*) dentro de las oficinas de la administración tributaria.	Los criterios de acceso lógico a información deben ser determinados por las personas responsables del proceso de negocio que utiliza la aplicación tributaria relevante, y refrendados por la alta dirección de la administración tributaria. Los altos directivos son responsables del funcionamiento de los sistemas de la administración tributaria, por lo que deben ser ellos quienes decidan en última instancia cómo debe ser el diseño de los controles de acceso. Por ejemplo, el alto funcionario de la administración tributaria encargado de la gestión del sistema de AEOI debe ser responsable de determinar los criterios de acceso a ese sistema. Si los controles de gestión del acceso fueran demasiado laxos podría verse comprometida la confidencialidad, y si fueran demasiado estrictos podría verse perjudicada la eficiencia operativa. Como sucede con muchas cuestiones relacionadas con la seguridad, existe un delicado equilibrio entre confidencialidad y accesibilidad. Las consecuencias de romper este equilibrio son de tipo operativo, no son consecuencias informáticas. No obstante, una buena práctica sería definir los criterios de forma conjunta con el departamento de TI. Este departamento tiene conocimientos técnicos acerca de las ventajas y desventajas de la provisión de acceso, así como de las áreas concretas en las que puede ser necesario imponer restricciones: por ejemplo, las que cuentan con altos privilegios de acceso, como las funciones de administrador. Los administradores son usuarios que suelen ser responsables de la administración de la infraestructura de TI dentro de la red de la administración tributaria, y no deberían disponer normalmente de acceso a Internet, incluido el correo electrónico, como parte de su función de administrador.

Fase 1: Definición de la política y los criterios relativos al acceso lógico a la información.

La Tabla 13 resume la definición de los criterios relativos al acceso lógico a la información.

Fase 2: Proceso de provisión y revocación del acceso lógico

Aprovisionamiento del acceso lógico

Una vez se hayan determinado los criterios de los derechos de acceso lógico, la siguiente fase consiste en aprovisionar efectivamente el acceso a la información, es decir, otorgar a los usuarios derechos de acceso predefinidos con respecto a su función concreta (véase el Recuadro 18). La provisión de acceso lógico es relevante en ciertas circunstancias tales como:

- Cuando se contrata nuevo personal que necesita acceso.
- Cuando un miembro del personal cambia de puesto o funciones (p. ej. un funcionario de la administración tributaria es trasladado de una división de proyectos a una de cumplimiento, por lo que necesita acceder a información del contribuyente).
- Cuando el personal asuma nuevas funciones o responsabilidades adicionales a las que tiene en la actualidad (p. ej. se encomienda a un directivo la gestión de sujetos pasivos del impuesto sobre sociedades y del impuesto sobre personas físicas).
- Solicitudes de acceso específicas para funciones concretas.

No se pretende que esta lista sea exhaustiva, pues puede haber otras circunstancias a tener en cuenta. En cualquier caso, como parte del aprovisionamiento de acceso lógico, las administraciones tributarias deben definir cada una de las diversas circunstancias en las que puede ser necesario conceder acceso lógico a aplicaciones de TI, sistemas o servicios.

14. Los detalles de los controles que deben aplicarse cuando se utilizan servicios de proveedores externos se describen en el RE 3.2.4.4.

15. Los departamentos gubernamentales están considerando cada vez más el uso de servicios en la "nube" en lugar de centros de datos controlados por el propio departamento.

Recuadro 18. **¿Por qué es tan importante el aprovisionamiento efectivo de acceso lógico?**

La provisión de acceso efectiva permite que el personal de la administración tributaria adquiera oportunamente los derechos de acceso legítimos que necesitan para desempeñar sus tareas. No obstante, si no existe una ruta clara para lograrlo, es posible que esas personas generen procesos de acceso ad hoc que les permitan seguir desempeñando sus tareas. Es improbable que dichos procesos ad hoc se ajusten a los principios de seguridad y confidencialidad.

A modo de ejemplo hipotético, la administración tributaria de la Jurisdicción B no ha adoptado procedimientos formales, controlados por la alta dirección, a fin de conceder acceso en base a las funciones. En cambio, existen prácticas manuales y ad hoc entre las divisiones operativas y el departamento de TI para el aprovisionamiento de derechos de acceso específicos. En ciertos casos, cuando un miembro del personal necesita un acceso determinado, envía simplemente un correo electrónico a un colega del departamento de TI que concede dicho acceso sin que intervenga la dirección. En otros casos, la solicitud de acceso recibe la aprobación previa del supervisor del empleado antes de su envío al departamento de TI, pero incluye derechos que no son necesarios para que el empleado desempeñe sus funciones laborales. En este caso no se conservan registros de auditoría de la concesión de acceso. Durante una evaluación de los estándares de confidencialidad, se recomendaría a esta jurisdicción elaborar y aplicar un proceso de gestión del acceso, junto con procedimientos formales para el aprovisionamiento y revocación de derechos de acceso lógico.

Revocación del acceso lógico

Otro requisito crítico es la capacidad de retirar o revocar los derechos de acceso (véase el ejemplo del Recuadro 19). El pirateo de los derechos de acceso se reconoce como una causa significativa de violaciones de datos. Por ello, las administraciones tributarias deben tomar las debidas precauciones a fin de garantizar en todo momento que los únicos accesos al sistema disponibles en cualquier momento son los requeridos por los usuarios legítimos. Las situaciones que se espera que queden cubiertas por los mecanismos de revocación incluirían:

- **Personal saliente**. Los derechos de acceso deben revocarse el último día de trabajo, si no antes. Cuando se extingue la relación laboral de una persona por circunstancias específicas como una conducta indebida, debe ser posible revocar los derechos de acceso de manera inmediata.
- **Cambio de puesto o funciones**. Los derechos de acceso deben revocarse tan pronto como se cese en el antiguo puesto y en el momento en que se concedan nuevos derechos de acceso, o antes.
- **Retirada provisional**. Por ejemplo, si el miembro del personal se ausenta durante largos períodos por vacaciones o enfermedad, o cuando se estén llevando a cabo investigaciones de conducta indebida.
- **Acceso no utilizado**. Los derechos de acceso que no se estén usando deben ser revocados.
- **Acceso temporal**. Debe ser posible la concesión, con carácter general, de acceso temporal, de modo que el proceso revoque de manera automática el acceso una vez transcurrido cierto período de tiempo (y puede existir un proceso asociado para restaurar el acceso inmediatamente, cuando sea necesario).

Controles de procedimiento tras la concesión del acceso lógico

Una vez concedido el acceso a los sistemas, deben llevarse a cabo verificaciones del procedimiento adecuadas con el fin de garantizar que solo los usuarios legítimos tengan realmente derechos de acceso (véase el ejemplo del Recuadro 20). Las verificaciones del procedimiento pueden incluir:

- Verificaciones periódicas por parte del personal especializado, los superiores o los altos directivos que aprobaron la solicitud de acceso, a fin de verificar que:
  - Las personas que aparecen como titulares de derechos de acceso son realmente usuarios legítimos.
  - Las personas a las que se ha concedido el acceso son realmente usuarios actuales (por ejemplo, que siguen cumpliendo esa función o que no se han jubilado).
- Verificaciones periódicas por parte de la función de auditoría interna.

Fase 3: Controles que se aplican cuando se usan los derechos de acceso lógico

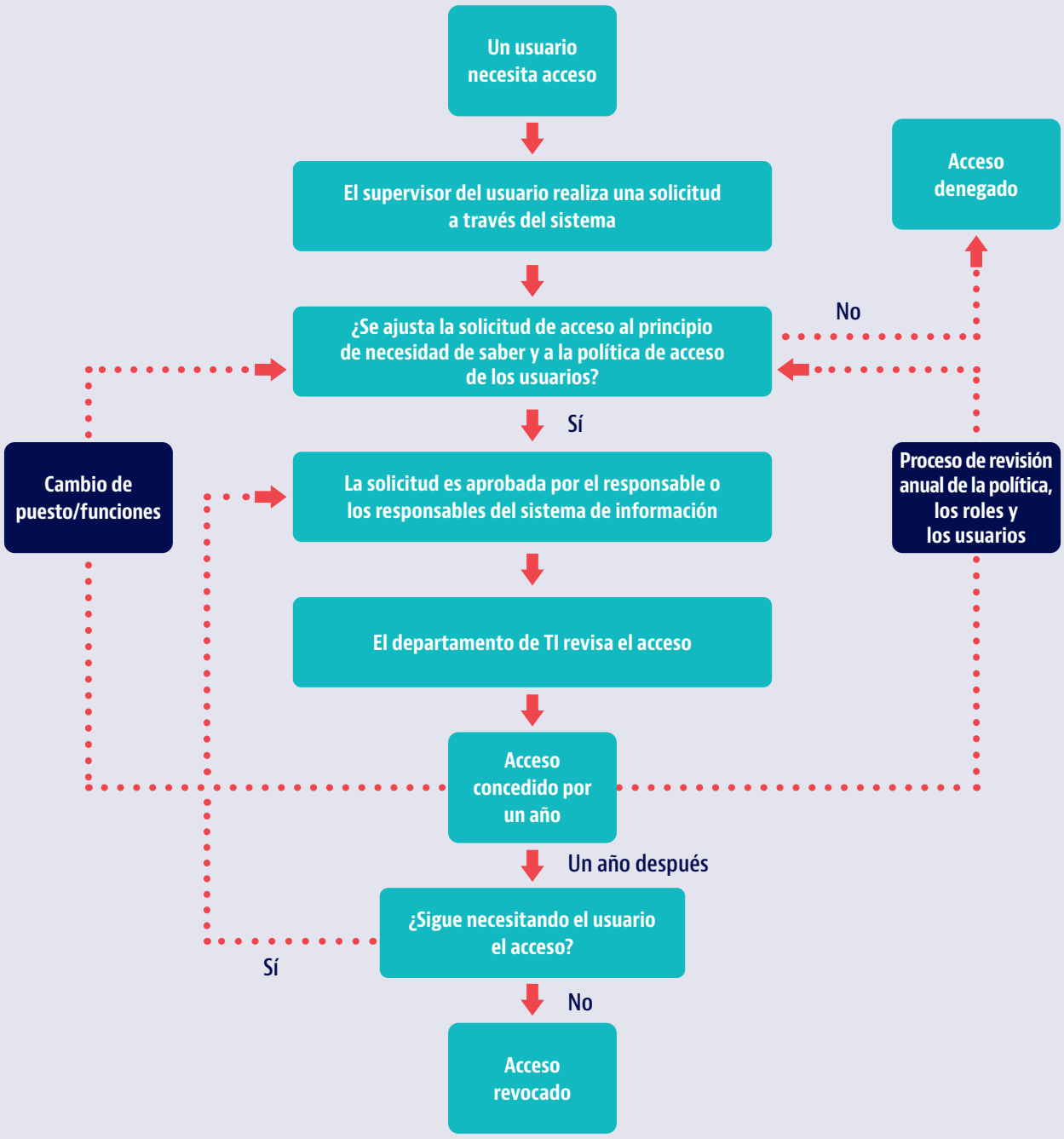
Una vez que los usuarios reciben derechos de acceso a los sistemas de información, tendrán que acceder a esos sistemas o 'iniciar sesión' en ellos. Las administraciones tributarias deben garantizar que los usuarios puedan identificarse y autenticarse de forma única cada vez que acceden a un sistema.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Recuadro 19. **Ejemplo de aprovisionamiento y revocación de acceso lógico**

En la administración tributaria de la Jurisdicción C, el acceso de los usuarios a varios sistemas de información ha sido preestablecido en base a las funciones del puesto, y se basa en la "Política de Provisión y Revocación de Acceso del Usuario en los Sistemas de la Administración Tributaria de la Jurisdicción C". La concesión de accesos a los usuarios exige la aprobación de su supervisor (como mínimo, del jefe de unidad). Así, los accesos deben ser refrendados por los responsables del sistema de información respectivos, y solo los cargos directivos pueden ser designados como responsables del sistema. Tras la aprobación por parte de dichos responsables, el departamento de TI revisa y concede el acceso como parte de un último procedimiento de verificación técnica.

La siguiente figura muestra un ejemplo del proceso de aprovisionamiento y revocación:



Recuadro 20. **Ejemplo de controles de procedimiento de acceso lógico**

La administración tributaria de la Jurisdicción A ha designado un equipo de coordinadores de derechos de acceso para revisar los derechos concedidos a todos los usuarios, tanto empleados como contratistas. Una vez concedidos los derechos, los coordinadores envían correos electrónicos de confirmación a los supervisores y cargos directivos con el fin de verificar que han aprobado realmente las solicitudes de acceso. Este equipo de coordinación también verifica periódicamente la validez de todos los derechos de acceso, así como la supresión de todas las cuentas y accesos obsoletos. Estas comprobaciones se reportan, revisan y ratifican por el responsable de impuestos sénior encargado del sistema de información, así como por el departamento de recursos humanos. La frecuencia de las comprobaciones varía en función de las clasificaciones de los sistemas, pero se llevan a cabo, como mínimo, con periodicidad semestral.

Identificación

Todos los usuarios de sistemas de TI deben disponer de uno o varios identificadores exclusivos a fin de cumplir con el principio de que todas las acciones deben poder asociarse a personas identificables.

Sería posible que un usuario tuviese múltiples identidades como, por ejemplo, si tuviese funciones de acceso con distintos niveles de privilegio, pero estas identidades deben seguir siendo exclusivas del usuario en cuestión. Cuando, de manera muy excepcional, no sea posible usar identificadores exclusivos, deben aplicarse controles compensatorios como, por ejemplo, una combinación de un registro de control con una autorización de la dirección.

Autenticación

La identificación debe reforzarse con exigencias de autenticación. La forma estándar de autenticación es una contraseña, o grupo de caracteres conocidos únicamente por la persona que posee el identificador exclusivo. El Recuadro 21 describe una serie de buenas prácticas internacionales en materia de gestión de contraseñas y cuentas de usuario.

Pueden utilizarse otros tipos de requerimientos de autenticación, además de contraseñas. Un ejemplo es el uso de identificadores de estaciones de trabajo. Pueden utilizarse estaciones de trabajo (ordenadores de escritorio, portátiles, etc.) habilitados por una administración tributaria con identificadores exclusivos para obtener una garantía adicional como parte del proceso de autenticación. Por ejemplo, solicitar la introducción del identificador exclusivo del ordenador de escritorio o portátil después de la contraseña de usuario, con el fin de acceder. Aunque este tipo de asociación puede ser útil para conseguir una mayor seguridad en el proceso de autenticación, también puede resultar restrictivo, desde un punto de vista operativo, vincular a los usuarios con su propia máquina. Este factor debe tenerse en cuenta antes de optar por el uso de identificadores de estaciones de trabajo u otras opciones de autenticación adicionales.

Autenticación multifactor

Puede haber situaciones especiales en las que sea necesario establecer controles de autenticación adicionales o una "autenticación multifactor". Existen tres tipos de autenticadores: algo que se sabe, p. ej. una contraseña; algo que se tiene, p. ej. un token; y algo que se es, p. ej. una huella dactilar. La administración tributaria debe escoger al menos dos de los tres autenticadores para establecer una autenticación multifactor.

Entre las situaciones que pueden requerir una autenticación multifactor se incluyen:

- **Datos sensibles**. En caso de datos sensibles como, por ejemplo, información intercambiada, puede

Recuadro 21. **Buenas prácticas internacionales en materia de gestión de contraseñas y cuentas de usuario**

Gestión de contraseñas. Las prácticas pueden incluir limitaciones o requisitos mínimos en relación con el tipo y la cantidad de contraseñas que pueden utilizarse, restricciones relativas al número de intentos fallidos de introducción de la contraseña y la exigencia de cambiar periódicamente las contraseñas. Por ejemplo, una longitud mínima de la contraseña de al menos 10 caracteres alfanuméricos, el bloqueo de la cuenta tras 5 intentos de acceso fallidos y el cambio de contraseñas cada 90 días o menos.

Gestión de sesiones. Las prácticas pueden incluir el bloqueo de ordenadores de escritorio cuando no se están utilizando y barreras (*back-stop*) para proteger la información si los usuarios no bloquean sus dispositivos. Por ejemplo, los ordenadores de escritorio pueden configurarse por defecto para que caduquen y exijan una nueva autenticación del usuario después de 10 minutos sin actividad del usuario.

Cuentas inactivas. Las prácticas pueden incluir el monitoreo del uso de la cuenta y la desactivación de las cuentas que no se usan. Por ejemplo, las cuentas a las que no se haya accedido en un período de al menos 30 días consecutivos serán inhabilitadas.

ser necesario adoptar controles de autenticación más estrictos. Esos controles pueden incluir una autenticación de dos factores estándar (p. ej. una contraseña muy segura, acompañada de un token de seguridad o biometría), pero podrían reforzarse aún más con controles de autenticación adicionales como, por ejemplo, vinculando al usuario con una estación de trabajo específica (ordenador de escritorio, portátil, etc.) ubicado en una habitación muy protegida. Con independencia de los controles que se utilicen para proteger datos sensibles, el grado de control debe basarse siempre en una evaluación de riesgos rigurosa, y es preciso encontrar un equilibrio entre la necesidad de confidencialidad y la necesidad de accesibilidad.

- **Administradores**. Respecto de los usuarios que trabajan en el departamento de TI que tienen acceso privilegiado en calidad de administradores a infraestructuras y sistemas de TI, a menudo denominados "administradores" o "súper usuarios", normalmente estará justificada la adopción de controles de autenticación adicionales. La buena práctica internacional para este tipo de usuario es aplicar una autenticación de, como mínimo, dos factores más controles adicionales que pueden incluir:
  - La concesión de acceso privilegiado durante un período de tiempo limitado, de modo que el derecho de acceso esté sujeto a verificaciones periódicas y se revise el desempeño antes de que pueda restablecerse por un período adicional.
  - La norma de que los usuarios privilegiados deben trabajar en pareja, con el fin de que cada uno supervise las actuaciones del otro.
  - El uso de paquetes comerciales estandarizados específicamente destinados a la gestión de accesos privilegiados.
- **Acceso remoto de los usuarios**. El acceso a información del contribuyente está controlado estrictamente, y fuera de la oficina se limita únicamente a funciones y tipos de acceso al sistema específicos. Cuando se permita el acceso externo a datos sensibles, los riesgos deben medirse y mitigarse de manera eficaz. Los principales desafíos no son técnicos (ya que existen métodos muy eficaces de cifrado de la información), sino en relación con el control eficaz del acceso del usuario a su dispositivo (p. ej. portátil o tableta).

REQUISITO ESPECÍFICO 3.2.4: SEGURIDAD DEL SISTEMA DE TI

El RE 3.2.4 se refiere a la protección de la información mediante la protección de la infraestructura (tanto del software como del hardware) en la que se conserva la información y a través de la cual se emplea y utiliza. La protección de la información en sí se analiza en la siguiente sección, el RE 3.2.5.

Bajo el RE 3.2.4, se espera de las administraciones tributarias que:

- RE 3.2.4.1: Hagan que la seguridad forme parte de la prestación de servicios de TI en apoyo de las funciones del negocio, adopten un plan de seguridad para las aplicaciones del negocio y armonicen sus sistemas con la seguridad.
- RE 3.2.4.2: Implanten una serie adecuada de controles de seguridad de TI.
- RE 3.2.4.3: Gestionen debidamente sus activos de TI.
- RE 3.2.4.4: Gestionen debidamente la prestación de servicios por parte de los proveedores.
- RE 3.2.4.5: Garanticen la continuidad de los servicios de TI y su resiliencia ante fallos.

La Tabla 14 contiene las definiciones de los principales conceptos comprendidos en el RE 3.2.4.

RE 3.2.4.1. Hacer que la seguridad forme parte de la prestación de servicios de TI

Los sistemas informáticos no se encuentran en un vacío: respaldan la gestión eficaz y la automatización de las actividades y procesos operativos del negocio de las administraciones tributarias. Por lo tanto, todas las funciones de TI, incluidas las de gestión de la seguridad de la información, deben alinearse estrechamente con las necesidades de las operaciones y los procesos de negocio que respaldan. Las administraciones tributarias deben entonces tomar una decisión sobre cómo implementar la seguridad de TI.

Alineando la TI y la seguridad con las funciones del negocio

Para lograr la alineación, durante los procesos de diseño de las TI debe haber un nivel alto de compromiso entre la función de TI y los gerentes y usuarios de los procesos de negocio tributarios. La administración tributaria debe identificar, por tanto, a las personas responsables de asegurar la comunicación entre esas partes interesadas. Sin dicho compromiso, los sistemas de TI podrían no lograr lo que los procesos de negocio les requieren, lo que a su vez podría crear problemas que pongan en peligro la confidencialidad y la integridad de la información.

Tabla 14. **Glosario de principales conceptos**

Concepto	Descripción
Gestión de activos	Proceso que garantiza que los activos de la administración tributaria se identifiquen y rastreen desde su creación o adquisición hasta su destrucción o eliminación.
Controles básicos	Conjunto de controles de seguridad mínimos que una administración tributaria aplica a ciertos riesgos, con independencia de su gravedad.
Firewall	Equipo instalado en puntos estratégicos de una red (normalmente frente al acceso externo o interno y zonas internas divididas) que permite o bloquea el tráfico en base a ciertas reglas.
Control de seguridad de TI	Medida administrativa, técnica o física implantada para mitigar un riesgo de TI.
Malware	Software malicioso. Programa creado para explotar una vulnerabilidad en un sistema seleccionado con el fin de dañarlo o sustraer información.
Externalización	Recurrir a un proveedor externo para el suministro de bienes y servicios.
Pruebas de penetración	Las pruebas de penetración simulan las acciones de un pirata informático contra la organización.
Recuperación	Se refiere a la restauración de servicios y operaciones en caso de fallo grave.
Resiliencia	Se refiere a la mitigación del riesgo de interrupción del servicio y la garantía de tolerancia a los fallos en los servicios, proporcionando la continuidad del servicio hasta cierto punto.
Acuerdo de Nivel de Servicio	Acuerdo que establece un nivel de servicio mínimo que debe cumplir una entidad que presta un servicio.
Gestión de proveedores	Proceso basado en el riesgo que garantiza que un proveedor externo que acceda a los datos o instalaciones de una administración tributaria no ponga en riesgo la confidencialidad y seguridad.

La integración de la seguridad en la TI y la alineación de la TI al negocio, requieren un departamento de TI bien organizado. Un departamento de TI debe:

- Identificar y definir sus funciones, definiendo con claridad los perímetros funcionales (p. ej. calidad, desarrollo y asistencia).
- Identificar las personas de contacto claves en los departamentos del negocio.
- Reunirse periódicamente con las partes interesadas de los departamentos del negocio.

Un organigrama (véase el ejemplo de la Figura 11) que muestre los flujos de comunicación entre el departamento de TI y otras áreas (incluidas la de gobierno, seguridad y unidades del negocio) ayudará a identificar quién debe determinar y comunicar los requisitos de seguridad para los procesos del negocio, así como las soluciones de TI que los apoyan.

Son muchas las variables que influyen en el modo en que las administraciones tributarias estructuran su función de TI, cómo ésta sirve de apoyo a las funciones operativas y cómo se implantan los controles de TI (véase la Tabla 15).

Con independencia de la organización de TI que se adopte, deben tenerse en cuenta sus efectos sobre la gestión de TI y de seguridad de la información. Esta consideración debe conducir a la adopción de estructuras y procesos de gobierno adecuados que garanticen una integración entre la seguridad de TI y las operaciones cotidianas de la administración tributaria. Las administraciones tributarias deben establecer también procedimientos claros que garanticen la priorización de las cuestiones de seguridad a la hora de implementar proyectos de TI, incluidos el órgano o las personas concretas que son responsables.

Implementando la seguridad informática

Después de haber decidido una estructura adecuada que integre la seguridad de TI, una administración tributaria tendrá que adoptar también decisiones relativas a la implementación de sistemas y seguridad de TI. Las cuestiones que deben tenerse en cuenta incluyen:

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

- ¿Los servicios de TI se desarrollarán internamente, externamente o de ambas maneras (tanto en términos de aplicaciones como de sistemas de TI)? (véase el Recuadro 22).
- ¿Quién decidirá y quién será responsable de los diferentes servicios de TI?
- ¿Cómo se garantizará que las evaluaciones de seguridad en el desarrollo o la adquisición de servicios y aplicaciones de TI se lleven a cabo adecuadamente?
- ¿Cómo se incorporará en la práctica la seguridad en las TI (es decir, en el diseño de entornos de TI, el desarrollo de nuevos sistemas, los cambios en los sistemas existentes, así como en la infraestructura subyacente)?

Un proceso esencial para lograr la integración entre sistemas de TI, seguridad y sistemas del negocio consiste en la gestión del cambio, cuestión que se analiza con más detalle en el RE 3.2.6.5. Los cambios en los sistemas pueden plantear riesgos adicionales o afectar negativamente a la eficacia de los controles de seguridad ya implantados. La gestión del cambio, por lo tanto, garantiza que el diseño y el cambio en los sistemas de TI sean procesos controlados que tienen en cuenta las exigencias de seguridad e incorporan una evaluación de impacto adecuada.

RE 3.2.4.2. Implantar una serie adecuada de controles de seguridad de TI

Las administraciones tributarias deben implantar controles de seguridad de TI teniendo en cuenta los distintos insumos que permiten determinar qué controles se aplican, y cómo se aplican. Estos insumos incluyen información obtenida de la gestión de incidentes y problemas (RE 3.2.6.6), la gestión de las

FIGURA 11. **Ejemplo de organigrama que muestra los flujos de comunicación entre el departamento de TI y otras áreas**

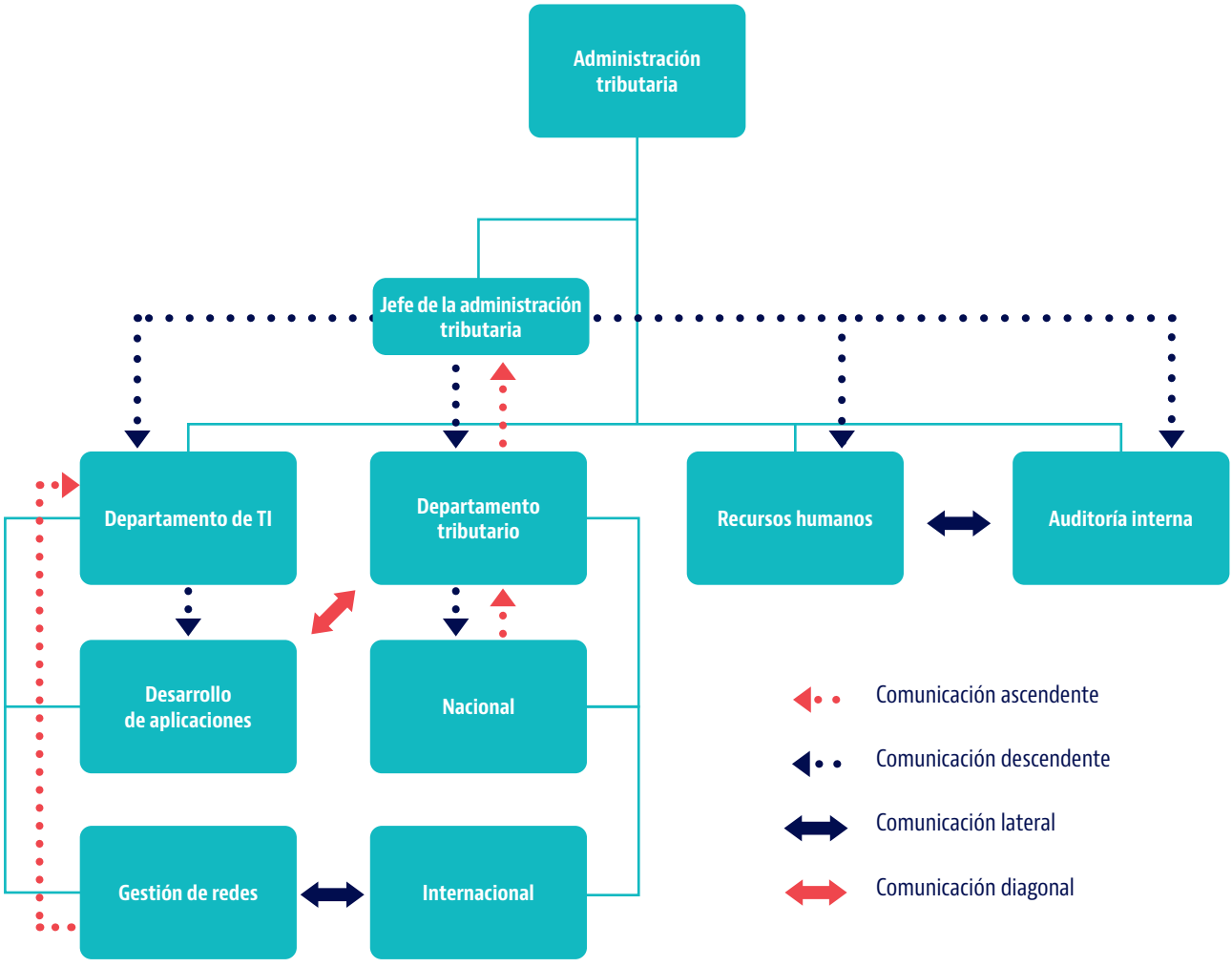


Tabla 15. **Ejemplos de variables que influyen en el modo en que se estructura la función de TI**

Tamaño de la administración tributaria	Externalización de funciones de TI	Enfoque del ciclo de vida	Armonización del sistema de TI
En administraciones grandes o más complejas, la función de TI podría incluir actividades muy diferentes, como la arquitectura de TI, el diseño, el desarrollo, la gestión de proyectos, la gestión de entregas de software, operaciones, administración de servicios y gestión de la seguridad de TI. Estas actividades podrían estructurarse en sub departamentos. En administraciones más pequeñas, no obstante, puede haber un único departamento que desempeñe todas esas actividades. Una parte o la totalidad de las actividades y las decisiones técnicas asociadas podrían externalizarse, por ejemplo, a través de la adquisición de soluciones de TI estándar.	El propio departamento de TI podría ser externo a la administración tributaria. Por ejemplo, una función de TI separada dependiente del Ministerio de Hacienda, que preste servicios de TI a todos los departamentos ministeriales. En otros casos, algunas o todas las funciones de los departamentos de TI podrían externalizarse a empresas privadas, incluida la prestación de servicios de escritorio.	Las actividades que respaldan la prestación de servicios de TI pueden estructurarse en períodos del ciclo de vida de TI, con equipos dedicados a cada parte del ciclo de vida (p. ej. diseño, desarrollo, entregas de software y operaciones). La estructura podría determinar cómo los distintos equipos del departamento de TI responsables de cada parte colaboran entre ellos, así como las unidades del negocio y los usuarios de TI.	La integración de la seguridad de la información en la prestación de servicios de TI podría simplificarse si los sistemas de TI están armonizados, de modo que se utilicen pocas soluciones, pero que sean las mismas para toda la infraestructura. Las administraciones tributarias con un alto grado de armonización pueden comprobar que esto les ayuda a reducir costes y gestionar los problemas de seguridad. La armonización podría aplicarse también a dispositivos móviles y equipos conectados desde fuera de la administración tributaria (p. ej. teletrabajo y dispositivos móviles que accedan a la red de la administración tributaria).

vulnerabilidades (RE 3.2.6.4) y, de manera aún más importante, la gestión del riesgo (RE 3.2.1.4).

Dependiendo de cómo se estructure la función informática, el enfoque para la implantación de los controles puede formalizarse o documentarse en mayor o menor medida. Con independencia de dicho enfoque, debe quedar claro dentro de la función de TI y la administración tributaria cómo los distintos insumos contribuyen a adoptar decisiones sobre la aplicación de los controles de TI. Esto permite la trazabilidad por parte del personal del equipo de TI encargado de administrar los controles. Esas personas también tienen que comprender de forma clara los impactos que produce cualquier cambio en el sistema, de modo tal que puedan actuar en consecuencia con el fin de asegurarse de que los controles vigentes siguen funcionando de manera adecuada.

Como se muestra en la Figura 12, los controles de seguridad de TI (y los controles de seguridad en general) incluyen:

- **Controles básicos**: Controles mínimos aplicados como consecuencia de la identificación inicial por la administración tributaria de riesgos específicos, con independencia de su gravedad.

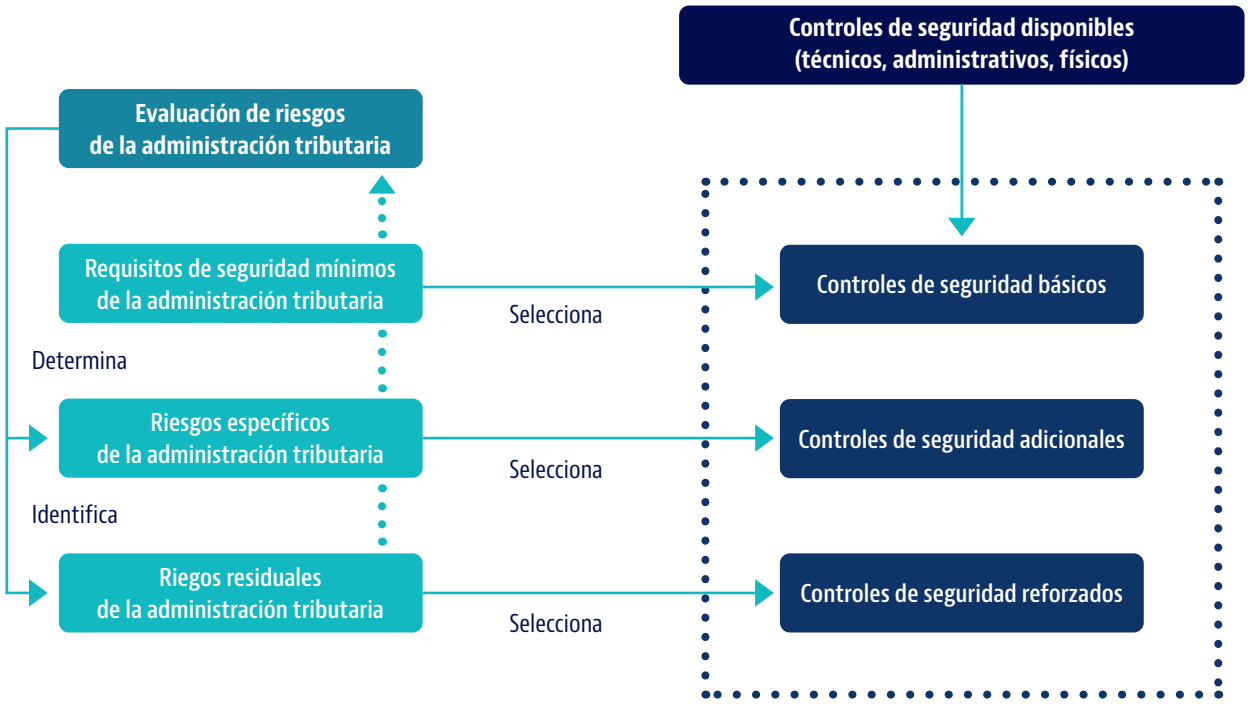
Recuadro 22. **Posibles ventajas y desventajas del desarrollo a nivel interno o externo de los servicios de TI**

Desarrollo interno
Entre las ventajas se incluyen una mejora del control interno de los servicios de TI, relaciones de confianza más sólidas y mayor confidencialidad. Entre las desventajas se encuentran la necesidad de desarrollar capacidades y conocimientos internos, programas de formación intensiva o mayores gastos.

Desarrollo externo
Entre las ventajas se incluyen la mejor capacidad de la función de TI para centrarse en las actividades esenciales de la administración tributaria, el acceso a nuevas tecnologías, la reducción de los gastos corrientes y una mayor flexibilidad. Entre las desventajas pueden incluirse la necesidad de supervisar a los terceros proveedores y sus empleados, los posibles desencuentros culturales entre el proveedor y el personal interno o problemas de confidencialidad.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

FIGURA 12. **Tipos de controles de seguridad**



- **Controles adicionales**: Medidas adicionales implantadas para mitigar los riesgos identificados, en base al nivel de gravedad del riesgo evaluado. Tal y como se analiza en el RE 3.2.1.4, al identificar sus riesgos, las administraciones tributarias tendrán que decidir, con respecto a cada riesgo, de qué manera desean gestionarlo, decisión que incluye qué controles se van a aplicar. Los controles se aplicarían, por lo tanto, en función de la tolerancia al riesgo de una administración tributaria.

- **Controles reforzados**: Controles que ayudan a hacer frente a amenazas avanzadas, tales como tecnologías para detectar y prevenir la exfiltración de datos (es decir, la transferencia no autorizada de datos).

Se espera que las administraciones tributarias evalúen la eficacia de los controles de seguridad aplicados, preferiblemente con el uso de indicadores mensurables, y adopten un proceso formal para llevar a cabo esas revisiones.

La naturaleza de cada tipo de control puede ser administrativa (p. ej. una política o proceso), física (p. ej. cámaras de vigilancia) o técnica (p. ej. un firewall o un software). Puede ser necesario combinar distintos tipos de controles para mitigar un único riesgo (véanse los ejemplos de la Tabla 16). Los distintos tipos de controles se analizan a su vez.

Controles básicos

Dependiendo de la sensibilidad de la información alojada en un sistema, y el nivel de confidencialidad requerido, se elegirán los controles básicos correspondientes. El Recuadro 23 contiene ejemplos de controles básicos comunes basados en riesgos de seguridad de TI.

Tabla 16. **Ejemplos de controles básicos, adicionales y reforzados**

Controles básicos	Antivirus, registro y seguimiento	CCTV, sistema de iluminación	Política de contraseñas
Controles adicionales	Autenticación multifactor	Vallas, trampas	Política de formación sobre sensibilización
Controles reforzados	Sistemas de prevención de pérdida de datos, Centro de Operaciones de Seguridad interno y continuo	Centro de datos de nivel 1, *hot site* activo/replicación activa	Política "Trae tu propio dispositivo", política de cifrado reforzado para información muy sensible

Recuadro 23. Ejemplos de control básico

Antivirus y *firewalls*

Los antivirus y *firewalls* son protecciones obligatorias. Si bien la mayoría de las organizaciones consideran obvia la necesidad de estos dos controles, numerosos ciberataques se aprovechan de una mala configuración y de una gestión indebida de esos equipos y software.

Mientras el antivirus protege los terminales y servidores ante amenazas conocidas, los *firewalls* permiten aislar las distintas partes de la red y disparar alertas cuando detectan tráfico inadecuado. Mantener el antivirus actualizado y configurar debidamente las reglas de *firewall* son requisitos esenciales.

Gestión de parches y actualizaciones

La aplicación de parches en aplicaciones y sistemas operativos es un aspecto crítico para proteger la infraestructura informática. Normalmente, amenazas cibernéticas tales como el pirateo informático implican el uso de un código de *exploit* publicado que aprovecha las vulnerabilidades de seguridad para las que ya existe un parche durante un período considerable. Los piratas informáticos son conscientes de que si bien los sistemas orientados al exterior se parchean de forma rutinaria, es posible que los internos, por razones comerciales, no sean parcheados tan rigurosamente.

Los parches deberían ser instalados por defecto. Pueden surgir problemas con los parches, si bien son poco habituales, y en caso de que se produzca un problema pueden revertirse hasta que el problema se haya incorporado a la siguiente versión del parche.

Se recomienda a las administraciones tributarias que elaboren y apliquen una política de gestión de parches como medida de control que garantice que los parches y las actualizaciones de todos los sistemas operativos y del *firmware* se instalen dentro de un marco temporal definido (normalmente en unos días). Debe aplicarse asimismo un proceso de instalación de parches críticos con el fin de asegurar que los parches críticos se instalen dentro de los marcos temporales definidos (normalmente en unas horas). Las administraciones tributarias también pueden definir cómo se clasifica un parche como crítico.

Fortalecimiento del sistema

La configuración de los sistemas para que estén protegidos por defecto es una protección necesaria para combatir las amenazas cibernéticas. Las administraciones tributarias deben ser capaces de impedir que los piratas informáticos ejecuten código malicioso en su entorno de TI, y es importante que tengan conocimiento de los procesos que se ejecutan en el entorno para asegurarse de que son adecuados.

Para lograrlo, las administraciones tributarias deben configurar los sistemas operativos estándar siguiendo las recomendaciones de los proveedores. En relación con el uso de aplicaciones, la instalación de una herramienta de listas blancas (*whitelisting*) puede configurarse para que restrinja únicamente la ejecución de archivos ejecutables y secuencias de comandos (*scripts*) autorizados. Además, las macros deben restringirse para que sea necesario autorizar su ejecución, o que solo se ejecuten cuando sean firmadas. Por último, es importante deshabilitar las aplicaciones que sean potencialmente peligrosas, tales como las extensiones (*add-ons*) de los exploradores web, la publicidad digital y los *applets*.

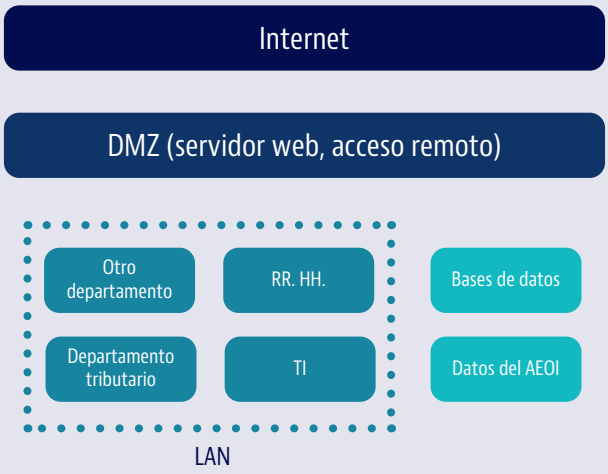
Segmentación de redes

La implementación de segmentación de redes consiste en levantar barreras entre sistemas críticos y redes internas y externas. Un "segmento plano", sin barreras o con barreras limitadas, puede crear un entorno que requiere solo una única intrusión en la red para que un pirata informático consiga un acceso generalizado. Una red plana permite al pirata informático pivotar entre anfitriones y servicios con mínimos obstáculos y escasa probabilidad de ser detectado. Una estación de trabajo comprometida no debería poder conectarse a bases de datos importantes.

Una manera habitual de diseñar redes es dividirlas en redes más pequeñas, tal como se ilustra en la figura que se muestra a continuación, por lo común con zonas exclusivas:

- Sistemas orientados al exterior, normalmente denominados, por sus siglas en inglés, DMZ (Zona desmilitarizada).
- Una zona dedicada para el administrador.
- Una zona para bases de datos sensibles y aplicaciones críticas, como bases de datos y aplicaciones de AEOI.
- Una zona para la red interna, normalmente denominada, por sus siglas en inglés, LAN (Red de Área Local).

Las redes internas pueden segmentarse a su vez en función de la actividad, p. ej. departamentos de recursos humanos, financiero, de informática, de cumplimiento tributario, etc. A continuación se muestra un ejemplo de segmentación de redes.



Gestión del acceso y los derechos del administrador

Los piratas informáticos se dirigen contra cuentas privilegiadas y de administrador para llevar a cabo actividades tales como la extracción de datos de bases de datos y la exfiltración de datos, pues dichas cuentas suelen ser capaces de sortear todas las restricciones. Por tanto, es importante restringir los derechos y accesos del administrador mediante una gestión adecuada.

Es altamente recomendable aplicar autenticación multifactor (que se analiza en más detalle en el RE 3.2.3, relativo a la gestión del acceso) a las cuentas de administrador de las administraciones tributarias, con el fin de desactivar o renombrar todas las cuentas del sistema integradas, así como adoptar una política que garantice que el acceso de los administradores esté restringido siempre que sea posible.

Asimismo, debe impedirse que las cuentas privilegiadas lean correos electrónicos y accedan a Internet de manera general, incluyendo la descarga o subida de archivos a través de servicios en línea. Además, pueden utilizarse "*jump boxes*" como paso intermedio necesario para que los administradores accedan a sistemas críticos. Un *jump box* es un servidor especializado seguro ubicado en una zona DMZ, que solo admite unos pocos protocolos de comunicación con el fin de que los administradores puedan autenticarse usando una autenticación robusta, a fin de poder acceder desde ahí a recursos específicos ubicados en la red interna.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Los controles básicos no son estáticos: controles que no eran muy comunes no hace mucho tiempo pueden considerarse hoy en día controles básicos para muchas administraciones tributarias, como sucede, por ejemplo, con las soluciones de gestión de eventos e información de seguridad (SIEM, siglas en inglés de *Security Information and Event Management*).

Controles adicionales

Una administración tributaria puede decidir aplicar controles adicionales con el fin de mitigar riesgos identificados, basándose en su evaluación de la importancia o gravedad relativa de dichos riesgos y en sus decisiones de tratamiento del riesgo.

Recuadro 24. **Ejemplo de control adicional: prueba de penetración de interfaces externas**

La prueba de penetración es un aspecto fundamental para averiguar si existen debilidades en el entorno de TI. También conocida como "hacking ético", simula las acciones de un pirata informático contra la organización. El objetivo principal consiste en encontrar vulnerabilidades aprovechables antes de que lo haga otra persona, para poder parchearlas y tratarlas como corresponde. Durante una prueba de penetración, normalmente se identificarán los riesgos y se calificarán con respecto a una matriz de riesgos, usualmente de este modo:

- Bajo
- Medio/Moderado
- Importante/Serio
- Alto/Severo/Crítico/Catastrófico

Los múltiples puntos y servicios de integración que existen en los entornos de TI modernos, hace que la falta de pruebas de penetración de las interfaces externas e internas pueda poner en peligro la seguridad de los datos, incluida la información intercambiada (p. ej. puede haber riesgos para la información intercambiada si dicha información tiene algún nivel de integración con los entornos de sistemas centrales de la administración tributaria).

Si bien las pruebas internas son muy importantes, aún lo es más probar las interfaces externas, pues los piratas informáticos de cualquier parte del mundo pueden dirigir sus ataques directamente contra ellas. Una interfaz externa es simplemente cualquier servicio que responda a entradas externas. Podría ser un modelo electrónico de liquidación del impuesto sobre el valor añadido, un portal del contribuyente o un servidor de protocolo de transferencia de archivos. La prueba de penetración se describe con mayor detalle en el RE 3.2.6.4, relativo a la gestión de las vulnerabilidades.

Los controles de TI adicionales actúan como complemento de los controles básicos, y deben incluir del mismo modo controles administrativos, técnicos y físicos que, conjuntamente, tratarán de alcanzar el objetivo final de mantener la confidencialidad. Esto se denomina como "defensa en profundidad". El Recuadro 24 ofrece un ejemplo de un control adicional frecuente.

Controles reforzados

También pueden utilizarse controles reforzados para proteger la infraestructura de TI frente a amenazas avanzadas tales como métodos sofisticados de exfiltración de datos. Las administraciones tributarias implantan controles reforzados en función de la madurez de sus procesos y controles de seguridad vigentes, así como del nivel general de riesgo en relación con posibles violaciones de los datos (en relación tanto con los datos fiscales nacionales como con la información intercambiada). Véase el Recuadro 25 para

Recuadro 25. **Ejemplo de control reforzado: Prevención de pérdida de datos (DLP)**

La previsión de pérdida de datos (DLP, por sus siglas en inglés) detecta posibles violaciones de datos, incluyendo sofisticadas transmisiones de exfiltración de datos, y las previene mediante la supervisión, la detección y el bloqueo de datos sensibles mientras están en uso (acciones de terminales o *endpoints*), en movimiento (tráfico de red) y en reposo (almacenamiento de datos). La DLP detecta datos sensibles que salen de la administración tributaria y circulan por ella cuando no deberían hacerlo, y adopta medidas con respecto a estos datos como el bloqueo, la admisión o el envío de alertas.

Una solución de DLP es una combinación de dos herramientas de DLP:

- DLP de terminales, que consiste en un software instalado en todos los ordenadores portátiles y estaciones de trabajo que analiza los datos almacenados en los equipos e impide que los usuarios ejecuten acciones prohibidas tales como la copia de un archivo en un dispositivo de almacenamiento externo.
- DLP de red, que impide la filtración de datos mientras circulan por la red de la administración tributaria, por ejemplo, cuando se envía un correo electrónico a un destinatario externo.

Con el fin de sacar el máximo provecho de una solución de DLP, es muy importante etiquetar adecuadamente todos los datos (en función de la clasificación de los datos que aplique la administración tributaria: véase el RE 3.2.5.1, relativo a la protección de la información). Los sistemas DLP requieren técnicos altamente cualificados para ser eficientes y estar correctamente configurados.

consultar un ejemplo de control reforzado.

Evaluando de la eficacia de los controles de seguridad

Las administraciones tributarias deben adoptar medidas para evaluar la eficacia de los controles de seguridad (básicos, adicionales y reforzados), pues aunque puedan haberse implementado dichos controles es posible que no funcionen adecuadamente en la práctica (p. ej. se pone en marcha un programa de sensibilización pero, tras revisarlo, la organización comprueba que solo el 5% de sus destinatarios lo ha completado efectivamente). Entre las herramientas útiles para medir la eficacia se incluyen los indicadores clave del rendimiento, las pruebas de penetración, las evaluaciones de las vulnerabilidades y las pruebas con conjuntos de datos (para obtener más información, véase el RE 3.2.6.4, relativo a la gestión de las vulnerabilidades).

RE 3.2.4.3. Gestión de activos y servicios de TI, y gestión del nivel de servicio

El RE 3.2.4.3 aborda la gestión operativa de los activos de TI de las administraciones tributarias. La gestión de activos es importante para la confidencialidad de la información, pues los activos pueden contener información, y la información relativa a los activos es necesaria para investigar las incidentes de seguridad.

Es preciso identificar y gestionar cada activo de TI, pues representa una vulnerabilidad de seguridad potencial y, por tanto, un riesgo.

La gestión de activos puede dividirse en dos funciones, cuya ejecución se lleva a cabo normalmente desde áreas separadas del departamento de TI:

- **Gestión de activos y servicios de TI**, normalmente gestionada por administradores de activos de TI especializados.
- **Gestión del nivel de servicio**, o la gestión de las relaciones que sustentan la prestación de los activos y servicios de TI a los usuarios de la administración tributaria. Suele estar asociada a los gerentes de las relaciones del negocio.

Tabla 17. **Ciclo de vida de la gestión de activos**

Componente de la gestión de activos	Descripción del componente	Ejemplos de elementos que deben incluirse	Ejemplos de información que debe registrarse
Inventario de activos	Lista que incluye cada uno de los activos de TI que posee la administración tributaria, con su descripción y un identificador exclusivo	Terminales, discos duros, ordenadores portátiles, pantallas, dispositivos móviles, *routers*, *firewalls*, auriculares, licencias de software	Identificación – descripción - número de serie - clasificación - estado "en uso" o "disponible para uso"
Propiedad del activo	Descripción del propietario del activo	Entidad, persona, servicio, tercero	Propietario - función – última revisión
Gestión de la configuración del activo	Garantiza que los sistemas se configuren adecuadamente y estén listos para ser usados	Garantía, gestión de la licencia de software, gestión de parches, distribución, revisión de código	Versión de firmware – última actualización – propietarios anteriores - estado de "configuración en curso" – estado de parches, estado de garantía, estado de mantenimiento
Gestión de la capacidad de activos	Proporciona un plan para gestionar la capacidad de TI, con el fin de asegurarse de que las TI disponen de los recursos necesarios y pueden crecer	Capacidad del centro de datos, equipos disponibles para los nuevos empleados, capacidad de grabación de la copia de seguridad, disponibilidad de la información	Capacidad del hardware (%) – última actualización del hardware - capacidad de almacenamiento restante - consumo eléctrico - capacidad de carga del servidor - ancho de banda
Eliminación de los activos	Cómo gestiona la administración tributaria la eliminación de sus activos	Renovación de ordenadores portátiles, impresoras, destrucción de equipos, política de saneamiento	Actualización de estado a "no está en uso", "sanear", "vendido"

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Gestión de activos y servicios de TI

La Tabla 17 describe los componentes de la gestión de activos que debería seguir una administración tributaria. Los componentes pueden denominarse fases del ciclo de vida de la gestión de activos.

Lo ideal es que todos los activos se gestionen con un criterio similar, con independencia del número de activos poseídos, a fin de asegurar criterios mensurables correctos, datos coherentes y una supervisión y auditoría más sencillos. La gestión de activos suele respaldarse con herramientas de TI (véase el Recuadro 26).

No obstante, algunas variables pueden influir en el modo en que las administraciones tributarias gestionan activos:

- **Los activos pueden gestionarse con diferentes grados de detalle**. Un ordenador de escritorio, por ejemplo, puede registrarse como un único activo o puede desglosarse hasta el nivel de sus componentes. Si bien cualquiera de estos enfoques es válido, el enfoque debe ser lo suficientemente detallado como para permitir la identificación de los atributos relevantes del activo. Por ejemplo, no basta con registrar únicamente el número de ordenadores de escritorio que hay en una oficina, sin información alguna sobre los atributos de dichos ordenadores (p. ej. número de serie, modelo, marca, información técnica).

- **La gestión de los activos informáticos puede externalizarse**. Si una administración tributaria externaliza la gestión de sus activos de TI, debe evaluar y asegurarse de que el proveedor realiza el trabajo de manera correcta y eficaz. Si bien la externalización libera a la administración tributaria de una carga, la supervisión del proveedor puede requerir un esfuerzo mayor.

Algunos procesos de la administración tributaria pueden estar basados en la información relativa a los activos, y las administraciones tributarias deben ser capaces de respaldar estos procesos y realizar modificaciones en los servicios sin poner en peligro la confidencialidad. Por ejemplo, si los cambios en el software afectan a activos tales como navegadores, es posible que la administración tributaria necesite comprobar si cada uno de los distintos tipos y versiones de navegador que usa la administración han sido verificados a la luz de esos cambios. Las administraciones tributarias deben ser capaces de identificar cuáles son las versiones del software que se están usando, en qué dispositivos se usan y que todas las versiones que se están ejecutando siguen estando cubiertas por las actualizaciones de seguridad.

Gestión del nivel de servicio

La gestión del nivel de servicio se refiere a las relaciones globales entre las divisiones del negocio tributario que requieren servicios de TI y las entidades con la responsabilidad general de prestar dichos servicios de TI (a saber, el departamento de TI de la administración tributaria o un proveedor externo).

Esas relaciones se reflejan principalmente en un Acuerdo de Nivel de Servicio (SLA, por sus siglas en inglés). Los SLA condensan un acuerdo entre esas partes únicamente en lo que se refiere a los requisitos no funcionales de un servicio de TI. Los requisitos funcionales están relacionados con los objetivos de las divisiones del negocio (es decir, qué debe hacer una aplicación o servicio de TI), mientras que los requisitos no funcionales se basan en los servicios (es decir, la mínima disponibilidad del servicio aceptable).

Los SLA forman parte de los contratos con los proveedores, tanto si el proveedor es el propio departamento de TI (o una subfunción del mismo), o si el servicio de TI es externalizado por el departamento de TI.

Además de los SLA, la gestión del nivel de servicio comprende:

- **Acuerdos de nivel operativo**, celebrados entre entidades internas en una administración tributaria cuando el servicio de TI depende de otro departamento para poder funcionar de forma plena.

Recuadro 26. **Herramientas de TI para la gestión de activos**

Lo ideal sería que la gestión de activos se llevase a cabo usando herramientas tales como una Base de Datos de Gestión de Configuraciones (CMDB, por sus siglas en inglés), que registran todos los activos informáticos, incluidos los ordenadores de escritorio, portátiles, periféricos, software *off-the-shelf*, etc., y que se mantuviese actualizada de manera automatizada. Esta herramienta contendrá toda la información pertinente del ciclo de vida de cada activo (p. ej. la fecha de compra, versión, ubicación y propietario actuales, fecha de fin de su vida útil, etc.). Esta información es muy útil en un contexto de seguridad porque si se produce un incidente de seguridad, una CMDB actualizada permitirá que se investigue dicho incidente para llegar a la raíz del problema con mayor rapidez. Esta herramienta mitiga asimismo los riesgos asociados a la gestión del gestión y permite al departamento de TI ofrecer un mejor servicio a los usuarios.

- **Contratos marco**, que son los mismos que los acuerdos de nivel operativo, pero en los que un proveedor de TI depende también de los servicios prestados por un subcontratista.

Acuerdos de Nivel de Servicio

Los SLA en las administraciones tributarias garantizan que los servicios de TI cubran las necesidades de todas las partes interesadas dentro de la administración, incluidos los directores y otros cargos directivos responsables de los procesos tributarios que se apoyan en servicios de TI, los empleados que usan los sistemas y el OSI.

Los requisitos no funcionales de los SLA contienen por lo general:

- **Un grupo básico de requisitos de seguridad** tales como la gestión del acceso (interno o externo) del proveedor a los sistemas de la administración tributaria.
- **Requisitos adicionales específicos** que puedan haberse identificado con respecto a un sistema en particular, que complementan a los requisitos básicos. Pueden incluir la especificación de la manera en que el proveedor debe manejar determinados tipos de datos como, por ejemplo, información intercambiada o datos financieros.

Algunos requisitos no funcionales se incorporarán en el diseño de los servicios de TI y el entorno de la infraestructura (p. ej. *firewalls*, fortalecimiento del servidor o antivirus), mientras que otros no se incorporarán y tendrán que ser monitoreados por el departamento de TI (p. ej. acceso a datos). En ambos casos, los requisitos de seguridad deben gestionarse de manera eficaz con el fin lograr buenos resultados en materia de seguridad. Ambos tienen que estar regulados en los SLA.

Los requisitos no funcionales de los SLA que no estén relacionados directamente con la seguridad deben incluir:

- Una descripción del servicio, incluidos los resultados y productos clave.
- La disponibilidad del servicio y otros objetivos de desempeño.
- Las medidas de mantenimiento.
- La regulación de los tiempos de inactividad planificados, incluidos los períodos en que debe evitarse dicha inactividad.
- Los tiempos de recuperación.
- Las normas que regulen los cambios del sistema.
- Los mecanismos para el reporte de incidentes.
- Los puntos de contacto.

Los principales puntos que deben tenerse en cuenta a la hora de implementar un SLA son:

- Los arreglos generales, en particular si existe un solo grupo de requisitos estándar en lugar de requisitos complementarios específicos para cada sistema.
- La naturaleza de los arreglos, esto es, si será un SLA directo entre las áreas del negocio tributario y el departamento de TI interno o algo más complejo que implique a proveedores externos.
- Los mecanismos de reporte, tanto por escrito como a través de reuniones periódicas entre los interesados (ambos se recogerán en el SLA).
- Si existe un grupo estándar de requisitos en materia de seguridad, p. ej. dos o más grupos estándar para distintos tipos de procesos, o disposiciones diferentes para cada uno de los sistemas.
- Si los sistemas que gestionan información intercambiada, p. ej. bajo el estándar AEOI, tienen su propio SLA específico. En caso negativo, si existe un proceso dentro del ámbito de un SLA global que permita al equipo de EOI competente validar que todos los controles de seguridad pertinentes están instalados y funcionan, en colaboración con el proveedor pertinente (interno o externo) de los servicios de TI.
- Las medidas que deben adoptarse en circunstancias excepcionales, en especial el reporte de incidentes. En particular, cuando el departamento de TI identifica una incidente de seguridad, este debe ser reportado de la manera prescrita.
- La designación de puntos de contacto tanto dentro del departamento de TI como en toda la administración tributaria.

El Recuadro 27 muestra un modelo básico de SLA.

Un aspecto importante a considerar es el uso de un solo SLA o de varios. Algunas administraciones pueden adoptar la decisión central de que todas las aplicaciones informáticas se construyan, posiblemente en una única plataforma de infraestructura con un solo SLA, mientras

que otras pueden acordar SLA separados para cada una de las diferentes aplicaciones de gestión tributaria.

En la práctica, las administraciones tributarias usan una combinación de ambas. Normalmente, llegará un momento en que una administración tributaria disponga de varias plataformas distintas heredadas. La gestión de TI puede ser compleja en estas circunstancias, por lo que las administraciones tributarias pueden considerar la estandarización de los servicios de TI en una sola plataforma moderna. Podrán integrarse nuevas aplicaciones en la plataforma, y las aplicaciones heredadas se migrarán siempre y cuando lo permitan las circunstancias. Cada pocos años surge un nuevo paradigma de TI, y ha de comenzarse de nuevo todo el proceso.

Será preciso tener en cuenta muchos factores diferentes a fin de decidir cuál es la estructura de SLA más adecuada para una organización.

En cualquier caso, los SLA multinivel son los más utilizados y sus componentes de nivel incluyen:

Nivel de organización

Este nivel aborda todas las cuestiones generales relevantes para la organización y que son comunes a toda la organización. Por ejemplo, bajo las condiciones en materia de seguridad de un SLA a nivel de organización, se puede requerir a cada empleado que cree una contraseña de 8 caracteres que debe cambiar cada treinta días o que disponga de una tarjeta de acceso con su fotografía.

Nivel de cliente

Este nivel aborda cuestiones específicas de un usuario o "cliente" del servicio de TI. Por ejemplo, los requisitos de seguridad de uno o más departamentos dentro de la organización pueden ser más estrictos que los de otros departamentos, p. ej. una división financiera o una división de EOI que requiera medidas de seguridad reforzadas debido a su función de tratamiento de información y recursos particularmente sensibles.

Nivel de servicio

Este nivel aborda las cuestiones correspondientes a un servicio específico (en relación con el usuario o cliente). Se aplica a todos los usuarios o clientes que se benefician del mismo servicio (por ejemplo, la contratación de servicios de TI para cualquiera que use un proveedor de telefonía IP concreto).

El uso de esta estructura de SLA multinivel por una organización grande puede reducir la duplicación de esfuerzos al mismo tiempo que ofrece adaptación para los distintos usuarios y servicios dentro de la organización.

La Tabla 18 ofrece un ejemplo de medidas de asistencia al usuario o cliente que un proveedor de servicios puede garantizar bajo un SLA, dependiendo de la gravedad o urgencia de un problema. Como se muestra, cuanto mayor es la gravedad o urgencia, menor es el tiempo de respuesta. En este ejemplo, se ofrece una garantía con respecto al 90% de los incidentes o problemas reportados, lo que implica que, una vez finalizado el período de servicio acordado relevante, se realizará un cálculo de los problemas a los que se dio respuesta. Si la puntuación es inferior al 90% de resolución a tiempo, podrían imponerse al proveedor sanciones económicas u otras medidas de compensación. Por lo tanto, tanto el proveedor de servicios como el destinatario deben revisar y comparar las cifras.

Recuadro 27. **Modelo básico de lo que se espera en un documento SLA**

Un SLA se compone normalmente de:

- Una introducción, que describe la finalidad del acuerdo.
- Una descripción del servicio, que indica a qué servicios se aplica el SLA y los detalles de dichos servicios.
- Las responsabilidades recíprocas, esto es, quién es responsable de qué parte de los servicios.
- Una descripción del ámbito de aplicación del SLA.
- Las horas de servicio aplicables, esto es, desde qué hora y hasta qué hora están disponibles los servicios según el acuerdo.
- Disponibilidad del servicio, es decir, en qué medida están disponibles los servicios durante el horario de servicio y fuera de él.
- Fiabilidad del servicio.
- Mecanismos de asistencia al cliente.
- Puntos de contacto y escalamiento de incidencias, incluida una matriz de comunicación.
- Indicadores de desempeño del servicio
- Requisitos de seguridad.
- Costes y método de cobro empleado.

Tabla 18. **Ejemplo de medidas de asistencia al usuario o cliente bajo un SLA**

Prioridad/ Descripción	Baja	Normal	Alta	Crítica
Gravedad del incidente	No obstaculiza la labor de la administración tributaria.	Interrupción de la labor de la administración tributaria; solución alternativa probablemente disponible.	Interrupción de procesos críticos que afectan a usuarios individuales; no existe una solución alternativa.	Interrupción de procesos críticos de la administración tributaria que afectan a varios usuarios; no existe una solución alternativa.
Urgencia de la remediación	La administración tributaria no necesita una remediación inmediata.	La administración tributaria no necesita una remediación inmediata.	La administración tributaria necesita una remediación inmediata.	La administración tributaria necesita una remediación inmediata.
Objetivos del SLA				
Tiempo de respuesta inicial del 90%	Dentro de 2 días	Dentro del mismo día hábil	Dentro de 4 horas	Dentro de 2 horas
Tiempo de resolución del 90%	Dentro de 2 semanas	Dentro de 1 semana	2-3 días laborables	24 horas (*hotfix* inmediato)

RE 3.2.4.4. Gestión de la prestación del servicio por el proveedor

El RE 3.2.4.4 aborda cómo se garantiza la seguridad en el uso de la subcontratación y cadenas de suministro mediante una gestión cuidadosa de las relaciones de una administración tributaria con sus proveedores. Se trata de un requisito muy importante, ya que se han producido varias infracciones de alto nivel en materia de seguridad atribuidas a deficiencias en la red de proveedores.

Muchas administraciones tributarias tratan de garantizar que todos los datos del contribuyente permanezcan en sus instalaciones en todo momento, operados y controlados por ellos y/o por otros organismos gubernamentales con una estricta supervisión de cualquier acceso por parte de terceros. No obstante, las administraciones tributarias permiten cada vez más a terceros proveedores de TI un acceso remoto a sus centros de datos con el fin de que presten asistencia remota en tareas de desarrollo, mantenimiento y actualización. En esos casos, deben establecerse de forma clara los tipos de acceso permitidos y aplicarse controles adecuados. En la Figura 13 se sintetiza un proceso de gestión de proveedores.

Los acuerdos contractuales de una administración tributaria con proveedores deben incluir requisitos específicos para abordar los riesgos de seguridad de la información asociados a los servicios de TI y la cadena de suministros de productos. A modo de ejemplo, en relación con un sistema de correo electrónico basado en la nube o una aplicación de recursos humanos de un proveedor, el acuerdo debe garantizar (véase el Recuadro 28) que el proveedor cumpla también todos los requisitos y salvaguardas de seguridad aplicables, especialmente cuando esté procesando datos e información.

A la luz de la necesidad de abordar los riesgos para la seguridad de la información en el contexto de la contratación de proveedores, las administraciones tributarias deben definir de modo general una política sobre seguridad de la información para proteger los activos y datos a los que puedan acceder dichos

FIGURA 13. **Proceso de gestión de proveedores**

proveedores. Esta política debe ser acordada con los proveedores y estar documentada. De manera implícita, deben identificarse los riesgos específicos y aplicarse controles de seguridad, tal como se describe en el RE 3.2.4.2, relativo a la implementación de una serie adecuada de controles de seguridad. Algunos controles podrán ser implementados por la propia administración tributaria, mientras que otros se encargan a los proveedores. Dichos controles podrían incluir:

Recuadro 28. **Seguridad en los acuerdos con proveedores**

Es altamente recomendable que las administraciones tributarias acuerden de manera formal requisitos de seguridad con cada proveedor que pueda acceder, procesar, conservar, comunicar o proveer componentes o servicios de TI y/o acceder a sus datos. Los acuerdos con proveedores suelen documentar los siguientes elementos:

- Una descripción de la información proporcionada o a la que ha accedido el proveedor, así como los métodos de suministro o acceso a la información.
- La clasificación de la información.
- Los requisitos legales y regulatorios en materia de confidencialidad y seguridad.
- Las obligaciones de cada parte de implementar los controles de seguridad pertinentes y, cuando proceda, de cumplir con un estándar reconocido a nivel internacional en materia de seguridad de la información.
- Normas sobre usos de la información aceptables e inaceptables.
- Si procede, una lista del personal del proveedor autorizado para acceder a la información de la administración tributaria o para recibirla (o las condiciones y procedimientos para obtener dicha autorización).
- Las políticas sobre seguridad de la información de la administración tributaria aplicables al acuerdo.
- Los mecanismos para abordar situaciones en las que el proveedor no sea capaz de suministrar su producto o servicio, a fin de evitar problemas o retrasos en la actividad de la administración tributaria.
- Procesos de resolución de conflictos.

Debe tenerse en cuenta que los acuerdos podrían involucrar a otras partes tales, como los subcontratistas. Asimismo, los acuerdos pueden diferir mucho entre distintos tipos de proveedores.

- La identificación, clasificación y documentación de todos los proveedores, y la definición del tipo de información a la que pueden acceder.
- Formación para la sensibilización en materia de confidencialidad destinada a miembros del personal de la administración tributaria con respecto a la información que traten de forma conjunta con los proveedores y a cómo deben interactuar con estos últimos.
- SLAs.
- Acuerdos de no divulgación.
- Procedimientos y procesos de gestión de incidentes.

Monitoreo y revisión de los servicios del proveedor

Las administraciones tributarias deben monitorear, revisar o garantizar de otro modo, de manera periódica, que la prestación del servicio del proveedor esté sujeta a auditorías con el fin de asegurarse de que se cumplen los términos y condiciones en materia de confidencialidad y seguridad de la información, y de que los incidentes y problemas se gestionan de manera adecuada.

También podría ser conveniente tener un proceso de gestión de las relaciones de servicio que:

- Supervise los niveles de rendimiento del servicio.
- Solicite y revise los informes de servicio que deben elaborar los proveedores.
- Establezca la realización de auditorías del proveedor (por la propia administración tributaria o un auditor independiente).
- Revise los registros de auditoría y los registros de eventos relacionados con la seguridad de la información, problemas operativos, fallos, el seguimiento de fallos e interrupciones relacionadas con el servicio prestado.

Recuadro 29. **Proveedores de servicios no informáticos**

Frecuentemente, las violaciones de datos no están relacionadas con proveedores de TI, sino con proveedores de otros servicios. Infracciones han surgido, por ejemplo, cuando contratistas de servicios de limpieza tienen acceso a sistemas de recursos humanos de clientes (a fin de actualizar la información del personal de limpieza de servicio y que necesita acceder al edificio) y piratas informáticos fueron capaces de explotar las debilidades en los sistemas informáticos del proveedor para conseguir acceder de forma remota a los sistemas de la organización. Por lo tanto, también es importante adoptar controles de seguridad sobre los proveedores de servicios no informáticos cuando estos proveedores tengan acceso a la infraestructura, ya sea remoto o de otro tipo.

- Garantice que el proveedor mantiene una capacidad de servicio suficiente y los niveles de continuidad del servicio acordados.

Se alienta a las administraciones tributarias a mantener un control global y una visibilidad suficientes sobre todos los aspectos de seguridad de información sensible o crítica o de las instalaciones de procesamiento de información a las que accede, procesa o gestiona un proveedor. Para lograrlo podrían adoptarse procesos de reporte para las áreas particulares de gestión del cambio, gestión de las vulnerabilidades y notificación y respuesta a incidentes de seguridad.

La responsabilidad última de la gestión de las relaciones con proveedores debe asignarse a una persona especializada o a un equipo de gestión de servicios, que debe adoptar medidas adecuadas cuando se observen deficiencias en la prestación del servicio.

RE 3.2.4.5. Garantía de continuidad de los servicios de TI mediante Acuerdos de Nivel de Servicio

Como explicado en el RE 3.2.1, la seguridad de la información no se refiere únicamente a la prevención del acceso no autorizado a información, sino también a asegurar de que los usuarios legítimos que necesitan acceso puedan hacerlo cuando lo necesiten ("disponibilidad" en la tricotomía "confidencialidad, integridad y disponibilidad"). Si el personal no puede confiar en que los servicios formales de acceso a información funcionen adecuadamente cuando necesitan acceder a la información para desempeñar sus tareas, es posible que traten de crear sus propias rutas informales de acceso como, por ejemplo, descargando partes de una base de datos en sus propios almacenes de archivos privados.

La falta de disponibilidad suficiente conduce, por tanto, a prácticas inseguras y rutas de acceso informales, que a su vez plantean riesgos de seguridad no controlados. Por lo tanto, es importante asegurarse de que la continuidad de los servicios del negocio, incluidos los servicios de TI, sea lo más efectiva en la medida de lo posible.

Esta sección se refiere a asegurar la buena práctica de Continuidad de los Servicios de Tecnologías de la Información (CSTI), con especial atención a tres aspectos fundamentales:

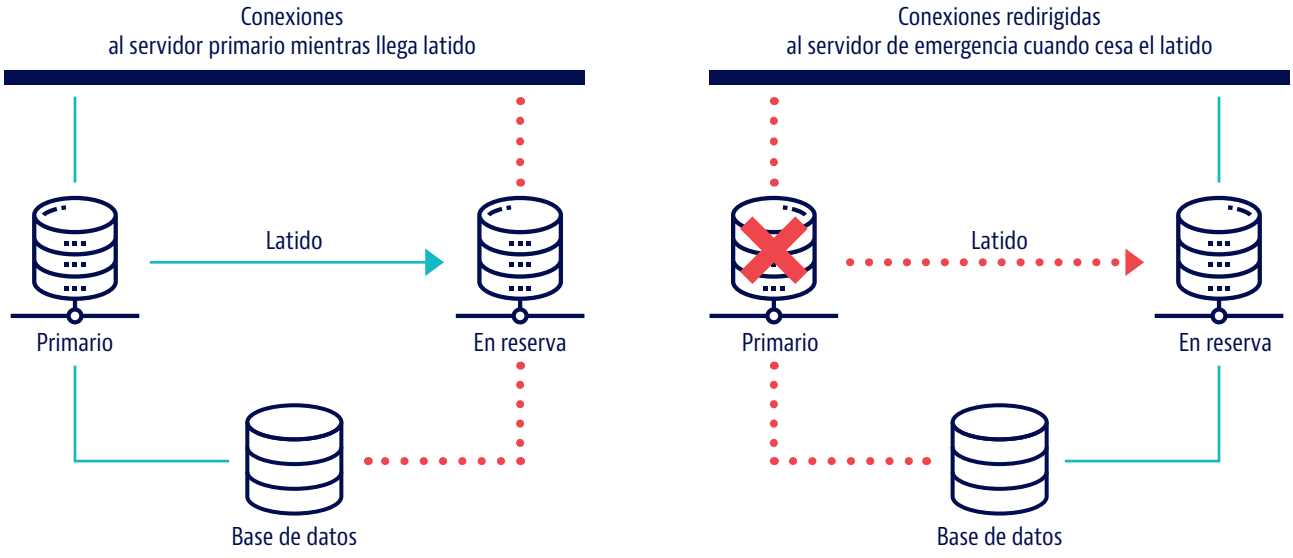
- Recuperación y resiliencia.
- Copia de seguridad de datos.
- Planificación, implementación y verificación de la continuidad de la seguridad de la información.

Recuperación y resiliencia

La resiliencia consiste en la mitigación del riesgo de interrupción del servicio, mientras que la recuperación consiste en restaurar un servicio que ha sido interrumpido.

Cualquier enfoque de CSTI incluirá elementos de las dos. Asimismo, muchos controles de seguridad individuales incluirán los dos elementos de recuperación y resiliencia (véase la Figura 14 para un ejemplo de implementación de recuperación y resiliencia a través de un acuerdo de tolerancia a fallos).

FIGURA 14. **Ejemplo de acuerdo de tolerancia a fallos**



Nota: En este caso existe un servidor principal (activo) y otro secundario (pasivo) (por lo que no existe equilibrio de carga). El servidor activo emite un "latido" regular al servidor de reserva, y si no se recibe latido se activa la tolerancia a fallos.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

La resiliencia tiene la ventaja de que es más eficaz para reducir las situaciones de interrupción del servicio. En base a las buenas prácticas internacionalmente reconocidas, las medidas que una administración tributaria puede adoptar para mejorar la resiliencia y, por tanto, la disponibilidad del servicio, incluyen:

- Garantizar la resiliencia a nivel de componentes y servicios. Cuando los servicios se desarrollen o se modifiquen, es importante asegurarse de que los elementos del servicio y los componentes que respaldan a los elementos del servicio se seleccionen, diseñen, desarrollen y mantengan de manera tal que se vea aumentada la resiliencia y se reduzca el riesgo de interrupción del servicio.

- Garantizar varias instancias del mismo servicio. Disponer de dos instancias paralelas del mismo servicio supone que, en caso de que falle un componente en una de las instancias, el procesamiento se traslade a la instancia que sigue operativa.

- Garantizar una fuente de energía de reserva. A nivel del centro de datos, existen puntos únicos de fallo tales como el suministro de agua, el aire acondicionado y la electricidad. Cuando sea posible, debe existir una fuente de energía de reserva, ya sea extraída de una red independiente o de algún tipo de sistema de alimentación ininterrumpida (UPS, por sus siglas en inglés) de respaldo. La garantía de disponibilidad en los centros de datos se denomina "Nivel de disponibilidad" (*Tier Level*, por sus siglas en inglés). Existen 4 niveles de disponibilidad y la elección debe hacerse en función del tiempo de indisponibilidad que una administración tributaria está dispuesta a aceptar. Esta clasificación es proporcionada por The Uptime Institute, fundado en 1993.

  - Un centro de datos de **Tier 1** dispone de una única vía de alimentación y refrigeración y pocos componentes redundantes y de reserva, de haber alguno. Tiene un tiempo de actividad previsto del 99,671% (28,8 horas de inactividad al año).

  - Un centro de datos de **Tier 2** dispone de una única vía de alimentación y refrigeración y algunos componentes redundantes y de reserva. Tiene un tiempo de actividad previsto del 99,741% (22 horas de inactividad al año).

  - Un centro de datos de **Tier 3** dispone de varias vías de alimentación y refrigeración y de sistemas de actualización y mantenimiento sin desconexión. Tiene un tiempo de actividad previsto del 99,982% (1,6 horas de inactividad al año).

  - Un centro de datos de **Tier 4** se desarrolla con una plena tolerancia a fallos y todos sus componentes son redundantes. Tiene un tiempo de actividad previsto del 99,995% (26,3 minutos de inactividad al año).

- Garantizar servicios operativos desde varios centros de datos. Las jurisdicciones más pequeñas y medianas deberían considerar la posibilidad de disponer de algún tipo de instalación alternativa en la que se lleve a cabo por lo menos una parte del procesamiento diario, aun cuando no cuente con las mismas dimensiones que el centro de datos principal. En todo caso, las administraciones más grandes ejercerán su actividad desde múltiples centros de datos, y es deseable diseñar los centros de modo tal que el procesamiento pueda trasladarse de un centro a otro sin problemas. Una opción aquí sería un centro de datos de respaldo que no se utilice de forma activa, pero que pueda utilizarse en caso de emergencia. La ventaja de este tipo de arreglo es que el centro de datos de respaldo puede compartirse con otras organizaciones para que el coste sea más manejable. La desventaja de estos arreglos es que solo funcionan mientras no sean varias las organizaciones que necesiten el centro de datos de respaldo al mismo tiempo, algo que podría ocurrir, por ejemplo, en caso de catástrofe natural.

- Usar un sitio dedicado para reiniciar las operaciones del negocio en caso de fallo crítico. Una administración tributaria, en función de sus costes y necesidades, podría escoger una solución de sitio frío, templado, caliente o móvil:

  - Un **sitio frío** proporciona instalaciones, aire acondicionado, energía, estantes y cableado.

  - Un **sitio templado** proporciona el mismo equipamiento que el sitio frío más hardware y software dedicados similares a la infraestructura de una administración tributaria, pero no datos.

  - Un **sitio caliente** es una reproducción en tiempo real del centro de datos de la administración tributaria, que contiene exactamente los mismos equipos y datos.

  - Un **sitio móvil** es similar a un sitio caliente pero en estantes móviles de tipo militar, de modo que son fácilmente transportables.

Una administración tributaria también puede optar por reproducir únicamente una parte de sus servicios de negocio, o solo aquellos que sean más críticos o que contengan los datos más sensibles (p. ej. datos del contribuyente o datos intercambiados).

Copia de seguridad de los datos

Los datos de una administración tributaria deben guardarse en una copia de seguridad. En jurisdicciones con varios centros de datos conectados por fibra oscura esto puede hacerse automáticamente, con la disponibilidad de una copia de seguridad completa en cada centro. No obstante, por lo general en la mayoría de los casos se usará algún tipo de copia de seguridad fuera de línea utilizando cintas y/o discos. Es importante tener en cuenta varios aspectos:

- Cómo se procesa la copia de seguridad.
- Quién es responsable de la operación.
- Cómo se conservan las copias fuera de línea.
- Qué controles existen para garantizar que no se usen indebidamente los datos descargados.
- El proceso de comprobación de que una copia descargada puede restaurarse de manera fiable y precisa.
- Cada cuánto tiempo se realizan estas comprobaciones.

En relación con los datos del AEOI, debería existir una comprensión clara sobre cómo se gestionan los datos en estos procesos y cómo se garantiza su protección.

Por último, como las cuestiones clave son la disponibilidad y la confidencialidad, se recomienda que los datos muy sensibles almacenados (en reposo), ya se trate de los datos originales o de una copia de seguridad, se cifren con un mecanismo de cifrado reconocido a nivel internacional (véase el RE 3.2.5, relativo a la protección de la información).

Planificación, implementación y verificación de la continuidad de la seguridad de la información

Un punto importante de la CSTI, como suele ocurrir en la seguridad de TI, es la planificación. Todos los aspectos tratados anteriormente deben abordarse por lo general en los PCO[16] o en los Planes de Recuperación ante Desastres (PRD), o en ambos. Dicho de otro modo, la CSTI debe planificarse antes y después de que se produzca un incidente, a fin de hacer posible una gestión continua de la seguridad.

En ausencia de planificación de la continuidad de la actividad o la recuperación ante desastres, las administraciones tributarias deben asumir que en condiciones adversas los requisitos de seguridad de la información siguen siendo los mismos que en condiciones operativas normales. De manera alternativa, las administraciones tributarias pueden llevar a cabo un Análisis de Impacto en el Negocio (AIN) sobre aspectos de la seguridad de la información a fin de determinar los requisitos de seguridad de la información aplicables a situaciones adversas.

Para jurisdicciones más pequeñas, se recomienda llevar realizar los esfuerzos de planificación durante los AIN iniciales de continuidad de la actividad y/o recuperación ante desastres.

Durante la aplicación de los PCO/PRD, se recomienda a las administraciones tributarias que instauren, documenten y mantengan controles con el fin de garantizar los niveles requeridos de continuidad de los servicios y la seguridad de TI. Aspectos importantes que deben tenerse en cuenta incluyen:

- Tener una estructura de gestión adecuada para preparar, mitigar y responder a un evento disruptivo. Un ejemplo típico es la definición de un órgano de gestión de crisis que reúna a las funciones y personas pertinentes.
- Instaurar controles compensatorios con respecto a los controles de seguridad de la información que no pueden mantenerse durante una situación adversa. Por ejemplo, en caso de fallo de energía, el personal de seguridad podría encargarse del control manual del acceso físico mientras no funcionen los torniquetes.
- Documentar los planes y los procedimientos de respuesta y recuperación aprobados por la dirección.

Una vez implementados, estos controles deben ser verificados, revisados y evaluados de manera periódica con el fin de asegurar de que sean válidos y eficaces. Para cumplir este objetivo, las administraciones tributarias podrán:

- Ejercitar y comprobar el conocimiento del personal así como las rutinas para operar los procedimientos, procesos y controles de continuidad de TI, con el fin de asegurar que su desempeño sea consistente con los objetivos definidos.
- Revisar la validez y eficacia de las medidas de continuidad en caso de modificación de los sistemas, procesos, procedimientos y controles, o de las soluciones de continuidad de la actividad/recuperación ante desastres.

Si no se llevan a cabo dichas comprobaciones podría producirse un fallo operativo total de los sistemas. Un ejemplo de ello es la falta de comprobación y restauración de las copias de seguridad de los datos, que puede derivar en una pérdida total de los datos. Este no es un resultado aceptable, en particular si se trata de datos del AEOI.

16. La gestión de la continuidad de las operaciones se aborda en detalle en el RE 3.2.1.5.

REQUISITO ESPECÍFICO 3.2.5: PROTECCIÓN DE LA INFORMACIÓN

La "Protección de la información" consiste en proteger los distintos tipos de información en papel y digital que manejan las administraciones tributarias, ya se encuentren en reposo, en uso o en movimiento entre entornos y lugares de trabajo, con controles acordes a su clasificación con respecto a su sensibilidad y confidencialidad.

El RE 3.2.5.1 requiere que las administraciones tributarias gestionen la información eficazmente de conformidad con una serie de políticas y procedimientos a lo largo de todo el ciclo de vida de gestión de la información (incluida la denominación, clasificación, manejo, almacenamiento, seguimiento, auditoría y destrucción de documentos; así como los dispositivos y medios en los que se conserva la información).

En particular, los controles a lo largo de todo el ciclo de vida de la información incluyen controles del entorno de trabajo tales como:

- Políticas de escritorio limpio/despejado.
- Controles de impresora.
- Mecanismos de almacenamiento físico y digital de la información.
- Controles de cifrado y dominio.
- Controles de medios seguros para soportes de información tales como dispositivos periféricos.
- Controles al finalizar el ciclo de vida, tales como políticas de eliminación de información.

La protección de la información *intercambiada* es la preocupación específica del proceso de evaluación del Foro Global. Por lo tanto, se espera que las administraciones tributarias se aseguren de que los controles generales posibiliten dicha protección, y que controles reforzados sean utilizados con el fin de proteger la información intercambiada en particular. Estos últimos controles se abordan en el RE 3.2.5.2, que requiere que las administraciones tributarias tengan procesos con respecto a la información recibida de otras autoridades competentes a fin de garantizar el cumplimiento de las obligaciones previstas en los acuerdos internacionales sobre intercambio de información, incluidas las destinadas a impedir su mezcla con otra información.

Es importante distinguir el RE 3.2.5 de otros REs, como los que requieren controles de acceso lógico a datos (REs 3.2.3.3, 3.2.3.4), de seguridad de los sistemas de TI (RE 3.2.4) y de gestión de la seguridad operativa (RE 3.2.6). Esos REs describen los controles que se aplican *con carácter general* para proteger la información, mientras que los controles del ciclo de vida previstos en el RE 3.2.5 se refieren a los controles de seguridad que deben aplicarse *a los propios datos* como consecuencia de las políticas de clasificación de la confidencialidad.

Tabla 19. **Glosario de principales conceptos**

Concepto	Descripción
Política de uso aceptable	Conjunto de normas que establecen las prácticas permitidas y prohibidas en relación con los sistemas de información que contienen información confidencial.
Clasificación de información	Proceso dirigido a identificar los tipos de información en poder de las administraciones tributarias y determinar el nivel de protección que deben recibir.
Política de escritorio limpio/despejado	Una política de escritorio limpio/despejado (CDP, siglas en inglés de clean/clear desk policy) especifica cómo deben dejar su espacio de trabajo los empleados cuando abandonan sus escritorios o salen de la oficina, a fin de garantizar la confidencialidad de la información.
Autoridad competente	La(s) autoridad(es) competente(s) es(son) la(s) persona(s) o autoridad(es) gubernamental(es) designada(s) por una jurisdicción como competente(s) para intercambiar información con arreglo a cualquier acuerdo internacional de intercambio de información.
Cifrado	El cifrado es un mecanismo de protección aplicado a datos para que sean accesibles únicamente cuando se facilite la clave de descifrado adecuada.
Saneamiento de medios	El saneamiento es el proceso por el cual se tratan datos conservados en medios de almacenamiento con el fin de reducir la probabilidad de recuperación y restauración hasta un nivel aceptable.
Período de conservación	Requisito legal para conservar información durante un período determinado aun cuando la información deje de ser necesaria para cumplir los fines de la actividad tributaria.

Esta sección se divide en tres partes:

- Una breve descripción de las tres fases del ciclo de vida de la información en las administraciones tributarias.
- Una descripción de los controles de seguridad generales que deben aplicarse en cada una de esas tres fases (RE 3.2.5.1).
- Una descripción de los controles del ciclo de vida de la información aplicables a la información intercambiada (RE 3.2.5.2).

La Tabla 19 contiene las definiciones de los principales conceptos cubiertos en el RE 3.2.5.

Ciclo de vida de la información

Tal como se ilustra en la Figura 15, los controles de la información, ya sea digital o en papel, deben aplicarse en las tres fases generales del ciclo de vida de gestión de la información. Deben aplicarse controles reforzados sobre la información intercambiada a lo largo del ciclo vital.

Las fases del ciclo de vida y los controles se presentan basándose en la práctica habitual de las administraciones tributarias. No obstante, se alienta a las administraciones tributarias a que adopten el enfoque del ciclo de vida que mejor les convenga.

Antes de detallar cuáles son los controles para la protección de la información en cada fase del ciclo de vida, es importante destacar la importancia de los procesos de gobierno y del negocio para la protección de la información, tal como se ilustra en el Recuadro 30.

RE 3.2.5.1. Controles generales sobre el ciclo de vida de la información

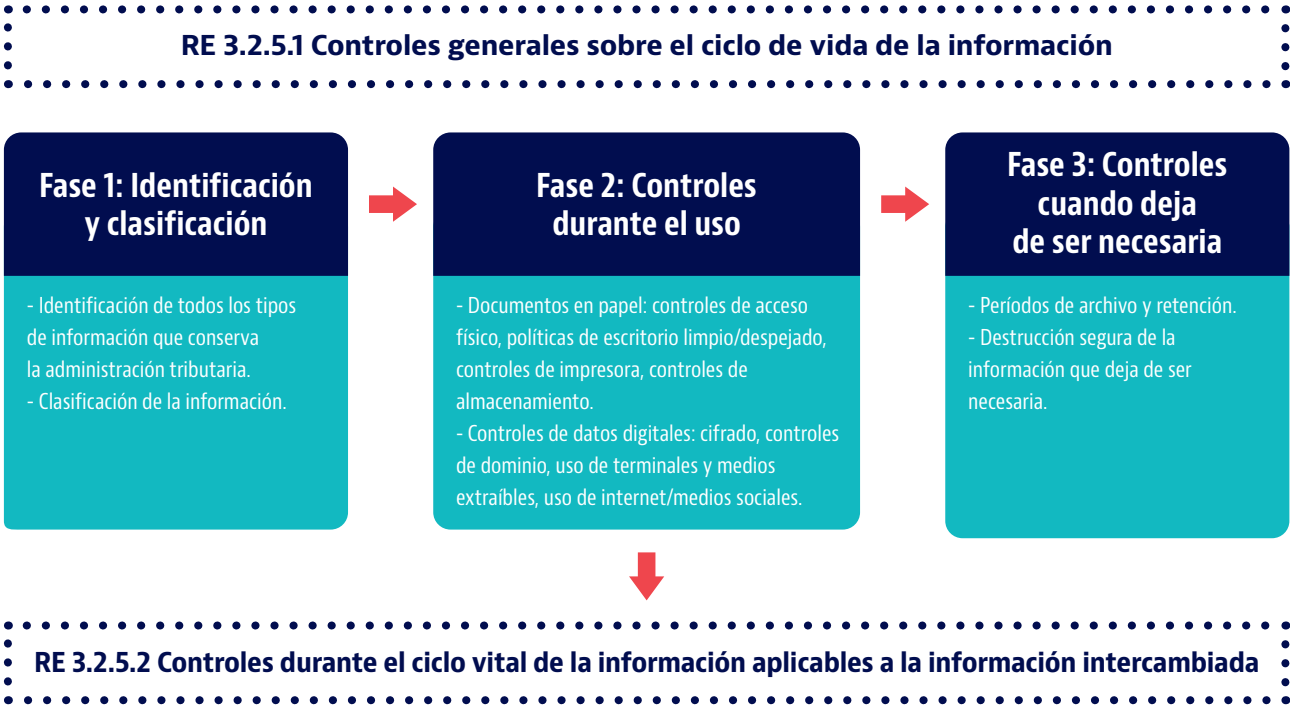
Fase 1. Identificación y clasificación de la información

La clasificación de la información es el punto de partida y el centro neurálgico de la gestión del ciclo de vida de la información, desde donde deben fluir los demás controles de seguridad. El propósito de la clasificación de la información es garantizar que ésta reciba una protección adecuada y acorde a su clasificación.

La información tratada por las administraciones tributarias procede de numerosas fuentes, tales como:

- Declaraciones de impuestos de los contribuyentes.
- Reporte de información por parte de terceros con los que el contribuyente tenga una relación comercial o laboral (p. ej. bancos, empleadores).

FIGURA 15. **Ciclo vital de la gestión de la información**



Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Recuadro 30. **Protección de la información, y procesos de gobierno y del negocio**

Solo es posible proteger la información durante todo el ciclo vida cuando se gestiona adecuadamente con reglas de gobierno claras. Idealmente, deberían existir líneas claras de rendición de cuentas con respecto a todos los activos de información, con un responsable de la información designado para cada tipo de información.

Además, los usuarios deben gestionar y tratar la información tributaria siguiendo procesos de negocio debidamente desarrollados y definidos. Por ejemplo, los datos sensibles de contribuyentes suelen tratarse dentro de procesos del negocio tributario básicos predefinidos tales como la recaudación de impuestos y el cobro de deudas tributarias. Siempre que sea posible, deben desarrollarse procesos de negocio para todas las formas significativas de uso de datos sensibles, incluida la información intercambiada. Esto es importante porque:

- Permite a la administración tributaria gestionar eficazmente, a través de políticas y procedimientos bien definidos, la manera en que los usuarios acceden a los datos y los usan, otorgándoles una mayor protección frente al acceso no autorizado y el uso indebido.
- Cuando existen procesos definidos, resulta mucho más fácil evaluar la eficacia del proceso en la protección de los datos, así como identificar e introducir mejoras que hagan más efectiva esa protección.
- Si no existen procesos de negocio definidos, lo más probable es que en la práctica no haya consistencia y puedan surgir métodos riesgosos de manejo de datos.

- Reporte de información por parte de otras entidades gubernamentales como, por ejemplo, el departamento de seguridad social.
- El EOI internacional.

Todos estos tipos de información tienen un cierto grado de sensibilidad y confidencialidad, y deben clasificarse en consecuencia, de modo que la información más sensible reciba mayores niveles de protección.

Si la información no está clasificada o no ha sido clasificada de acuerdo con su nivel de sensibilidad o confidencialidad, podrían ocurrir dos escenarios indeseados: que toda la información reciba el mismo nivel de alta protección o que toda esté protegida de manera inadecuada.

La aplicación de estándares elevados de protección a todos los tipos de información sería demasiado costosa y podría afectar a la disponibilidad de la información, mientras que proteger toda la información con menores estándares expondría la información sensible a un uso indebido y a la amenaza de violaciones de seguridad por parte de aquellos que no deberían tener acceso a la información.

Identificación de todos los tipos de información mantenida

Antes de la clasificación, lo primero que deben hacer las administraciones tributarias es conocer e identificar claramente los tipos de información que conservan. Los principales activos de información conservados por las administraciones tributarias, ya se encuentren en formato digital o físico, incluyen por lo general:

- Declaraciones de impuestos sobre la renta de las personas físicas y sobre sociedades.
- Información de empleadores.
- Correspondencia con los contribuyentes.
- Información intercambiada (automático, espontáneo y previa petición).
- Liquidaciones, resoluciones y dictámenes fiscales.
- Guías para el personal (y para los contribuyentes) relativas a la cumplimentación de declaraciones de impuestos.
- Guías sobre la realización de inspecciones fiscales y otras actividades de cumplimiento.
- Información relativa a investigaciones penales en curso.
- Circulares internas, documentos de trabajo y estudios de investigación.
- Información sobre TI que podría utilizarse con el fin de obtener acceso a la información del negocio tributario como, por ejemplo:
  - Credenciales de acceso, incluidas las contraseñas del sistema.
  - Código fuente.
  - Configuración de dispositivos de gateway y dominio.

Clasificación de la información

Una vez las administraciones tributarias han identificado todos los tipos de información que conservan, deben clasificarlos, estableciendo cómo cada categoría debe gestionarse y controlarse, y reflejarlo de forma clara en una política.

Las administraciones tributarias pueden usar distintos criterios de clasificación. Por lo general, se usan cuatro enfoques, que no son excluyentes entre sí (véase la Tabla 20). Las administraciones tributarias pueden usar más o menos criterios, en función de la información que conservan, sus leyes y prácticas nacionales y el tamaño y la escala de sus operaciones.

Cada tipo de información debe recibir su propia clasificación de acuerdo con los criterios que se usen. La Tabla 21 muestra un ejemplo simplificado de una matriz de clasificación de información, si bien los ejemplos que se muestran no son exhaustivos y se ofrecen únicamente a efectos de consulta e ilustrativos. No obstante, es importante señalar que la información intercambiada debe ser, como mínimo, clasificada como confidencial dentro de la administración tributaria, a fin de garantizar controles adecuados.

Fase 2. Controles para la protección de información durante el uso

Una vez que las administraciones tributarias hayan definido los tipos de información que conservan y los criterios para su clasificación, deben identificar los principales controles que son adecuados para cada categoría e incorporarlos de forma clara en una política. El marco de control diseñado debe hacer posible una protección adecuada de la información sensible y confidencial, a la vez que garantiza más facilidad para acceder a la información menos sensible.

Tabla 20. **Criterios para la clasificación de la información**

Criterios	Descripción
Sensibilidad	El criterio más habitual es la clasificación basada en la sensibilidad, con categorías que pueden incluir: ● Pública (p. ej. material utilizable en un sitio web externo) ● Interna (comunicaciones generales internas de la oficina) ● Restringida/confidencial (una categoría que normalmente incluye información del contribuyente) ● Secreta/de alto secreto (normalmente restringida a situaciones en las que existe una amenaza significativa para intereses individuales o colectivos como, por ejemplo, la vida, intereses empresariales o comerciales o el funcionamiento del Estado).
Acceso restringido	Usado normalmente junto con el criterio de sensibilidad, este criterio se refiere a controles adicionales que se basan en el principio de "necesidad de saber", más que en la sensibilidad propiamente dicha. Por ejemplo, debido a su sensibilidad, los datos del EOI suelen clasificarse como restringidos/confidenciales (son datos del contribuyente) pero, como consecuencia de las obligaciones contenidas en los tratados, el acceso se restringe aún más aplicando el principio de necesidad de saber y se concede únicamente a aquellos empleados que necesiten manejar datos del EOI para desempeñar sus funciones específicas.
Escala/ volumen	Los registros a gran escala representan una vulnerabilidad mayor que un registro individual, por lo que deben aplicarse controles reforzados cuando se trabaja con registros agregados. Estos criterios pueden clasificarse usando "niveles de impacto", relativos al impacto en la confidencialidad e integridad de los datos cuando el acceso es comprometido, y el tipo de controles de acceso que deben adoptarse en función del nivel de impacto. Por ejemplo, puede aplicarse una escala del 1 al 5, siendo 1 el impacto menor y reservando el nivel 5 para el impacto más elevado en términos de "amenaza para la vida o para el Estado". Un único registro individual de EOI que se lleve en un ordenador portátil o en una memoria USB cifrada podría tener un impacto de nivel 2 o 3; mientras que la base de datos del AEOI podría tener un impacto de nivel 4. Estas clasificaciones determinarían, por ejemplo, el tipo de controles de acceso que deben adoptarse, p. ej. si los datos deben cifrarse o no.
Tipo de información	Este criterio puede usarse para clasificar distintos tipos de información, por ejemplo, los registros de recursos humanos o de contrataciones pueden ser clasificados como En Confidencia, y el material de orientación para contribuyentes puede clasificarse como información No en Confidencia.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Tabla 21. **Ejemplo de matriz de clasificación de información**

Categoría	1 – Pública	2 – De uso interno	3 – Confidencial	4 – Muy confidencial
Descripción	Información que puede ponerse a disposición del público e información interna cuya divulgación no autorizada no causaría daño alguno a la administración tributaria.	Información interna de carácter no sensible, pero cuya divulgación no autorizada podría ser inadecuada/ inconveniente para la administración tributaria.	Información interna de carácter sensible a la que solo puede accederse en atención a la necesidad de saber, y cuya divulgación no autorizada podría causar algún daño a la administración tributaria y a los interesados afectados.	Información interna de carácter muy sensible y en ocasiones de amplio alcance a la que solo puede acceder un número muy limitado de personas en atención a una estricta necesidad, y cuya divulgación no autorizada podría causar daños graves y/o importantes a la administración tributaria y a los interesados afectados.
Información comprendida en la categoría	• Guías para contribuyentes relativas a la cumplimentación de declaraciones de impuestos. • Sitio web externo	• Procedimientos operativos para la realización de inspecciones fiscales. • Materiales formativos para el personal. • Circulares internas no confidenciales.	• Información de los empleadores. • Correspondencia con los contribuyentes. • Evaluaciones/ resoluciones/ determinaciones. • Contratos, Acuerdos de Nivel de Servicio. • Circulares internas confidenciales.	• Declaraciones de impuestos individuales. • Datos del EOIR. • Datos del AEOI. • Información de TI para el acceso a datos del negocio (código fuente, credenciales de acceso)

Por lo general, deben aplicarse controles:

- **Mientras la información se encuentra en uso o "en movimiento"**, es decir, mientras se esté usando para cumplir los fines del negocio tributario o circule entre ubicaciones o entornos de trabajo.
- **Mientras se encuentre almacenada o "en reposo"** entre usos.

Los controles deben basarse en los principios de acceso descritos en el RE 3.2.3 (gestión del acceso), tales como los principios de necesidad de saber y mínimo privilegio aplicables al acceso. La información sensible, tanto en formato digital como físico, solo debe ser accesible para quienes tengan un fin de negocio legítimo.

En el pasado, la información del contribuyente se gestionaba principalmente en formato físico. Con el tiempo, con el avance de la tecnología y la necesidad de llevar a cabo la actividad de la administración tributaria de forma más eficaz a la vez que se protege la información, las administraciones tributarias han empezado a alejarse del concepto de archivo físico y a conservar la información de forma digital. En la actualidad, la información que conservan las administraciones tributarias más avanzadas se recibe por medios digitales o se digitaliza cuando se recibe y se gestiona a través de flujos de trabajo automatizados. Las administraciones tributarias se encuentran en distintas fases de transición del papel al funcionamiento digital, por lo que, a efectos de la evaluación de la confidencialidad, es importante que se tengan en cuenta ambos formatos de gestión de la información, según el caso, a la hora de determinar los controles que deben aplicarse.

Las siguientes secciones ofrecen orientaciones y principales controles de buenas prácticas que suelen aplicar las administraciones tributarias con respecto a la información en papel y digital.

Controles para la protección de documentos en papel

Los principales elementos de la protección de documentos en papel en las instalaciones de la oficina tributaria incluyen medidas de acceso físico de empleados a documentos en papel, controles de políticas de escritorio despejado, controles de impresora y controles de almacenamiento cuando la información no se está utilizando y se encuentra "en reposo".

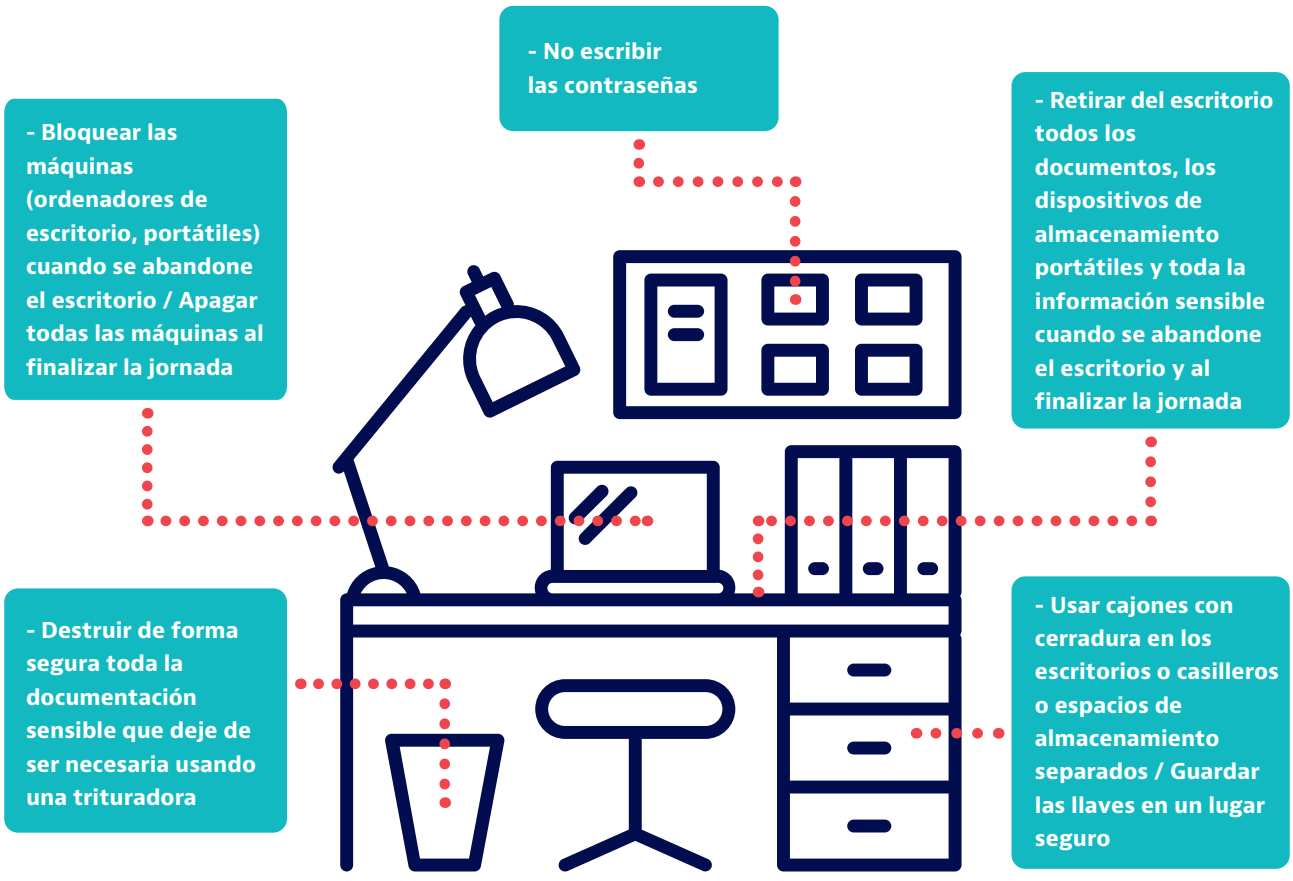
Acceso físico de personal autorizado a documentos en papel

El acceso de empleados a documentos en papel es más difícil de gestionar que los datos digitales, pues el acceso a estos últimos puede ser relativamente más fácil de gestionar y restringir a través de controles de acceso lógico (véanse el RE 3.2.3.3 y el RE 3.2.3.4, relativos a los controles que se aplican al acceso lógico).

El acceso a los documentos en papel normalmente se restringe del siguiente modo:

- Limitando el acceso a edificios e instalaciones únicamente a personas autorizadas e implantando controles para segregar los espacios de trabajo dentro de las administraciones tributarias. Las medidas de seguridad pueden incluir la obligación de que los empleados autorizados utilicen un pase electrónico o una identificación con fotografía, o la adopción de sistemas de entrada con código para acceder a algunas o todas las zonas de la oficina, incluida la unidad de EOI u otra zona o almacén de archivos donde se ubique la información sensible. Estos controles pueden complementarse con sistemas de control secundarios tales como personal de seguridad, CCTV y políticas para impedir el acceso de visitas no acompañadas. Estos aspectos se han analizado con más detalle en la sección relativa a los requisitos de seguridad aplicables al acceso físico, comprendida en el RE 3.2.3.1 y el RE 3.2.3.2.
- Implementar normas claras relativas el alcance de la información del contribuyente a la que pueden acceder los empleados en función de la necesidad para desempeñar sus funciones. Por ejemplo, si se realizaron pesquisas sobre un aspecto concreto de los asuntos de un contribuyente, el funcionario de la administración tributaria a cargo de dichas pesquisas debe tener acceso únicamente a la información relacionada con ese aspecto, pero no a todos los registros físicos del contribuyente.

FIGURA 16. **Controles de la política de escritorio limpio/despejado**



- El etiquetado de los documentos clasificados como confidenciales, y una descripción clara en una política del modo en que los empleados pueden acceder a los documentos etiquetados o marcados como "confidencial" y gestionar dichos documentos.

Política de escritorio limpio/despejado

Los controles de la documentación física van más allá de la gestión del papel: también guardan relación con la debida gestión y control del entorno de escritorio.

Una política de escritorio limpio/despejado (CDP) especifica el estado en que los empleados deben dejar su espacio de trabajo cuando abandonan sus escritorios o salen de la oficina, con el fin de hacer cumplir el principio de necesidad de saber y prevenir que usuarios no autorizados vean información que no les corresponde ver. La CDP limita la exposición a empleados sin derechos de acceso y a partes externas (p. ej. personal de limpieza, personal de mantenimiento, vigilantes de seguridad).

Las CDP pueden exigir (véase la figura 17):

- Que los empleados retiren de sus escritorios toda información sensible, documentación, dispositivos de almacenamiento portátiles (USB, unidades de disco) cuando abandonen sus escritorios y al acabar su jornada.
- Bloqueo de máquinas (ordenadores de escritorio, portátiles) siempre que abandonen el escritorio o que las apaguen al finalizar su jornada.
- Prohibición de anotar las contraseñas.
- El uso de cajoneras con cerradura en los escritorios, o casilleros o espacios de almacenamiento separados.
- Guardar las llaves en un lugar seguro.
- Destrucción segura de todos los documentos sensibles que dejen de ser necesarios, utilizando trituradoras.

El jefe de oficina u otra persona responsable puede encargarse de la labor de revisar la oficina al final de la jornada y confiscar o destruir todas las carpetas, documentos en papel o medios de almacenamiento portátiles que los empleados hayan dejado en su escritorio.

Al igual que sucede con todas las políticas sobre confidencialidad y seguridad, para que una CDP sea eficaz debe estar documentada y ponerse en conocimiento de los empleados.

Controles de impresora

Es posible que el personal tenga que imprimir información sensible que se conserva digitalmente. Una vez impresa dicha información, si no se aplican controles adecuados puede comprometerse o perderse la eficacia de los controles de acceso lógico (véanse el RE 3.2.3.3 y el RE 3.2.3.4, relativos a los controles aplicables al acceso lógico). Los controles de impresora pueden incluir:

- Las circunstancias en las que la información puede y no puede imprimirse, cuando sea posible ejecutadas mediante reglas de impresión codificadas.
- Si se imprime información sensible, establecer instrucciones de manejo claras y marcas de confidencialidad que, por ejemplo, se muestren en el documento impreso con una marca de agua o en el encabezamiento/pie de página.
- Controles para reducir el riesgo de que el material sea recogido por una persona distinta del usuario autorizado como, por ejemplo, el uso de controles de proximidad, de modo que solo el usuario previsto o autorizado pueda completar el proceso de impresión estando físicamente presente junto a la máquina.
- Saneamiento o cifrado del almacenamiento de la impresora. Como las impresoras disponen de almacenamiento, si no se adoptan controles adecuados las impresoras arrendadas podrían ser devueltas a los arrendadores con la grabación de los contenidos del material impreso.

Controles de almacenamiento de documentos en papel cuando están "en reposo"

Cuando los documentos en papel no se estén utilizando (esto es, cuando se encuentren almacenados o "en reposo") las administraciones tributarias pueden considerar los siguientes controles:

- Almacenamiento de documentos en papel en unidades de almacenamiento, cajas fuertes o habitaciones con cerradura. Los armarios o las cajas fuertes deben estar inmovilizados y cerrados con llave en todo momento. El acceso a las llaves debe restringirse exclusivamente a empleados autorizados. El uso de armarios con múltiples cerraduras para guardar información clasificada y sensible es deseable, aunque si el acceso a las instalaciones es suficientemente seguro esto podría compensar controles con menos cerraduras.
- El uso de zonas de almacenamiento separadas para guardar archivos de contribuyentes y otros documentos sensibles. Los controles de seguridad en estas zonas deben garantizar el acceso únicamente de empleados que tengan una necesidad de negocio

legítima como, por ejemplo, personal de seguridad que vigile la entrada al depósito y permita el acceso únicamente a personal autorizado con identificación con fotografía, códigos de seguridad para acceder al depósito, identificación biométrica o video vigilancia.

- Inventarios de todos los documentos almacenados.

El Recuadro 31 contiene un ejemplo de controles de documentos en papel.

La lista completa de controles que deben aplicarse a la información puede elaborarse en forma de matriz o matrices dependiendo de las distintas clasificaciones de la información, y la escala y la complejidad de la información que conserva una administración tributaria. La Tabla 21 muestra un ejemplo simplificado de una matriz con controles aplicables a los documentos en papel según su clasificación y nivel de confidencialidad.

Esta matriz se utiliza únicamente a efectos ilustrativos y muestra ejemplos de controles que siguen el orden con el que se presentan en este manual. Se recomienda a las administraciones tributarias que diseñen matrices adaptadas a sus propios criterios de clasificación de la información y procedimientos organizativos concretos.

Tabla 22. **Ejemplo de matriz con controles relativos a la información en papel según el nivel de confidencialidad**

1 – Pública	2 – De uso interno	3 – Confidencial	4 – Altamente confidencial
• No se necesita etiquetado.	• Etiquetada como "solo para uso interno".	• Etiquetada como "confidencial".	• Etiquetada como "altamente confidencial".
• No se necesitan restricciones de acceso ni almacenamiento específicos. Puede dejarse en cajones o armarios sin cerradura.	• Acceso restringido a grupos o departamentos específicos. • Asegurada en cajones o armarios con cerradura.	• Acceso restringido a personas específicas en función de la necesidad de saber. • Debe almacenarse en archivadores con cerradura en escritorios, o en una habitación a la que únicamente puede acceder personal autorizado.	• Acceso restringido a personas específicas en función de la necesidad de saber. • Asegurada en armarios fijos con candados de alta seguridad, localizados en una habitación segura a la que solo puede acceder personal autorizado. • Vigilantes de seguridad y video vigilancia cuando se almacenen en habitaciones seguras.
• Sin restricciones de reproducción e impresión. • Puede dejarse en un escritorio o impresora sin protección.	• Puede copiarse e imprimirse únicamente por grupos y departamentos autorizados • No puede dejarse en un escritorio o impresora sin medidas de seguridad.	• Puede copiarse e imprimirse únicamente por personas autorizadas • Si se copia e imprime, no debe dejarse en un escritorio o una impresora sin medidas de seguridad.	• Puede copiarse e imprimirse únicamente por personas autorizadas y con autorización de un responsable de alto nivel en cada caso concreto. • Si se copia e imprime, no debe dejarse en un escritorio o una impresora sin medidas de seguridad. • Todas las copias deben numerarse y registrarse.
• Puede eliminarse en el contenedor de reciclaje de papel.	• Trituración tras su uso.	• Trituración tras su uso.	• Microtrituración o trituración transversal tras su uso.

Recuadro 31. **Ejemplo de controles de documentos en papel**

Toda la información confidencial en la administración tributaria de la Jurisdicción A, como la información del contribuyente, está claramente etiquetada como "Confidencial".

El acceso a información en papel confidencial se restringe a personas específicas sobre la base de la necesidad de saber, y debe almacenarse en archivadores con cerradura en los escritorios o en una habitación a la que pueda acceder únicamente personal autorizado. La información confidencial puede ser copiada e impresa únicamente por personas autorizadas. Cuando abandonen sus escritorios, el personal debe guardar de forma segura copias impresas con información confidencial en los cajones de su escritorio bajo llave. Toda la información confidencial debe ser triturada después de su uso.

Todos los ordenadores de escritorio y portátiles deben ser apagados al finalizar la jornada. El último funcionario de la administración tributaria que salga de la oficina debe revisar todos los escritorios y apagar todos los dispositivos que se hayan dejado encendidos, así como retirar todas las copias no recogidas de la fotocopiadora/impresora. Las políticas de escritorio limpio y los controles de impresora se recogen de forma clara en la Política de Seguridad de la Información de la administración, y se aplican sanciones por incumplimiento.

La información intercambiada que se reciba en formato de papel es separada del resto de información del contribuyente obtenida dentro del país, y los registros se guardan en un depósito seguro al que solo tiene acceso el personal de la unidad de EOI en función de la necesidad de saber. La información de EOI siempre debe ser devuelta al depósito cuando finalice la jornada, y todos los accesos son registrados. El acceso a la sala de archivos se activa con la identificación electrónica del funcionario autorizado.

Controles para la protección de información digital

Cuando están en uso, los datos conservados digitalmente pueden enviarse por correo electrónico entre el personal o viajar a través de sistemas de información o a través de jurisdicciones (p. ej. datos del EOI). El personal también puede usar los datos en medios extraíbles. La información digital también puede estar "en reposo", almacenada en bases de datos en el centro de datos o guardada en un sistema de archivos del servidor.

Las violaciones de datos tributarios digitales como, por ejemplo, los datos del AEOI, podrían tener un impacto considerable, por lo que es esencial que se preste plena atención a los controles adecuados y que estos, por lo general, se basen en los riesgos. Los controles específicos incluyen:

- Cifrado.
- Controles de dominio.
- Controles de terminales o *endpoints*, medios extraíbles y dispositivos periféricos.
- Políticas de uso aceptable.
- Endurecimiento de sistemas o *computer hardening*.
- Controles en relación con el uso de Internet y medios sociales.

Si bien estos controles se superponen a los descritos en el RE 3.2.4.2, este último aborda los principales controles de seguridad del sistema de TI implantados en el entorno y la infraestructura de TI, mientras que los controles descritos en esta sección se aplican a los datos en sí.

Cifrado

Los datos son más vulnerables a su acceso no autorizado cuando se encuentran en movimiento y, bajo los estándares internacionales, los datos confidenciales deben cifrarse cuando están en uso y cuando circulan de un punto a otro como, por ejemplo, entre sistemas de información o cuando se transmiten por correo electrónico o a través de medios extraíbles.

Cuando se encuentren en reposo en bases de datos, los datos sensibles no necesariamente deben ser cifrados, siempre y cuando se implementen otras protecciones adecuadas a esas bases de datos a fin de garantizar que los datos no sean comprometidos. Estas protecciones podrían implementarse a través de controles de dominio, que se analizan en la siguiente sección.

A la hora de decidir si cifrar datos en reposo, las administraciones tributarias pueden tener en cuenta:

- **Análisis del riesgo**. El enfoque debe basarse en el riesgo y en una clara comprensión de las amenazas.
- **Rendimiento de los datos**. El cifrado puede afectar al rendimiento como, por ejemplo, provocando un retraso en la presentación de los datos, y existe un compromiso o *trade-off* entre confidencialidad y disponibilidad. No obstante, una administración tributaria puede considerar el retraso aceptable cuando la información es muy sensible y ha identificado riesgos para su integridad.

Si se realiza de forma adecuada, el cifrado puede proteger completamente los datos. Sin embargo, aun cuando se use el cifrado para datos en reposo, deben aplicarse a las bases de datos controles de dominio complementarios, incluyendo pruebas de penetración de sistemas y aplicaciones.

Recuadro 32. **Controles de cifrado para datos digitales en tránsito y en reposo**

Datos en tránsito

- Controles para la transmisión de información a través de aplicaciones web (p. ej. portales del contribuyente), tales como *Transport Layer Security* (TLS) o *Hypertext Transfer Protocol Secure* (HTTPS).
- Controles para la transmisión de información durante su intercambio digital (p. ej. videoconferencias, mensajería móvil), tales como el cifrado de extremo a extremo.
- Controles para la transmisión de información por correo electrónico, tales como StarTLS.

Datos en reposo

- Controles para prevenir violaciones de datos que se conservan en bases de datos, tales como estándares de cifrado simétrico.

En el Recuadro 32 se enumeran algunos de los controles de cifrado que pueden tenerse en cuenta.

Controles de dominio

Al igual que con la información en papel, que normalmente se protege guardándola en un único lugar o dominio como, por ejemplo, una caja fuerte, los datos digitales se almacenan en bases de datos centralizadas con servidores que gestionan el acceso a los mismos. Las administraciones tributarias deben aplicar protecciones adecuadas a esas bases de datos y servidores con el fin de garantizar que los datos sensibles y confidenciales no sean comprometidos. Estas protecciones se denominan "controles de dominio".

Si bien los controles de dominio se analizan en más detalle en el RE 3.2.4.2 relativo al entorno de seguridad del sistema de TI, y en el RE 3.2.6 relativo a la gestión operativa (registro y auditoría), por lo general incluyen:

- Segregación de entornos de infraestructura.
- *Firewalls* y antivirus.
- Controles de acceso reforzados, tales como la autenticación multifactor, el inicio de sesión de un solo uso y el acceso por tiempo limitado, en particular para cuentas privilegiadas.
- Reforzamiento de la seguridad del sistema operativo como, por ejemplo, a través de la desactivación de puertos.
- Registro y seguimiento reforzados.
- Exploración y auditoría de vulnerabilidades.

Reforzamiento de la seguridad de ordenadores de escritorio, mantenimiento del software

La protección de la información digital también implica controles con respecto a ordenadores de escritorio y la gama de aplicaciones de software que utiliza el personal, tales como el reforzamiento de la seguridad de los ordenadores de escritorio y el mantenimiento del software. Dado que estos controles no solo afectan a los datos manejados en ordenadores de escritorio y aplicaciones de software, sino también a la seguridad del entorno de TI de la administración tributaria en su conjunto, se abordan en el RE 3.2.4.2 relativo a los controles de seguridad de las tecnologías de la información.

Terminales, medios extraíbles y dispositivos periféricos

Esta parte se refiere a los controles de dispositivos de usuario final que se usan en el escritorio, incluidos:

- Terminales, como ordenadores de escritorio o portátiles.
- Medios extraíbles, como memorias USB o discos duros externos.
- Dispositivos periféricos como *mouse*, teclado o cámara web.

Deberán aplicarse controles cuando los dispositivos de usuario final tengan acceso a datos sensibles y sean móviles. Los controles esenciales suelen incluir:

- Cifrado de memorias USB.
- Saneamiento seguro de información sensible que haya sido transferida a medios extraíbles, una vez cumplido el fin para el que fue transferida.
- Uso de software específico de monitoreo de terminales.
- Sistemas de alerta cuando se usen periféricos no aprobados.
- Sistemas de prevención de pérdida de datos.

Uso de Internet, medios sociales y correo electrónico

El hacking social es un método que se utiliza para acceder de manera ilícita a datos digitales. Los piratas informáticos pueden tratar de vulnerar los datos mediante el envío de correos electrónicos de *phishing* al personal de la administración tributaria con el fin de distribuir *malware* por las redes de información tributaria. El *malware* también podría introducirse en los sistemas de la administración tributaria a través de redes o plataformas sociales.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Aunque los correos electrónicos de *phishing* básicos suelen tener una elaboración bastante tosca que permite a una persona capacitada detectarlos fácilmente, los piratas informáticos también emplearán técnicas de "ingeniería social" para adquirir información personal con el fin de lanzar ataques por correo electrónico cuidadosamente elaborados, que a veces se conocen como "*spear phishing*". Dichos correos utilizan a menudo el aspecto de los correos electrónicos internos, por lo que su detección puede resultar mucho más difícil. Las direcciones de correo electrónico gubernamentales suelen seguir un formato estándar, lo que facilita la elusión de los controles formales por parte de los piratas informáticos más capacitados.

Esto ilustra que, en última instancia, son seres humanos quienes controlan el uso de los equipos de TI y que, por tanto, es muy importante que los empleados tengan una comprensión clara e inequívoca de lo que está permitido y lo que no lo está con respecto al uso de terminales, medios extraíbles, dispositivos periféricos, internet y medios sociales. El éxito o fracaso de la gestión de los equipos y servicios que contienen información dependerá principalmente de que se logre la cooperación y el apoyo de los empleados. Por lo común, esto se logra mediante la adopción de una "política de uso aceptable" (PUA).

Aunque las administraciones tributarias pueden establecer PUAs, también pueden optar por evitar totalmente los riesgos, por ejemplo prohibiendo el uso tanto de medios extraíbles como de correos electrónicos personales y redes y plataformas sociales. Si se adopta un enfoque de políticas de uso aceptable, la realidad, no obstante, es que las administraciones tributarias solo disponen de un cierto nivel de control e influencia sobre los empleados, de tal modo que una formación eficaz acerca de los riesgos que presenta el uso de medios extraíbles, internet y medios sociales, combinada con campañas de sensibilización, es esencial para asegurarse de que las políticas se aplican de manera eficaz. Es preferible capacitar al personal para que haga lo correcto, antes que limitarse a confiar en la adopción de medidas disciplinarias cuando exista un incumplimiento.

Algunos elementos específicos que puede incluir una PUA son:

- Asumir siempre que un correo electrónico es una amenaza a menos que el empleado sepa que es genuino, es decir, que lo reconozca como genuino porque espera recibirlo y tanto el remitente como la dirección de correo electrónico son conocidos y genuinos.
- No abrir nunca documentos adjuntos a menos que se sepa que son genuinos y, en caso de necesidad, verificar su autenticidad con el remitente antes de abrirlos.

Recuadro 33. **Principios sugeridos para el diseño de políticas de uso aceptable**

Tanto si se diseña una PUA para el uso de medios extraíbles como de medios sociales, las administraciones tributarias pueden tener en cuenta:

- **El alcance y la lógica general**. Como punto de partida, es importante poner de manifiesto la lógica general que subyace a esta política, que es la protección de la información y los derechos a la privacidad de los contribuyentes. Lograr que los usuarios comprendan la función de esta política puede facilitar un mayor cumplimiento y cooperación.
- **Derechos y responsabilidades de los usuarios**. Las PUAs estándar definen los derechos y responsabilidades del personal, especialmente cuando se trata de garantizar la protección de la información.
- **Usos aceptables.** Siempre que sea posible, una PUA debe adaptarse a las necesidades de los empleados, p. ej. búsquedas en internet relacionadas con actividades laborales o incluso la tramitación de asuntos personales urgentes. Si no se permite el uso no profesional, la política debe definir qué es el uso no profesional y especificar en qué circunstancias está permitido.
- **Usos prohibidos**. A modo de ejemplo, los usos de internet y medios sociales pueden incluir búsquedas en internet específicas, descargas, navegación y realización de comentarios. La mayoría de las políticas incluyen prohibiciones contra usos o contenidos de carácter ilícito, nocivo u ofensivo, así como contra prácticas abiertamente ilícitas tales como esquemas fraudulentos, phishing, contenidos abusivos o de odio, la introducción de virus, la infracción de derechos de autor y de propiedad intelectual o industrial, la invasión de la privacidad, injurias y calumnias, acceso a sistemas sin permiso, uso que exceda los consentimientos relativos a la privacidad, extracción de listas de comercialización y envío de correo no deseado.
- **Estándares de privacidad**. Supone incluir disposiciones en materia de privacidad y uso de datos responsable en una PUA. La política puede definir qué tipos de datos son sensibles y por qué, y debe explicar en detalle el acceso y uso de datos sensibles.
- **Sanciones**. Deben incluirse las posibles consecuencias y las violaciones que se derivan de una infracción de la política.

Recuadro 34. **Ejemplo de controles aplicados a la información digital**

En la administración tributaria de la Jurisdicción B, la información confidencial que se conserva digitalmente solo puede transmitirse con cifrado. Los datos confidenciales, incluida la información intercambiada, solo pueden enviarse a un dominio de correo electrónico de la administración tributaria de la Jurisdicción B, o transmitirse por personas autorizadas a correos electrónicos externos fiables usando cifrado de extremo a extremo.

El acceso lógico a información confidencial está restringido a personas concretas en función de la necesidad de saber, y los derechos de acceso de usuarios y administradores se restringen mediante autenticación multifactor.

Todos los datos sensibles son únicamente legibles a través de dispositivos autorizados de la administración tributaria. La política de uso aceptable incluye una lista de todos los dispositivos de almacenamiento portátil cuyo uso está autorizado dentro de la administración tributaria. Los dispositivos extraíbles que contienen información confidencial deben guardarse en armarios o cajones fijos con candados de alta seguridad, o en una habitación a la que únicamente puede acceder personal autorizado. Existe un equipo especializado dentro del departamento de TI que lleva a cabo un seguimiento periódico del uso de terminales, medios de almacenamiento portátiles y dispositivos periféricos por parte del personal.

La información digital confidencial puede imprimirse únicamente cuando lo autorice la alta dirección, pero con la marca de agua "confidencial", y no debe dejarse sin supervisión una vez impresa.

La información confidencial se protege mediante el uso de sistemas de DLP y protecciones de terminales. El uso de medios sociales y de internet está bloqueado en la unidad de EOI, y en la política de uso aceptable se establecen procedimientos y sanciones específicos en esta materia.

- No hacer clic nunca en enlaces. Si se comprueba que es conveniente hacer clic en un enlace a la página web de una organización, es preferible que el empleado visite directamente su sitio web y acceda al enlace a través de la página de inicio.
- Prestar siempre atención a las advertencias de los productos antivirus y no ignorarlas bajo ningún concepto.
- Tener siempre cuidado con lo que publican los empleados en las plataformas de medios sociales.
- Aun cuando la política no permita el uso de medios sociales durante el desempeño de la actividad profesional, no obstante puede ser útil poner de manifiesto los riesgos que entrañaría usarlos.
- Solo deben utilizarse dispositivos aprobados y facilitados por la administración tributaria. Estos dispositivos deben cifrarse con arreglo a las políticas de clasificación de datos de la administración tributaria.
- Los dispositivos deben utilizarse únicamente según lo prescrito en las políticas de la administración tributaria.

El Recuadro 33 sugiere algunos principios que pueden tener en cuenta las administraciones tributarias a la hora de diseñar una PUA.

La PUA debe comunicarse al personal, tanto durante el proceso de incorporación como en la formación periódica y las campañas de sensibilización, como parte de los controles de recursos humanos contemplados en el RE 3.2.2.

También es importante que las actividades de los empleados sean monitoreadas, y que los superiores se involucren en el monitoreo y cumplimiento de estas políticas. Pueden aplicarse dos niveles de verificación:

- Los superiores deben tener la responsabilidad (y deben servir de ejemplo) de hacer hincapié en la importancia de una adecuada seguridad, incluso con respecto al uso de los equipos de trabajo.
- Los equipos de seguridad responsables deben realizar controles aleatorios.

Tal y como sucede con la información en papel, los controles que deben aplicarse a la información digital pueden presentarse en forma de matriz o matrices. La Tabla 23 muestra un ejemplo simplificado de una matriz para información digital según su nivel de confidencialidad, y el Recuadro 34 ofrece algunos ejemplos de controles aplicados en una administración tributaria.

Fase 3. Controles cuando la información deja de ser necesaria: períodos de retención y destrucción

Esta sección aborda la última parte del ciclo de vida, en la que deben eliminarse tramos de información concretos porque se vuelven menos relevantes o dejan de serlo con respecto a las necesidades de la administración tributaria.

Un principio general de las buenas prácticas en materia de seguridad de la información es que la información que deja de ser necesaria debe destruirse. Esto se debe a que la conservación de información, y en particular de información sensible, entraña un riesgo intrínseco que, como regla general, es proporcional a la sensibilidad de la información y al período durante el cual la información se conserva.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

Tabla 23. **Ejemplo de matriz con controles para la información digital según su nivel de confidencialidad**

1 – Pública	2 – De uso interno	3 – Confidencial	4 – Muy confidencial
• Sin cifrado. • Puede ser compartida entre el personal por correo electrónico, y conservarse internamente en dispositivos móviles.	• Sin cifrado. • Puede ser compartida entre el personal por correo electrónico dentro de grupos y departamentos.	• Debe cifrarse cuando se transmite. • Solo puede enviarse por correo electrónico o transferirse de modo cifrado por personas autorizadas.	• Debe cifrarse cuando se transmite. • Solo puede enviarse por correo electrónico o transferirse de modo cifrado por personas autorizadas y con autorización de un directivo en cada caso concreto.
• Acceso lógico sin restricciones.	• Acceso lógico restringido a grupos o departamentos específicos.	• Acceso lógico restringido a personas específicas según la necesidad de saber. • Los derechos de acceso de los usuarios y administradores se restringen con autenticación multifactor.	• Acceso lógico restringido a personas específicas según la necesidad de saber. • Los derechos de acceso de los usuarios y administradores se restringen con autenticación multifactor.
• N/A	• N/A	• Bases de datos segregadas del resto de información. • Guardada en servidores seguros protegidos con *firewalls*, antivirus y contraseñas.	• Bases de datos segregadas del resto de información. • Guardada en servidores seguros protegidos con *firewalls*, antivirus y contraseñas.
• Puede conservarse en dispositivos móviles. • Los medios extraíbles que contienen esta información pueden guardarse en cajones o armarios sin cerradura.	• Puede conservarse en dispositivos móviles dentro de grupos y departamentos. • Los medios extraíbles que contienen esta información deben guardarse en cajones y armarios con cerradura.	• Solo puede conservarse en dispositivos extraíbles autorizados y con cifrado. • Los dispositivos extraíbles que contienen esta información deben guardarse en armarios o cajones con cerradura, o en una habitación a la que únicamente pueda acceder personal autorizado.	• Solo puede conservarse en dispositivos extraíbles si son autorizados por superiores. • Los medios extraíbles que contienen esta información deben guardarse en armarios fijos con candados de alta seguridad, o en una habitación a la que únicamente pueda acceder personal autorizado según la necesidad de saber. • Uso de sistemas de protección de terminales y medios extraíbles. • Uso de sistemas de DLP.
• Sin restricciones de impresión.	• Puede imprimirse, pero con la marca de agua "solo para uso interno", y no debe dejarse sin supervisión una vez impresa.	• Puede imprimirse, pero con la marca de agua "confidencial", y no debe dejarse sin supervisión una vez impresa.	• Solo puede imprimirse con autorización de un superior en cada caso concreto.

Si la información sensible tiene una finalidad útil, el valor de retener la información compensa el riesgo de conservarla. No obstante, si la información deja de tener un valor esencial, la buena práctica requiere que la información sensible sea destruida, eliminando cualquier riesgo residual. Es posible, no obstante, que las administraciones tributarias estén sujetas a obligaciones legales de conservar información durante un plazo determinado aun después de que haya dejado de ser necesaria.

Las administraciones tributarias deben adoptar una política clara de destrucción de la información, haciendo referencia a los períodos de retención aplicables y los requisitos para la eliminación segura de los documentos, ya sean físicos o digitales. La política debe definir:

- Los distintos tipos de documentos que mantiene la administración tributaria.
- Su clasificación de seguridad.
- Los motivos por los cuales los documentos son retenidos.
- El período durante el cual deben retenerse los documentos.
- Los mecanismos de retención.
- Los métodos y procesos de saneamiento o destrucción.

La política debe estar respaldada por procesos de revisión de los documentos durante todo su ciclo de vida con el fin de asegurarse de que siguen siendo necesarios y se están utilizando, así como procedimientos para adoptar medidas en el momento en que dejen de ser necesarios.

No obstante, el hecho de que la información haya dejado de ser necesaria no necesariamente significa que tenga que ser destruida de manera automática. Las políticas pueden contemplar un proceso de revisión antes de llevar a cabo su destrucción o borrado.

Si se adopta una decisión tanto de retener como de destruir la información, debe llevarse un registro de lo siguiente:

- La información que se va a retener o destruir.
- La justificación desde un punto de vista del negocio de la retención o destrucción.
- La próxima fecha de revisión en caso de que se decida retener la información.

Las decisiones de retención o destrucción de la información deben adoptarse por parte de los altos directivos o los responsables de la información con responsabilidad general con respecto a ese ámbito operativo de la administración tributaria o tipo de información.

Períodos de retención

Si bien, como principio general, la buena práctica requeriría que la información que ya no sea necesaria se destruya, las administraciones tributarias pueden estar legalmente obligadas a retener información durante un plazo fijo, aun cuando haya dejado de ser necesaria a efectos fiscales. En algunos casos, ese plazo es permanente. En otros casos, existe una obligación de enviar una parte de la información del contribuyente a archivos nacionales.

Si se aplican plazos de retención obligatorios, las administraciones tributarias deben evaluar los riesgos de conservar la información y adoptar medidas adecuadas para reducir el riesgo de retención a un nivel aceptable. Es importante que el responsable de la información asuma su responsabilidad con respecto a esos riesgos y para garantizar una aplicación eficaz de las medidas de mitigación. Estas medidas de mitigación incluyen:

Documentos en papel

- **Clasificación o depuración**. Mantener únicamente los documentos que estén sujetos a una obligación estricta de retención.
- **Almacenamiento más seguro**. Los documentos en papel que deban seguir consultándose de manera regular pueden mantenerse en almacenes diseñados para facilitar el acceso, y los documentos que ya no sean necesarios pueden ser archivados en un depósito más seguro.
- **Digitalización de documentos físicos y almacenamiento de copias electrónicas fuera de línea**. Esto se aplica únicamente cuando no exista ninguna razón forense para retener la versión en papel. En algunas jurisdicciones, la normativa sobre evidencias exige que en los procedimientos judiciales se utilice el ejemplar original en papel y no una copia digital. Por lo tanto, es importante determinar si la legislación de una jurisdicción en particular tiene este requisito, a fin de conservar el ejemplar original en papel.

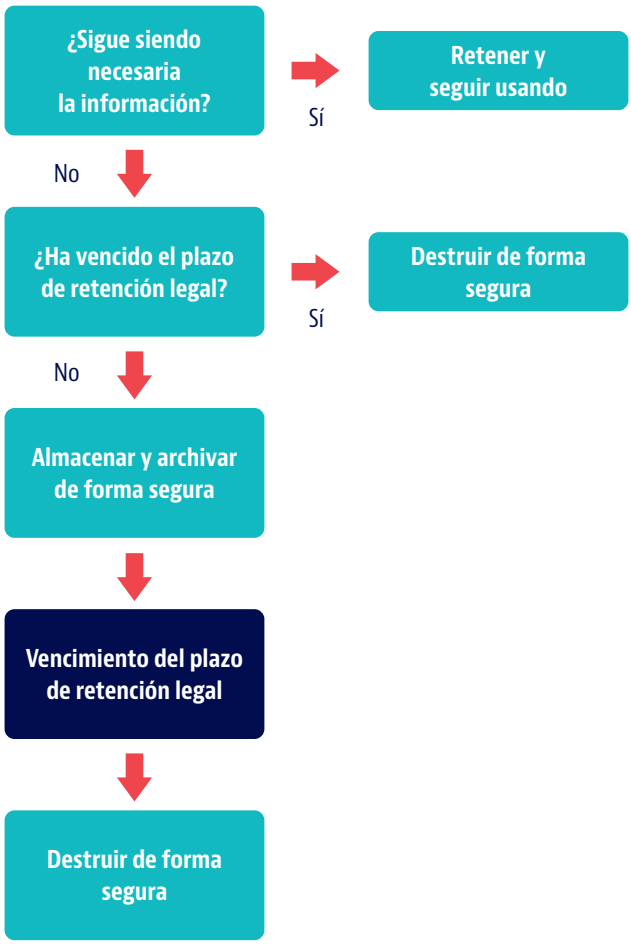
Documentos digitales:

- **Cifrado de datos**. El cifrado puede disminuir el riesgo de seguridad al retener la información.
- **Traslado de grupos de datos antiguos a un almacenamiento fuera de línea**. El almacenamiento fuera de línea significa que el dispositivo de almacenamiento no está conectado normalmente a ningún entorno operativo, y que solo se conecta cuando sea necesario. Esto puede lograrse a través de una base de datos separada o mediante algún tipo de medio

extraíble tal como un disco externo. Es importante que el almacenamiento fuera de línea se guarde de forma segura y se someta a revisiones periódicas.

Las administraciones tributarias deben llevar registros adecuados de todo el material, ya sea físico o digital, que está siendo retenido. Véase la Figura 17 a modo de ejemplo de un proceso de retención y destrucción de información.

FIGURA 17. **Ejemplo de proceso de retención y destrucción de información**



Eliminación de la información de forma segura

Las administraciones tributarias deben emplear métodos seguros de destrucción o saneamiento de la información que sean proporcionales a la sensibilidad de dicha información. Estos métodos deben garantizar que ningún material pueda recuperarse tras su destrucción o saneamiento. También deben adoptarse procedimientos claros para determinar la base sobre la que la información, o los medios que contienen información, se identifica y selecciona para ser destruida o saneada.

En caso de información en poder de terceros o contratistas externos, las administraciones tributarias también deben establecer requisitos de destrucción o eliminación, que deben incluirse en los contratos o en los SLAs.

Recuadro 35. **Saneamiento de medios de almacenamiento y su importancia**

El saneamiento es el proceso por el cual se tratan datos conservados en medios de almacenamiento con el fin de reducir la probabilidad de recuperación y restauración hasta un nivel aceptable. Algunas formas de saneamiento permitirán a las administraciones tributarias reutilizar los medios, mientras que otras son de naturaleza destructiva y dejarán los medios inutilizables.

Cuándo sanear los medios

Existen diversas circunstancias en las que las administraciones tributarias pueden considerar sanear medios de almacenamiento:

- Reutilización: cuando un dispositivo se asigne a un usuario diferente o se reutilice dentro de la administración tributaria.
- Reparación: cuando se devuelva un dispositivo defectuoso al vendedor para su reparación o sustitución.
- Eliminación o destrucción: saneamiento de medios no deseados antes de su eliminación o destrucción, especialmente cuando la administración tributaria haya contratado a un tercero para eliminar o destruir el material.

En todos estos casos, los medios saldrán de su entorno operativo normal y estarán con usuarios diferentes (p. ej. terceros y/u organizaciones y personas de menos confianza), por lo que estarán expuestos a un mayor riesgo.

Los riesgos de no sanear

Si los soportes de almacenamiento no se sanean debidamente, es posible que sigan conteniendo datos sensibles, dando lugar a la aparición de los siguientes riesgos:

- Paradero desconocido de datos sensibles o pérdida de control sobre activos de información.
- Apropiación de datos confidenciales del contribuyente y uso de los mismos para cometer fraudes o robos de identidad.

Fuente: www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

Los métodos de destrucción o saneamiento de información incluyen:

En papel

Normalmente el papel se tritura transversalmente o se incinera. Las jurisdicciones pueden establecer distintos niveles de trituración (tamaño y grosor de las partículas trituradas) según la clasificación de confidencialidad del documento.

Medios magnéticos

Los medios magnéticos deben tratarse y eliminarse siempre de la forma más apropiada para los datos más sensibles que hayan sido almacenados en ellos durante su vida útil. Los dispositivos de medios que no vayan a ser reutilizados (p. ej. dispositivos de estado sólido, discos duros, USB, discos) deben destruirse y degradarse, normalmente a través de un proceso de molienda con equipos especializados, hasta un punto en el que no quede material utilizable.

Si los medios magnéticos no van a destruirse y van a reutilizarse a nivel interno, deben adoptarse medidas adecuadas con el fin de eliminar la información existente antes de su reutilización, o bien sanear los medios. Medios extraíbles no saneados adecuadamente podrían exponer a los datos sensibles al riesgo de acceso por parte de usuarios no autorizados. El Recuadro 35 ilustra la importancia de sanear los medios de almacenamiento. Las administraciones tributarias pueden decidir aplicar distintos métodos, tales como técnicas de sobreescritura, y pueden consultar los estándares internacionales sobre saneamiento de medios para obtener más orientación.

Como puede ser difícil eliminar todo indicio de los datos de un disco, no suele ser buena práctica, sin embargo, reutilizar un disco que ha contenido información muy confidencial. En cualquier caso, se recomienda que las administraciones tributarias lleven registros, normalmente como parte del inventario de activos (que se analiza en el RE 3.2.4.3 relativo a los controles de gestión de activos), indicando el historial de uso de cada dispositivo.

El Recuadro 36 proporciona algunos ejemplos de procedimientos de destrucción.

RE 3.2.5.2. Protección de la información intercambiada

Esta sección aborda las medidas para hacer efectivas en la práctica las disposiciones de confidencialidad y uso adecuado contenidas en acuerdos internacionales de intercambio de información y leyes domésticas en materia de intercambio de información (véase el RP 3.1).

Recuadro 36. **Ejemplo de destrucción segura de información confidencial que deja de ser necesaria**

La administración tributaria de la Jurisdicción C lleva a cabo una destrucción masiva de documentos en papel y digitales como mínimo una vez al año, o cuando ha acumulado suficiente material. Contrata a un contratista con equipos especializados para trituración (microtrituración o trituración transversal) y/o molienda. Este proceso se materializa a través de un procedimiento por escrito para la destrucción y eliminación de información oficial de la administración tributaria:

- El material (en papel o soporte magnético) se incluye en un registro de materiales que deben destruirse. Este registro permite hacer un seguimiento del material hasta el momento en que se ha producido la destrucción y el hecho de la destrucción ha sido verificado y validado por el personal designado de la administración tributaria, nombrado por un alto directivo.
- Los materiales se transportan de forma segura a instalaciones adecuadas y se conservan de manera segura durante algún tiempo antes del evento de destrucción. El registro de materiales a destruir registra la ubicación actual del material esperando ser destruido y la persona que es responsable del material en ese momento. La persona responsable asume la responsabilidad de garantizar que los materiales se conserven de forma segura y de realizar las debidas comprobaciones para verificar que se conservan de ese modo.
- Cuando el material está destinado a su destrucción física y pase cierto tiempo antes de que se lleve a cabo dicha destrucción, los medios de almacenamiento se sanean de manera segura antes de su almacenamiento, como preparación para su destrucción.
- Antes del día de la destrucción, se elabora un programa con una descripción de todo el material que va a destruirse. Se envía una copia a un testigo independiente, que aprueba que se proceda a dicha destrucción. El testigo está presente durante todo el proceso de destrucción, en primer lugar para revisar el programa a medida que cada elemento se retira de su almacenamiento seguro, a continuación para verificar que cada elemento se destruye conforme a lo dispuesto en los procedimientos y, por último, para confirmar que todos los elementos del programa han sido destruidos conforme a lo previsto.

Un marco GSI que se ajuste a los estándares y mejores prácticas reconocidas internacionalmente (Requisito Principal 3.2)

A fin de proteger la información intercambiada, las administraciones tributarias pueden:

- Utilizar las políticas y prácticas desarrolladas para garantizar la confidencialidad con fines fiscales domésticos también con respecto a la información objeto intercambiada, p. ej. aplicando los tipos de controles que se describen en el RE. 3.2.5.1.
- Desarrollar políticas y prácticas a la medida y reforzadas expresamente para la información intercambiada. A veces estas políticas se incorporan al manual de EOI, y por lo general incluyen:
  - Clasificación de confidencialidad y etiquetado de la información intercambiada.
  - Controles de acceso a registros de EOI digitales y físicos.
  - Transmisión segura de información a autoridades competentes extranjeras.
  - Transmisión segura de información de instituciones financieras en el caso del Estándar AEOI.
  - Transmisión segura de información de la autoridad competente o la unidad de EOI a otras áreas de la administración tributaria o a partes externas.

Clasificación y etiquetado de la información intercambiada

La información intercambiada, tanto la enviada como la recibida, debe clasificarse adecuadamente como confidencial y etiquetarse visiblemente como tal. El etiquetado suele efectuarse a través de un "sello de tratado" para el correo postal y los archivos de EOI en papel, o una marca de agua en el caso de archivos intercambiados por medios electrónicos (es decir, la marca indica que la información ha sido intercambiada con arreglo a un acuerdo internacional de intercambio de información y que está sujeta a sus restricciones específicas en materia de divulgación y uso, conforme se describe en el RP 3.1).

El sello de tratado o marca de agua puede señalar, por ejemplo:

"SE FACILITA ESTA INFORMACIÓN CON ARREGLO A LAS DISPOSICIONES DE UN TRATADO FISCAL Y SU USO Y DIVULGACIÓN SE REGIRÁN POR LAS DISPOSICIONES DE DICHO TRATADO FISCAL."

Controles de acceso a registros de EOI digitales y físicos recibidos de autoridades competentes extranjeras

Estos controles pueden incluir:

- Que solo cierto personal autorizado pueda acceder a las instalaciones de la unidad de EOI, portando la debida identificación (p. ej. pase electrónico, identificación con fotografía). El resto de los empleados solo puede acceder a la unidad de EOI con autorización del jefe de la unidad de EOI. El público en general no puede acceder a dicha unidad bajo ninguna circunstancia.
- Los funcionarios de EOI están sujetos a comprobaciones de antecedentes reforzadas antes de asumir funciones de EOI y/o a un mayor grado de autorización de seguridad (véase el RE 3.2.2, relativo a los controles de recursos humanos). El personal de TI que trabaja con bases de datos que incluyen información intercambiada también está sujeto a controles de recursos humanos reforzados.
- Se aplican CDPs estrictas a toda la información intercambiada en papel y los dispositivos móviles que la contienen, que deben almacenarse en cajones o armarios con cerradura.
- Las copias en papel de información intercambiada solo pueden imprimirse por personas autorizadas en la unidad de EOI, y deben etiquetarse con un sello de confidencialidad y de tratado.
- Las copias en papel de información intercambiada deben triturarse de forma segura cuando dejen de ser necesarias.
- Se aplican controles de dominio reforzados en bases de datos que contienen información intercambiada.
- El acceso a sistemas y bases de datos de EOI se restringe al personal expresamente autorizado sobre la base de la necesidad de saber (véase el RE 3.2.3, relativo a la gestión del acceso).
- Todas las solicitudes de información que se reciban y toda la información recibida se introducen en un sistema de gestión de TI interno al que solo puede acceder personal autorizado a través de un inicio de sesión y una contraseña individuales. Los accesos se registran y son monitoreados (véase el RE 3.2.6.2, relativo a la gestión de registros).

Transmisión segura de información a autoridades competentes extranjeras

La transmisión es el núcleo del EOI. Deben haber controles específicos cuando la información es enviada

a una autoridad competente extranjera o recibida de ella, ya sea previa petición, de manera automática o espontánea.[17] Los controles deben extenderse a todos los documentos conexos, comunicaciones e información contextual relacionados con el intercambio. Pueden considerarse los siguientes controles:

- En el caso de EOI previa petición, confirmar que el funcionario extranjero que ha solicitado la información es la autoridad competente o su representante autorizado bajo el instrumento internacional de intercambio de información aplicable, y que, por lo tanto, está autorizado para realizar la solicitud y recibir la información, y confirmar que su nombre y dirección/correo electrónico son correctos antes de enviar cualquier información.

- Transmisión segura entre autoridades competentes, por ejemplo:

  - La transmisión electrónica, ya sea previa petición o automática, debe protegerse siempre con un nivel adecuado de cifrado.

  - Solo las personas autorizadas para manejar información intercambiada pueden tener acceso al buzón de correo del EOI, protegido con contraseña.

  - Solo debe enviarse información por correo postal por medio de un sistema de registro internacional con seguimiento.

  - El correo recibido de una autoridad competente extranjera debe entregarse directamente en la unidad de EOI.

  - Las cartas de presentación a las autoridades competentes extranjeras deben hacer hincapié del carácter confidencial de la información, incluyendo una declaración relativa a las restricciones de divulgación y uso previstas en el tratado que sean aplicables (véase el ejemplo anterior).

Transmisión segura de información de AEOI procedente de instituciones financieras

La transmisión electrónica de información de instituciones financieras a las administraciones tributarias en el marco del Estándar AEOI debe estar debidamente cifrada.

Asimismo, deben aplicarse mecanismos de certificación y autenticación de las instituciones financieras. Esto suele lograrse a través de una autenticación multifactor y/o una firma digital.

Transmisión segura de información de la autoridad competente o la unidad de EOI a otras áreas dentro de la administración tributaria y partes externas

A menudo es necesario que la información intercambiada sea enviada por la autoridad competente o la unidad de EOI a otros funcionarios o autoridades de la administración tributaria, o a partes externas (p. ej. un fiscal). Debe llevarse un registro que indique a quién se ha divulgado la información, cuántas copias se han realizado y quién tiene en su poder una copia en cada momento.

En muchos casos, la autoridad competente o la unidad de EOI recibe grandes cantidades de información relativa a múltiples contribuyentes, y a menudo solo una parte de dicha información es necesaria para el inspector del cumplimiento de las obligaciones fiscales o un funcionario similar en una cierta región del país. La autoridad competente o el personal de la unidad de EOI son responsables de garantizar que solo se remita la información específica que necesitan esas personas concretas y que no se lleve a cabo una mera retransmisión de información masiva.

Como se ha analizado anteriormente, cuando una autoridad competente envía información a otra, normalmente se incluyen sellos de tratado y advertencias a fin de proteger la confidencialidad de dicha información. Las autoridades competentes que luego transmiten esa información dentro de la administración tributaria también puede incluir advertencias. Además de declarar que la información es confidencial y que ha sido obtenida con arreglo a un tratado fiscal, las advertencias pueden advertir de que la información no puede ser divulgada amparándose en leyes sobre libertad de información, ni tampoco sin consultarlo antes con la autoridad competente extranjera pertinente. Esta advertencia contribuye a garantizar que no se realicen divulgaciones no autorizadas.

Algunas jurisdicciones incluyen advertencias en la portada y otras las incluyen en todas las páginas de la información previendo que las páginas puedan separarse. Cuando el acuerdo de intercambio permita que la información sea usada con otros fines (no fiscales), los organismos encargados del cumplimiento de la ley y las autoridades judiciales que la reciban deben tratar la información como confidencial, conforme a lo dispuesto en el acuerdo (véase el RP 3.1).

17. Para obtener información adicional sobre políticas y prácticas que tengan por objeto proteger la confidencialidad de la información intercambiada, véase "Garantizando la confidencialidad: Guía de la OCDE sobre la Protección de la Información Objeto de Intercambio con Fines Fiscales", www.oecd.org/ctp/exchange-of-tax-information/informe-garantizando-la-confidencialidad.pdf

Recuadro 37. Ejemplo de controles para proteger la información intercambiada

En la administración tributaria de la Jurisdicción A, todo el personal que maneja información intercambiada cuenta con la debida habilitación de seguridad y está capacitado en materia de EOI. Los datos de EOI se clasifican como información "Confidencial". Los controles de seguridad son acordes a esta clasificación, y toda la información en formato físico o digital se etiqueta claramente como "protegida por el tratado".

Las solicitudes de EOI recibidas y enviadas son gestionadas por el Equipo de EOIR, mientras que los intercambios de información bajo el Estándar AEOI son gestionados por el Equipo de AEOI. El manual de EOI orienta a los funcionarios fiscales en la gestión de las solicitudes de EOI recibidas y enviadas, así como de la información de AEOI.

La información de EOIR recibida se segrega del resto de información relativa al contribuyente, y solo puede accederse a ella sobre la base de la necesidad de saber. La información recibida a través del sistema de AEOI se almacena en una ubicación separada del resto de bases de datos de contribuyentes a la que tienen acceso los administradores autorizados sobre la base de la necesidad de saber, mediante autenticación multifactor.

Además de las medidas de acceso físicas aplicadas, los documentos físicos, registros y medios de almacenamiento (como CDs y memorias USB) recibidos de los socios de intercambio se conservan de forma segura en armarios fijos con varias cerraduras dentro de las oficinas del Equipo de EOIR/AEOI.

En todos los casos se cifra la información enviada de forma electrónica a los socios de intercambio.

Respecto de las solicitudes de EOI recibidas de socios de intercambio, solo se divulga y remite a las oficinas de las administraciones tributarias locales la mínima información de la carta de solicitud de EOI, a efectos de que los inspectores fiscales locales puedan obtener la información solicitada del titular de la información. Los inspectores fiscales locales deben confirmar por escrito que se mantendrá la confidencialidad de los datos y que solo se usarán de conformidad con el acuerdo internacional de intercambio de información aplicable. Los inspectores fiscales locales también reciben capacitación relativa al uso del manual de EOI y los procedimientos aplicables al tratamiento de la información intercambiada.

Cuando la información se remite a oficinas de la administración tributaria local se incluye la siguiente advertencia: "Toda la información recibida con arreglo a las disposiciones sobre intercambio de información de un tratado podrá utilizarse únicamente con fines fiscales, a menos que se autorice expresamente su uso con otros fines, y deberá mantenerse en la más estricta confidencialidad. La divulgación de estos documentos, incluida la que se realice con arreglo a la Ley de Privacidad o la Ley de Libertad de Información, debe consultarse al equipo de EOIR antes de ser divulgada. La Sección 1 del manual de EOI ofrece orientación adicional sobre esta materia".

La información intercambiada se archiva durante 10 años cuando deja de ser necesaria para el desempeño de la actividad, y una vez transcurrido dicho período se destruirá. Un empleado designado de la administración tributaria debe presenciar todo el proceso de destrucción.

El Recuadro 37 ilustra con ejemplos los controles (reforzados) que pueden aplicarse a la información intercambiada.

REQUISITO ESPECÍFICO 3.2.6: MARCO DE GESTIÓN DE LAS OPERACIONES, INCLUIDA LA GESTIÓN DE INCIDENCIAS, LA GESTIÓN DEL CAMBIO, SEGUIMIENTO Y AUDITORÍA

El RE 3.2.6 analiza la fase "check" del ciclo de vida PDCA. En otras palabras, se centra en los acuerdos operativos que las administraciones tributarias utilizan para verificar que el sistema GSI y sus controles están funcionando.

Si bien, en términos generales, las operaciones de seguridad pueden ser muy variadas, los análisis de confidencialidad del AEOI subrayan y se centran en algunas de las capacidades, procesos y controles críticos que deberían aplicar las administraciones tributarias, especialmente en el ámbito de las TI. Estos controles operativos comprenden los siguientes ámbitos, empezando con una descripción general del marco de gestión de las operaciones que las administraciones tributarias deberían tener y continuando con los controles aplicables en seis ámbitos de la gestión operativa:

- RE 3.2.6.1: Marco de gestión de operaciones general.
- RE 3.2.6.2: Gestión de registros.
- RE 3.2.6.3: Gestión del riesgo de TI.
- RE 3.2.6.4: Gestión de las vulnerabilidades.
- RE 3.2.6.5: Gestión del cambio.
- RE 3.2.6.6: Gestión de incidentes.
- RE 3.2.6.7: Auditoría interna y externa.

La Tabla 24 contiene las definiciones de los principales conceptos comprendidos en el RE 3.2.6.

RE 3.2.6.1. Visión general del marco de gestión de las operaciones de seguridad

La coordinación eficaz de las actividades de seguridad de las operaciones es un facilitador importante de los procesos estratégicos fundamentales en materia de seguridad, tales como el sistema GSI y la gestión corporativa de riesgos. Es fundamental para una administración tributaria tener visibilidad de los mensajes que transmiten los procesos operativos desde su funcionamiento cotidiano, incluyendo en relación con los controles de seguridad (incluidos aquellos que protegen la información intercambiada). Por lo tanto, el

Tabla 24. **Glosario de los principales conceptos**

Concepto	Descripción
Función de auditoría	Revisiones exhaustivas e imparciales para evaluar el cumplimiento de los procesos de sistemas de GSI establecidos en las políticas y procedimientos. Las conclusiones y resultados de la auditoría deben comunicarse directamente al jefe de la administración tributaria.
Gestión del cambio	Se refiere a la gestión controlada del desarrollo de nuevos sistemas y servicios, así como la realización de cambios importantes sobre los ya existentes.
Gestión de incidentes	Implica la identificación, documentación y gestión de incidentes de seguridad, tanto en ámbitos de informáticos como no informáticos.
Registro	Un registro, en un contexto informático, es la documentación automática y con indicación del momento en que se producen, de los eventos relevantes para un sistema informático concreto. También pueden llevarse registros manuales para actividades no informáticas.
Gestión de registros	Se refiere a los procesos y políticas colectivos que se utilizan para administrar y facilitar la generación, transmisión, análisis, almacenamiento, archivo y eliminación final de grandes cantidades de datos del registro generados en un sistema de TI.
Actividad de registro	La actividad de registro se refiere al registro y seguimiento por las administraciones tributarias de todo acceso a datos protegidos, incluido el acceso a instalaciones y áreas en las que se conservan los datos, y en particular a sistemas que contienen registros y otra información sensible de los contribuyentes.
Centro de Operaciones de Seguridad	Un Centro de Operaciones de Seguridad es un equipo de profesionales y sistemas especializados para el monitoreo y análisis continuo de la situación de seguridad de la administración tributaria.
Gestión de vulnerabilidades	Se refiere a los procesos y procedimientos de identificación y gestión de vulnerabilidades.

RE 3.2.6.1 requiere que las administraciones tributarias conozcan los controles que permiten proteger la información objeto de intercambio y dispongan de una planificación adecuada para gestionarlos.

Por "Marco de gestión de las operaciones de seguridad" se entiende un conjunto de prácticas operativas interconectadas que ayudan a mantener la posición de seguridad continua de la administración tributaria. Está formado por acuerdos operativos en materia de monitoreo, mantenimiento y gestión de los aspectos de seguridad del parque informático, su personal y sus procesos.

La escala del enfoque de gestión de las operaciones de seguridad dependerá del tamaño de la administración tributaria y de la complejidad de sus operaciones, por ejemplo:

- Las administraciones tributarias más grandes, con operaciones variadas y complejas, pueden disponer de funciones individuales de gestión de las operaciones (registro, riesgos de seguridad, gestión de vulnerabilidades, gestión del cambio, gestión de incidentes y auditoría) distribuidas entre sistemas de TI, servicios de negocio o equipos de apoyo, con una unidad centralizada encargada de la gestión de las amenazas para las operaciones.
- Las administraciones tributarias más pequeñas pueden carecer de la complejidad necesaria para justificar una planificación centralizada, y pueden ser los directores de operaciones quienes se responsabilicen de cada una de las funciones individuales de gestión de las operaciones.

Con independencia del tamaño de la administración tributaria, lo importante es que las actividades de gestión operativa deben planificarse y coordinarse entre las distintas áreas de manera eficaz.

Por lo tanto, debe adoptarse un enfoque global de gestión de las operaciones de seguridad, que se refleje de forma clara y se documente en el conjunto de políticas específicas a un ámbito (tal y como se describe en el RE 3.2.1) en el que se configura el contexto más amplio del marco GSI.

Las políticas específicas a un ámbito deben incluir acuerdos de reporte en virtud de los cuales los directores de operaciones presenten informes periódicos al OSI o alerten con respecto al rendimiento de los controles de seguridad en un determinado ámbito, con el fin de garantizar que se lleven a cabo actividades periódicas según sea necesario para mitigar eficazmente los riesgos (estos últimos deben reflejarse continuamente en un registro de riesgos, tal como se describe en el RE 3.2.1.4).

En la práctica, el enfoque de gestión de las operaciones suele estar centralizado en un Centro de Operaciones de Seguridad (COS). Un COS está formado por un equipo de profesionales especializados y sistemas adecuados para monitorear y analizar de manera continua la posición de seguridad de la organización. El objetivo del equipo del COS es detectar, analizar y responder a los incidentes de seguridad, mediante una combinación de soluciones tecnológicas y actividades de respuesta ante incidentes.

Las siguientes secciones describen las funciones esenciales de la gestión de las operaciones en cada una de las seis áreas pertinentes.

RE 3.2.6.2. Gestión de registros

La actividad de registro se refiere al registro y seguimiento por las administraciones tributarias de todo acceso a datos protegidos, incluido el acceso a instalaciones y áreas en las que se conservan los datos, y en particular a sistemas que contienen registros de los contribuyentes y otra información sensible. La gestión de registros se refiere a los procesos y políticas colectivos que se utilizan para administrar y facilitar la generación, transmisión, análisis, almacenamiento, archivo y eliminación final de grandes cantidades de datos del registro generados en un sistema de TI.

Las administraciones tributarias deben garantizar que el acceso se registre, monitoree y retenga de forma completa durante el tiempo suficiente para cumplir requisitos de control tales como el monitoreo de las operaciones, la gestión de incidentes y la auditoría.[18]

El registro cumple al menos dos fines: monitorear la eficacia de los controles y suministrar evidencia en caso de que ocurran incidentes.

Por lo tanto, el RE 3.2.6.2 requiere que las administraciones tributarias apliquen medidas adecuadas de registro y monitoreo, incluyendo la detección del acceso, uso o divulgación de información sin autorización.

Las administraciones tributarias deben, en particular, determinar una estrategia de registro y monitoreo de la información intercambiada, que o bien podría seguir el marco general de registro o bien formar parte de una estrategia de registro y monitoreo específico.

Las administraciones tributarias deben:

- **Llevar registros**. La llevanza de registros es una herramienta proactiva muy importante que permite consultar los registros en caso de actividad maliciosa o acceso ilícito, y que permite que las malas prácticas sean rastreadas hasta la(s) persona(s) responsable(s). Si se registran y conservan debidamente, los registros pueden utilizarse como evidencia en procedimientos sancionadores, ya sean de carácter administrativo o penal.

- **Monitorear registros**. El monitoreo de registros permite identificar y adoptar medidas adecuadas con respecto a actividades sospechosas antes de que se produzca un incidente grave. Por ejemplo, es posible que el monitoreo identifique actividades que, si bien no constituyen un incidente, podrían ser no obstante un motivo de preocupación, tales como solicitudes frecuentes de restauración de contraseñas. Esta actividad, en sí misma, no implica un incumplimiento de la política, pero podría ser una señal de que los empleados no están debidamente concienciados con respecto a las buenas prácticas de gestión de contraseñas y están generando contraseñas que no pueden recordar, o que las guías del departamento de TI relativas a cómo deben estructurarse las contraseñas para cumplir las exigencias relativas a su complejidad no son claras.

- **Proteger y almacenar registros**. Los registros en sí mismos son un activo de información importante que debe ser protegido y almacenado de conformidad con los requisitos legales y de seguridad. Los requisitos legales pueden incluir períodos de retención de los registros, que deben definirse y documentarse. Si no está definido en la ley, el período de conservación recomendado debe coincidir con el período de revisión de los registros y no ser inferior a 3 meses. Las administraciones tributarias deben ser capaces de recuperar los registros e interpretarlos cuando sea necesario, y esta capacidad debe revisarse periódicamente. Los requisitos de seguridad pueden incluir la aplicación de controles de acceso a los registros, la revisión de los derechos de acceso, la inclusión de registros en las copias de seguridad, la función hash para el control de la integridad, la destrucción de registros, etc.[19]

Las administraciones tributarias también deben identificar con claridad qué actividades deben registrarse, así como establecer procedimientos de monitoreo de los registros y gestión de las evidencias.

¿Qué actividades deben registrarse?

Sobre la base de una evaluación de los riesgos de seguridad de la información (véase el RE 3.2.1.4, relativo

18. El registro y el monitoreo también se analizan como control básico de TI en el RE 3.2.4.2, relativo a los controles de seguridad de TI.

19. La destrucción de registros debe seguir un procedimiento predeterminado que garantice una destrucción o eliminación seguras, tal y como se describe en el RE 3.2.5, relativo a la protección de la información.

a la gestión del riesgo), un OSI, en coordinación con el jefe del departamento de TI, debe identificar:

- Qué actividades deben registrarse.
- La frecuencia con que deben revisarse los registros.
- Los parámetros de monitoreo de los registros, para que se envíen alertas en caso de sospecha de incidente.

El registro y monitoreo de los registros puede cubrir tanto actividades relacionadas como no relacionadas con las tecnologías de la información, tales como:

- **Tráfico de internet**. El monitoreo del origen de las direcciones IP, en particular de las direcciones IP que se enlacen y las de origen extranjero, ofrece una información especialmente importante en el contexto de la administración tributaria, donde se espera que la inmensa mayoría de conexiones sean nacionales y/o estén encuadradas en determinadas categorías.
- **Software de prevención de malware**. El monitoreo de los registros del software antivirus puede permitir identificar si algún virus está infectando de manera reiterada un sistema y puede indicar la necesidad de bloquear el origen de procedencia. En cambio, si de los registros se infiere que se están bloqueando pocos virus, esto podría significar que el software no está actualizado con la última lista de definiciones de virus.
- **Firewall**. El monitoreo del tráfico de datos que salen de la administración tributaria permite identificar flujos no previstos que deben ser revisados, p. ej. para determinar si la salida de información a una empresa privada o un periódico es legítima.
- **Gestión del acceso**. El monitoreo de accesos usando los registros de dominio deben buscar accesos autorizados y no autorizados. Puede centrarse especialmente en el acceso desde dispositivos no registrados o imprevistos (p. ej. usuarios autorizados desde un dispositivo privado) o múltiples intentos de acceso no autorizado (p. ej. que sugieran un ataque de penetración o un ataque de denegación de servicio).
- **Bases de datos**. El monitoreo de los registros de bases de datos permite detectar cambios imprevistos o no autorizados en los datos, el acceso a bases de datos sensibles por parte de usuarios autorizados y/o los intentos de acceso por parte de usuarios no autorizados.
- **Acceso físico**. El monitoreo con cámaras de CCTV y otros controles de acceso electrónico, así como accesos a documentos confidenciales en papel o instalaciones de acceso restringido (p. ej. una unidad de EOI), permiten detectar intrusiones. Los registros de este tipo pueden llevarse de forma manual, aplicando menos procesos automatizados, pero sin embargo deben someterse a los mismos procedimientos de revisión, seguimiento y almacenamiento que los registros automatizados.
- **Cumplimiento de los controles de seguridad en el entorno de oficina**. Registro de la certificación de los extintores, reparto de llaves, etc.

Monitoreo del registro y gestión de evidencias

Las administraciones tributarias deben monitorear los registros periódicamente. El monitoreo puede ser pasivo, de modo que solo se lleve a cabo cuando ocurra un evento o incidente, o bien activo, esto es, una monitoreo sistemático o monitoreo de registros en tiempo real, empleando sistemas de gestión de registros.

En particular, el monitoreo activo puede aplicarse en distintos grados:

- **Alertas**. Pueden fijarse parámetros para que, si ocurre un determinado evento, pueda ser identificado en el momento en que se produce, investigado y, si es necesario, resuelto de manera inmediata. Algunos de estos eventos pueden incluir un aumento inesperado del tráfico de internet, un tipo de tráfico imprevisto o una exfiltración de grandes cantidades de datos. Algunas herramientas como la protección frente a la filtración de datos pueden emplearse para emitir alertas.
- **Monitoreo general**. Un ejemplo ilustrativo es la supervisión en tiempo real de las cámaras de CCTV para detectar infracciones de seguridad. El monitoreo general podría incluir igualmente el simple monitoreo del tráfico de internet con el fin de detectar eventos imprevistos para los que no se ha configurado una alerta.
- **Listas de tareas**. Se establecen criterios para los eventos que requieren revisión, y cuando estos ocurren se añade una notificación a una lista de tareas para que el evento se revise dentro del horario laboral normal, cuando sea posible dentro del mismo día hábil en que tenga lugar dicho evento. Esta forma de monitoreo se aplica a eventos que requieren una actuación o control, pero que no son críticos, por ejemplo porque solo afectan a un único registro. Este tipo de monitoreo activo podría describirse mejor como “casi en tiempo real” y es relativamente más parecido a la categoría de monitoreo pasivo.

Una organización haría normalmente una selección de métodos de monitoreo pasivo y/o activo en atención a varios factores como:

- Los riesgos evaluados.
- Las exigencias de seguridad y del negocio.
- El monitoreo de las competencias del personal.
- La capacidad de almacenamiento de registros.
- La cantidad de registros y las dinámicas que los generan, pues podrían tener implicaciones presupuestarias.

Las administraciones tributarias deben tener también en cuenta las siguientes prácticas de monitoreo de registros y gestión de evidencias:

- **Definición de parámetros de reporte entre lo que se considera un evento que requiere un reporte urgente o prioritario y eventos no urgentes que no requieren de priorización**. Por ejemplo, podrían establecerse alertas únicamente para grupos de registros sensibles (p. ej. registros de acceso a bases de datos del CRS) que en caso de fallo producirían consecuencias más graves. Las alertas activadas por el sistema de control de accesos podrían asociarse al procedimiento de gestión de incidentes previsto en el RE 3.2.6.6.
- **Aplicación de controles para proteger la integridad de los registros cuando se utilicen y analicen**. Esta práctica incluye la aplicación de la función hash para garantizar la integridad de los registros, la copia de seguridad periódica de registros y la imposición de un control estricto de los accesos en relación con las personas que pueden ver o administrar los registros.
- **Revisión de controles de monitoreo**. Las revisiones deben llevarse a cabo de manera periódica para que puedan ajustarse los criterios de alerta.
- **Definición clara de los roles y funciones de las personas relevantes en relación con los registros**. Incluye a las personas responsables de las actividades de monitoreo de registros, revisión del acceso a archivos de registro y los derechos de acceso, y la determinación de controles para proteger la integridad de los archivos de registro. Entre estos responsables pueden incluirse el OSI, funcionarios de TI, el COS o un proveedor externo cuando proceda. La organización debe documentar en qué circunstancias se autoriza a ciertas personas el uso y el análisis de los registros, p. ej. el OSI para el análisis de incidentes o para la medición de la eficacia de los controles de seguridad implementados, o el departamento de cumplimiento o auditoría interna para la investigación de un incidente reportado de uso indebido de información.
- **Definición de políticas o prácticas para la retención de registros y la gestión de evidencias**. Esta práctica posibilita el mantenimiento de la "cadena de custodia" de datos o documentos afectados, de manera que se puedan llevar a cabo las debidas investigaciones con arreglo a procedimientos disciplinarios internos o por parte de las autoridades encargadas de hacer cumplir la ley. Dichas políticas o prácticas incluirán políticas de gestión de registros con controles para la retención, la integridad y el acceso, así como procedimientos detallados para mantener y proteger evidencias mediante el uso de copias, cifrado y copias de seguridad.

El registro y el monitoreo pueden ampliarse y gestionarse a través de herramientas tales como los sistemas SIEM, si con ello la administración tributaria puede obtener un beneficio sobre costes adecuado. Véase el Recuadro 38 para un ejemplo de registro y monitoreo dentro de una administración tributaria.

Recuadro 38. Ejemplo de registro y monitoreo

Todos los sistemas de la administración tributaria de la Jurisdicción A registran todos los accesos a datos (intentos fallidos o exitosos). Un sistema de registro centralizado recoge y registra todas las actividades. El acceso a los registros también se registra. Existen medidas de protección especiales para mantener la integridad de los registros e impedir cambios no autorizados en los archivos de registro. Los registros se conservan durante 18 meses.

El monitoreo de registros y su frecuencia se basan en el sistema de clasificación de datos de la organización. Los registros de sistemas que contienen datos clasificados como sensibles o confidenciales y a los que pueden acceder usuarios con derechos de administrador como, por ejemplo, los sistemas de AEOI, son monitoreados a través de un sistema especializado de monitoreo en tiempo real que emite alertas cuando se detecta una actividad sospechosa. También se aplica un enfoque más pasivo para revisar registros de sistemas no sensibles y cuentas no privilegiadas, que se revisan de acuerdo con calendarios predeterminados o cuando es necesario.

El OSI revisa de forma periódica los registros de los distintos sistemas para comprobar la eficacia de los controles establecidos con respecto a ese sistema. El OSI, en colaboración con el funcionario responsable de la gestión de incidentes, revisa también los registros como parte de la estrategia de respuesta ante incidentes y análisis de incidentes, con el fin de comprender no solo el impacto y la causa del incidente en cuestión, sino también el problema subyacente que genera el riesgo.

RE 3.2.6.3. Gestión operativa de riesgos de seguridad de TI

La gestión operativa de los riesgos de seguridad de TI es una actividad clave en el entorno de una administración tributaria, pues las amenazas para las tecnologías de la información pueden causar un impacto profundo y de gran alcance cuando afectan a bases de datos que contienen información sensible.

El enfoque de una administración tributaria para la gestión de riesgos de seguridad informática debe ser compatible con el proceso general de gestión de riesgos utilizado conforme se indica en el RE 3.2.1.4, es decir, con la metodología de gestión de riesgos global, aplicable tanto a las actividades informáticas como las no informáticas.

Las administraciones tributarias deben tener en cuenta los siguientes aspectos específicos (véase el Recuadro 39 para un ejemplo de gestión de los riesgos de seguridad de TI):

- **La participación del departamento de TI en el proceso de gestión de riesgos global**. Es fundamental que el departamento de TI esté plenamente involucrado en los procesos de gestión del riesgo de la administración tributaria, puesto que la mayoría, si no la totalidad, de los riesgos del negocio significativos tendrá una dimensión informática. Esto es particularmente importante para la identificación de los controles más adecuados, así como para la evaluación del impacto o la eficacia de dichos controles en reducir efectivamente los riesgos identificados. Idealmente, el registro de riesgos de TI debería estar integrado con el registro de riesgos del negocio. Dicha integración podría aumentar la visibilidad de los riesgos de TI dentro del panorama general de riesgos, así como la comprensión del impacto que producirían los cambios en el riesgo del negocio sobre los controles de TI y de seguridad.

- **Las consecuencias informáticas de las decisiones de gestión del negocio**. Debido al aumento de la dependencia de las tecnologías de la información en todos los aspectos de las operaciones de las administraciones tributarias, la mayoría de las decisiones del negocio tienen implicaciones informáticas, es decir, requieren algún cambio o modificación de un sistema de TI existente. Dichas implicaciones deben analizarse y considerarse detenidamente en relación con la seguridad de los datos. Las decisiones del negocio relativas a la financiación del departamento de TI también pueden tener un impacto significativo sobre la seguridad, pues la seguridad se basa en controles cuya gestión operativa depende del departamento de TI.

- **Las consecuencias sobre el riesgo de las decisiones informáticas**. Durante el diseño, desarrollo e implementación de las nuevas aplicaciones e infraestructura de TI, o durante las mejoras periódicas del sistema informático, el personal de TI debe tener siempre en cuenta los cambios en el entorno de riesgo global que dichos desarrollos o modificaciones podrían provocar, y debe reflejar debidamente sus conclusiones en el registro de riesgos.

- **Monitoreo periódico de riesgos informáticos y revisión de controles de seguridad informáticos**. Como el entorno informático se encuentra en constante cambio, continuamente surgen nuevos riesgos, amenazas y vulnerabilidades que son identificados por los profesionales informáticos. Por tanto, el personal de TI debe llevar a cabo un monitoreo diario de los cambios y una revisión periódica de los riesgos de TI que plantean, así como de la validez de los controles aplicados (véase también el RE 3.2.6.4, relativo a la gestión de las vulnerabilidades).

Recuadro 39. Ejemplo de gestión de riesgos de seguridad de TI

La gestión del riesgo de seguridad de TI en la administración tributaria de la Jurisdicción B es llevada a cabo por un equipo de evaluación de riesgos integrado por el OSI y por representantes del departamento de TI y las áreas del negocio. Los miembros del equipo, bajo el liderazgo del OSI, identifican conjuntamente los riesgos de seguridad informática y evalúan su probabilidad de ocurrencia y posible impacto. Los criterios de aceptación del riesgo son predefinidos por la alta dirección con el asesoramiento del OSI, y se incorporan a la evaluación de riesgos que realiza el equipo. Todos los riesgos fuera de los riesgos aceptables deben abordarse con controles.

El departamento de TI proporciona los insumos técnicos y propone controles para mitigar los riesgos identificados, mientras que el OSI se asegura de que los controles sean coherentes con las políticas y procedimientos de seguridad de la información. Los representantes de las áreas del negocio proporcionan insumos para garantizar que los controles no afecten el rendimiento global de los procesos del negocio.

La evaluación de los riesgos y los controles seleccionados se registran en un registro de riesgos. El equipo revisa periódicamente la evaluación, y un gerente de TI debe realizar un seguimiento de la implementación de los controles de mitigación del riesgo de TI y su eficacia.

- **El enfoque relativo a proveedores externos de servicios de tecnologías de la información**. Cuando las tecnologías de la información se gestionan desde fuera de la administración tributaria, los acuerdos y SLA adecuados deben regular las relaciones con proveedores externos y la prestación por parte de estos de los servicios de tecnologías de la información, especificando cómo deben gestionarse y comunicarse los riesgos derivados de la prestación de dichos servicios. Esos riesgos deben integrarse en la propia gestión de riesgos de la administración tributaria.

RE 3.2.6.4. Gestión de vulnerabilidades

El RE 3.2.6.4 requiere que las administraciones tributarias tengan procesos y procedimientos para la identificación y gestión de vulnerabilidades. Por gestión de vulnerabilidades se entiende la exploración periódica del entorno informático de la organización con el fin de identificar vulnerabilidades que pueden plantear un riesgo de seguridad significativo. Deben desplegarse controles de TI adecuados para gestionar las vulnerabilidades identificadas (véase el análisis del RE 3.2.4.2).

Tanto la frecuencia como el alcance de la exploración de vulnerabilidades dependerán de la complejidad y escala de las operaciones de TI de una administración tributaria, sus riesgos identificados y el presupuesto disponible. Con independencia de la frecuencia y alcance, el análisis de vulnerabilidades debe ser exhaustivo para hacer posible la determinación de las políticas o controles del sistema GSI que necesitan mejoras. Aunque existen varias herramientas disponibles para identificar vulnerabilidades, el RE 3.2.6.4 se centra en la exploración de vulnerabilidades y las pruebas de penetración de los entornos informáticos.

Exploración de vulnerabilidades

La exploración de vulnerabilidades se refiere a la identificación de defectos de diseño en sistemas de TI que son propensos a ser explotados por algún agente interno o externo que presente una amenaza. Una herramienta de exploración comprueba automáticamente la existencia de posibles puntos de entrada por los que pueden entrar piratas informáticos a programas, servicios o puertos, así como defectos en la construcción de la infraestructura informática.

Existen varios tipos de herramientas de exploración de vulnerabilidades, en función del alcance y la intensidad de la exploración deseados. Entre esas herramientas pueden incluirse:

- **Exploración de vulnerabilidades de red**: la revisión de todos los sistemas de red y ordenadores para detectar vacíos de seguridad.
- **Exploraciones no autenticadas y autenticadas**: la exploración de sistemas en busca de vulnerabilidades puede realizarse simulando un pirata informático externo sin credenciales de usuario (exploración no autenticada) o con credenciales de usuario (exploración autenticada), tratándose en este último caso de un pirata informático que ya tiene acceso como usuario al sistema.

El informe de exploración de vulnerabilidades debe analizarse de manera inmediata y las vulnerabilidades identificadas debe resolverse con controles adecuados.

Pruebas de penetración

Las pruebas de penetración, también conocidas como "*hacking* ético", son un tipo particular de prueba de vulnerabilidades que comprueba el posible alcance e intensidad del acceso por parte de un usuario no autorizado en un momento dado. Se espera que todas las administraciones tributarias, con independencia de su tamaño, sometan a pruebas periódicas de penetración tanto las interfaces externas como las internas. Las interfaces que tratan datos de AEOI deben someterse periódicamente a pruebas de penetración.

Para que las pruebas de penetración sean eficaces, las administraciones tributarias deben tener en cuenta los siguientes aspectos:

- **Pruebas de penetración de interfaces tanto internas como externas.**
  - **Interfaces externas**. La prueba de penetración se centra en las conexiones entre el mundo exterior y el sistema de TI de la administración tributaria.
  - **Interfaces internas**. La prueba de penetración se centra en las conexiones internas dentro de la plataforma o el sistema de TI de la administración tributaria para asegurar que los principios de "necesidad de saber" y "mínimo privilegio" son adecuadamente implementados.
- **Prueba de penetración periódica**. Una prueba de penetración comprueba los sistemas en el momento dado en que se realiza la prueba. Por tanto, las pruebas de penetración son más útiles cuando prueban sistemas nuevos o cambios importantes en los sistemas, tanto antes como inmediatamente después de su puesta en funcionamiento. Las interfaces críticas deben someterse a pruebas de penetración periódicas, como mínimo una vez al año o incluso con mayor frecuencia en función de su importancia.

- **Contratación de terceros independientes y de prestigio para la realización de las pruebas de penetración**. Lo ideal sería que las pruebas de penetración sean llevadas a cabo por un tercero proveedor de pruebas de penetración independiente de la administración tributaria. Es importante contratar a proveedores de pruebas de penetración de prestigio con experiencia acreditada y dominio de las técnicas más recientes. Se recomienda la contratación de *hackers* éticos certificados.

- **Fijación de requisitos claros con el encargado de las pruebas de penetración**. El éxito de las pruebas de penetración depende en gran medida de la calidad de la relación con el encargado de realizar dichas pruebas. Las administraciones tributarias deben celebrar siempre un contrato con el encargado de las pruebas de penetración antes de la realización de dichas pruebas, y establecer un acuerdo de no divulgación con respecto a la información que el encargado de las pruebas pueda llegar a ver, en el que éste se comprometa a no hacer un uso indebido de dicha información. El contrato debe incluir restricciones predeterminadas dentro de las cuales trabajará el encargado de las pruebas, tales como el tipo de equipos que debe utilizar y qué información relativa al sistema que se somete a prueba va a recibir. En función de los parámetros definidos, las pruebas pueden ser de "*black box*" (no se da información sobre el sistema salvo la dirección del sitio web) o de "*white box*" (se ponen en conocimiento del encargado de las pruebas la infraestructura y la configuración del sistema). Los requerimientos de la prueba deben discutirse abiertamente con el encargado de la prueba de penetración, para que pueda conocer el contexto de la actividad en el que opera la administración tributaria y hacer recomendaciones. Debido a su experiencia, los encargados de las pruebas de penetración pueden tener una mejor idea del panorama actual de las amenazas y podrán sugerir alternativas en relación con el enfoque y el alcance de la prueba.

Véase el Recuadro 40 para ver un ejemplo de controles de gestión de las vulnerabilidades.

Recuadro 40. **Ejemplo de controles de gestión de vulnerabilidades**

La administración tributaria de la Jurisdicción C explora todos los sistemas, aplicaciones y bases de datos con el fin de detectar posibles vulnerabilidades que puede explotar un potencial atacante, y aplica los debidos controles. Todo el tráfico entre la web, las aplicaciones y las bases de datos se vigila 24 horas al día y 7 días a la semana mediante firewalls físicos y sistemas especializados que ofrecen actualizaciones en tiempo real frente a posibles ataques, permitiendo que puedan detectarse y abordarse de manera oportuna.

La administración tributaria también contrata a empresas de seguridad especializadas para que realicen hacking ético en interfaces internas y externas. Los sistemas de AEOI se someten a pruebas de penetración todos los años. Todas las aplicaciones nuevas tienen que someterse a una prueba de penetración en la web antes de ponerse en marcha, y todos los fallos y vulnerabilidades deben solucionarse antes de la puesta en marcha.

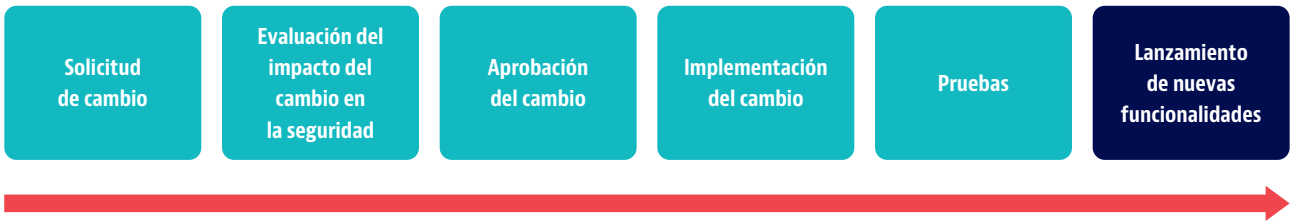
RE 3.2.6.5. Gestión del cambio

La gestión del cambio se refiere a la gestión controlada del desarrollo de nuevos sistemas y servicios, así como la realización de cambios importantes sobre los ya existentes. Comprende el diseño de soluciones sólidas, las pruebas y el control de lanzamientos, y es el medio por el cual se garantiza que la seguridad informática se incorpora a los cambios en los sistemas.

El RE 3.2.6.5 requiere que las administraciones tributarias tengan un proceso de gestión del cambio en el que se integre la seguridad. El proceso puede documentarse en una política o un procedimiento en función del nivel de detalle que se precise y debe ser revisado por el OSI de forma periódica.

Desde una perspectiva de la seguridad, el proceso de gestión del cambio es de por sí una actividad de alto riesgo. Los cambios en los sistemas sin una estrategia adecuada de seguridad de TI podrían resultar

FIGURA 18. **Etapas de la gestión del cambio**



en sistemas vulnerables y provocar importantes infracciones de seguridad. Esto puede incluir cambios apresurados debidos a restricciones de presupuesto y tiempo y sin disciplina de proyecto, pruebas inadecuadas y con advertencias ignoradas.

Por lo tanto, el departamento de TI, los responsables de los sistemas del negocio y usuarios y el OSI deben desarrollar y aplicar de forma conjunta un enfoque sólido de gestión del cambio. Dicho enfoque debe incluir la secuencia de pasos claves representada en la Figura 18.

- **Solicitud de cambio**. Todas las solicitudes de cambios deben documentarse indicando el beneficio que se espera obtener con el cambio, los sistemas o procesos involucrados, el o los problemas que resuelve (si se basa en algún incidente o vulnerabilidad conocidos), la urgencia y los plazos, y el nivel de prioridad y de importancia para los procesos del negocio.
  Las administraciones tributarias deben definir con claridad los tipos de cambios que pueden solicitarse, y los criterios aplicables a cada uno de ellos. Los dos tipos principales son:
  - **Cambios regulares**. Estos son cambios que pueden planificarse, priorizarse, aprobarse, probarse y lanzarse. A su vez, pueden dividirse entre cambios importantes y cambios menores, cuando proceda.
  - **Cambios de emergencia**. Estos son cambios que deben implementarse inmediatamente para resolver alguna deficiencia crítica, en caso de que los retrasos en su aplicación puedan agravar el daño. Se omiten las fases comunes del proceso de cambio y se ejecutan después de la implementación del cambio. A menudo, los cambios de emergencia se producen como consecuencia de un incidente. El proceso de gestión de incidentes se describe en la siguiente sección, el RE 3.2.6.6.
- **Evaluación del impacto en la seguridad**. Debe llevarse a cabo una evaluación de las distintas implicaciones del cambio en el proceso del negocio, las tecnologías de la información y la seguridad por parte del personal involucrado en cada uno de estos aspectos. Debe existir un equilibrio entre la funcionalidad que el negocio necesita, los controles de mitigación del riesgo que recomienda el OSI y los adelantos tecnológicos o las limitaciones que plantea el sistema.
- **Aprobación del cambio**. Normalmente asignada al OSI o la alta dirección, la responsabilidad de la aprobación de los cambios puede ser definida como parte de las funciones y responsabilidades en la política GSI (véase el RE 3.2.1.2).
- **Implementación del cambio**. Durante la implementación, los equipos involucrados deben asegurarse de que se cumplen los requisitos de seguridad antes del lanzamiento. Por ejemplo, si se realizan cambios en el código fuente del software, la integridad del código fuente se gestionará usando herramientas de versionado de código. Si el cambio implica procesos o procedimientos, debe ajustarse a la política global de GSI y otras políticas relevantes.
- **Pruebas**. La verificación de los cambios es crítica, especialmente cuando se implementan en sistemas de TI. Siempre que sea posible, las pruebas no deben realizarse directamente en el entorno de producción. En caso de cambios en el software, las pruebas deben realizarse en un entorno aislado con datos ficticios o *dummy*. Esto hace posible que puedan producirse errores sin riesgo alguno para los datos reales y/o para el funcionamiento real de los procesos. La política debe contemplar guías claras sobre el uso de datos para realizar pruebas, así como sobre los criterios para lanzar los cambios.
- **Lanzamiento de nuevas funcionalidades (lanzamiento de cambios)**. Siempre que sea posible, el lanzamiento de un cambio debe ser una actividad planificada. Esto significa que el lanzamiento de nuevas funcionalidades debe realizarse durante períodos en los que la interrupción de las operaciones de negocio normales de la administración tributaria se reduzca al mínimo. Es buena práctica lanzar los cambios contando con un plan de reversión ya preparado, esto es, un plan sobre cómo revertir o restaurar el modo de funcionamiento anterior en caso de que el lanzamiento a producción de los cambios no sea exitoso.

Recuadro 41. **Ejemplo de gestión del cambio**

La administración tributaria de la Jurisdicción A dispone de guías detalladas en materia de gestión del cambio y revisión de código. Las guías tienen en cuenta los requerimientos de los usuarios de los procesos del negocio y el departamento de TI, incluida la seguridad de la información.

Todos los cambios, incluido el código fuente, deben someterse previamente a pruebas por parte de los desarrolladores en un entorno de desarrollo. Los directivos del área de TI realizarán a continuación nuevas pruebas en un entorno de prueba al que no tendrán acceso los desarrolladores. La versión puede ponerse en producción únicamente después de que se hayan realizado estas dos pruebas.

Todos los códigos fuente se almacenan de forma segura en un archivo seguro con acceso privilegiado concedido a personas sobre la base de la necesidad de saber.

Los cambios mal ejecutados son una causa frecuente de incidentes, incluidos los incidentes de seguridad. Por lo tanto, se necesita una gestión adecuada. Esto puede lograrse en parte teniendo una entidad que autorice formalmente el lanzamiento del cambio, p. ej. el OSI o, en organizaciones más complejas, un Comité de Control de Cambios u otro órgano equivalente que incluya a los representantes de las distintas áreas operativas, incluida la seguridad. Dicha entidad elaborará por lo común un calendario de cambios estimados que será circulado a todos los actores relevantes de forma periódica, para proporcionar visibilidad de los cambios previstos y contribuir a evitar que se interrumpan las actividades del negocio.

La estrategia de gestión del cambio debe ser revisada periódicamente por un OSI con el fin de verificar su eficacia. Véase el Recuadro 41 para obtener un ejemplo de estrategia de gestión del cambio.

RE 3.2.6.6. Gestión de incidentes

El RE 3.2.6.6 requiere que las administraciones tributarias tengan un sistema de gestión de incidentes que cubra todas los incidentes de seguridad de cualquier tipo. La gestión de incidentes implica la identificación, documentación y gestión de incidentes de seguridad, tanto en ámbitos informáticos como no informáticos.

Por incidente se entiende básicamente algo que sucede cuando no debería haber sucedido. Aun cuando las administraciones tributarias implementen bien los controles, las cosas pueden salir de una forma distinta a la prevista. Existen dos razones principales para tener un sistema de gestión de incidentes:

- Subsanar los incidentes de la forma más rápida y eficiente posible, a fin de minimizar su posible impacto.
- Prevenir la repetición de los incidentes.

Los incidentes en las distintas áreas de la administración tributaria deben gestionarse de manera similar aun cuando no sean gestionadas por las mismas personas. Por ejemplo, los incidentes de TI suelen gestionarse a través de un servicio de asistencia informática. Los incidentes de seguridad no informáticos, como los incidentes de acceso físico o los incidentes de pases de seguridad, pueden ser gestionados por la unidad responsable de la gestión de edificios e instalaciones. Otros incidentes pueden ser gestionados por el departamento de recursos humanos o a través de auditoría interna.

En cualquier caso, debe existir una política o un procedimiento documentados que definan el enfoque de gestión de todos los incidentes de seguridad que afecten a la administración tributaria. Esto obedece principalmente a la necesidad de que el equipo de seguridad y otros involucrados puedan tener en cuenta posibles conexiones entre distintos tipos de incidentes, a fin de buscar patrones que puedan apuntar a riesgos que no se han considerado aún.

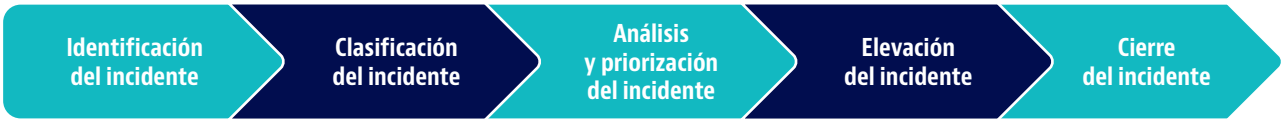
La estrategia de gestión de incidentes de la administración tributaria debe comunicarse con claridad a todo el personal. Además, se deben documentar responsabilidades claras para la gestión de incidentes como parte de las funciones y responsabilidades contempladas en la política GSI (según se describe en el RE 3.2.1.2) relacionada al marco de seguridad global.

La estrategia de gestión de incidentes debe seguir generalmente una serie de pasos, que pueden traducirse en la forma un flujo de trabajo descrito en la Figura 19.[20]

- **Identificación de incidentes informáticos y no informáticos**. El personal debe ser alentado a reportar cualquier evento, tanto informático como no informático, que a su juicio pueda ser un incidente de seguridad. Los canales de reporte de incidentes deben ser accesibles para todo el personal, y los procedimientos no deben ser engorrosos. La notificación de incidentes debe incluirse en la formación inicial o de sensibilización en materia de seguridad para todo el personal. Los incidentes se identifican también como parte de las actividades de monitoreo del registro (véase el RE 3.2.6.2).
- **Clasificación de incidentes**. La(s) persona(s) responsable(s) de gestionar los incidentes debe(n) revisar los incidentes reportados y clasificarlos a fin de que puedan adoptarse las medidas adecuadas. Las clasificaciones, que deben estar contempladas en la política, pueden incluir:

20. Pueden encontrarse orientaciones más detalladas en estándares internacionales tales como ISO20000 o ISO27035.

FIGURA 19. **Flujo de trabajo de la gestión de incidencias**



- Incidentes de seguridad de la información, o eventos que pueden producir resultados negativos desde la perspectiva de la seguridad de la información, esto es, que afecten a la confidencialidad o integridad de la información. Por ejemplo, la pérdida o el robo de un dispositivo USB que contenga información confidencial, o la pérdida de una identificación electrónica de un miembro del personal de la unidad de EOI.

- Otros incidentes como, por ejemplo, un incidente de TI sin impacto en la seguridad de la información, como una impresora que no funciona.

En base a la clasificación de un incidente, su resolución puede ser coordinada por el OSI, por el servicio de asistencia informática o por ambos, según se documente en el procedimiento de gestión de incidentes.

- **Análisis y priorización de incidentes**. Sobre la base de su posible impacto, los incidentes de seguridad deben analizarse y clasificarse como incidentes menores o mayores, para poder priorizar su resolución. Los criterios para la priorización pueden incluir el tipo de incidente (p. ej. pérdida de la identificación electrónica, pérdida o robo de un USB), el tipo de información afectado (p. ej. circulares internas, información de contribuyentes o intercambiada), el número de registros sensibles involucrados (p. ej. datos individuales, un grupo de datos completo) y la probabilidad de que ocurran daños si se divulga la información (p. ej. fraude financiero).
  En función de su prioridad, el tiempo de respuesta a un incidente de seguridad puede variar, y los incidentes mayores pueden activar un procedimiento de elevación del incidente.

- **Elevación de incidentes de seguridad**. Si el análisis del incidente muestra que se ha producido un incidente de seguridad importante, el incidente debe ser elevado e investigado conforme a procedimientos establecidos, para que todas las partes interesadas estén advertidas (p. ej. los individuos afectados, proveedores de datos, autoridades, administraciones tributarias extranjeras en caso de que el incidente involucre información intercambiada, etc.). La elevación y comunicación a otras autoridades, en función de la escala y del impacto de un incidente que constituya una violación de la confidencialidad, debe seguir la legislación nacional y otros requisitos legales o contractuales. Orientaciones más detalladas sobre estos procedimientos se incluyen en el RP 3.3, relativo a las disposiciones y procesos necesarios para abordar violaciones de la confidencialidad.

- **Cierre del incidente**. El cierre de un incidente implica su resolución, la reanudación de las operaciones normales y una evaluación de seguimiento del incidente. Dependiendo de la escala del incidente de seguridad, la evaluación debe identificar sus causas principales, los procesos que fallaron, las partes involucradas, los sistemas afectados, el tiempo de resolución y la eficacia de la solución implementada. Esta evaluación es importante para informar estrategias a largo plazo y así mitigar aún más la probabilidad de que un incidente de seguridad se repita en el futuro, o reducir su impacto perjudicial. Cuando esté justificado deberán imponerse multas o sanciones por incumplimiento, tal como se describe en el RE 3.3.2.

La estrategia definida para la gestión de incidentes debe incluir una revisión periódica de su eficacia. El OSI, junto con el jefe del departamento de TI y los representantes de las áreas del negocio, deben revisar los eventos reportados, la clasificación del incidente y su cierre. El análisis debe resultar en la identificación de cuestiones o problemas que sean la fuente de incidentes recurrentes, de modo que puedan implementarse soluciones más sistémicas.

RE 3.2.6.7. Función de auditoría interna y externa

La función de auditoría interna juega un papel importante en la seguridad de la información en todas las organizaciones, incluidas las administraciones tributarias, pues facilita:

- **Garantía del proceso**. La auditoría interna permite detectar deficiencias en los procesos que pueden aumentar el riesgo de filtración de datos o información e identificar las necesidades de mejora.

- **(In)cumplimiento de procesos**. La auditoría interna comprueba si el personal cumple con los procesos del sistema GSI establecidos en políticas y procedimientos, impulsa mejoras cuando la práctica es diferente de lo establecido y, cuando sea necesario, conduce a medidas disciplinarias en caso de incumplimiento. Aunque los supervisores y/o el departamento de recursos humanos normalmente se ocupan de los asuntos que implican conductas indebidas de los empleados y accesos ilícitos a información, una función de auditoría interna que funcione adecuadamente tendrá los recursos y la experiencia necesarios para identificar los rastros del incumplimiento antes de que sea evidente para los demás. La estrategia de auditoría interna debe documentarse, y debe garantizarse la capacidad de los auditores internos.

Las administraciones tributarias deben establecer políticas y procedimientos de auditoría interna que observen los siguientes principios fundamentales:

- **Independencia**. Los auditores no deben tener intereses particulares distintos de los objetivos generales de la administración tributaria conforme a lo dispuesto en la legislación y las políticas claramente establecidas para cumplir esos objetivos.
- **Acceso a evidencia**. Los auditores deben obtener evidencia de la efectiva implementación del sistema GSI a través de la interacción con el personal responsable de las actividades. En caso de sospecha, pueden pedir acceso directo a los datos, sistemas y controles correspondientes.
- **Acceso a los responsables clave de la toma de decisiones**. El jefe de auditoría interna debe tener acceso directo al jefe de la administración tributaria si las circunstancias así lo requieren.
- **Discreción sobre lo que se audita**. Aunque es una buena práctica que el jefe de auditoría interna se reúna periódicamente con los cargos directivos de la administración tributaria a fin de identificar procesos o funciones adecuados para auditar, la auditoría interna debe controlar al menos una parte de su programa de trabajo y ser capaz de auditar aquellos procesos y funciones que considere más adecuados. Debe prestarse especial atención a los procesos que plantean el mayor riesgo pero, por lo general, todos los procesos deben ser revisados, si no con carácter anual, en algún periodo intermedio.
- **Reporte de auditorías**. El reporte de auditoría debe presentar las conclusiones con respecto al nivel general de cumplimiento de los distintos procesos relacionados con la GSI, y proponer recomendaciones de mejora. La aplicación de las medidas correctivas propuestas debe coordinarse con el OSI. El reporte debe indicar asimismo la muestra de procesos que se ha auditado y el personal que ha intervenido en la auditoría, y debe ser presentado a los directivos de la administración tributaria.
- **Periodicidad de las auditorías**. Las auditorías internas deben llevarse a cabo de forma periódica. Dependiendo de la complejidad y el tamaño de la administración tributaria, los procesos que plantean mayores riesgos para la seguridad deben evaluarse mediante una auditoría interna al menos una vez al año.

Además de la función de auditoría interna, una buena práctica internacional sería requerir que las administraciones tributarias se sometan a auditorías externas llevadas a cabo por otras autoridades independientes en relación con el sistema GSI (p. ej. Inspección General del Ministerio de Hacienda, Autoridad Estatal de Auditoría, órgano de supervisión de la Protección de Datos, etc.).

En jurisdicciones en las que la administración tributaria es pequeña y puede resultar complicado dotar de recursos a la función de auditoría interna, posiblemente sea necesario basarse en varias auditorías externas realizadas por autoridades independientes en ese país o en una auditoría externa comercial realizada por un organismo de certificación acreditado.

El Recuadro 42 ofrece un ejemplo de auditoría interna de procesos de GSI.

Recuadro 42. Ejemplo de auditoría interna de procesos de GSI

La función de auditoría interna en la administración tributaria de la Jurisdicción B tiene como objetivo proporcionar evaluaciones independientes y objetivas sobre la eficacia del gobierno, la gestión de riesgos y los controles internos dentro de la administración tributaria. Las auditorías se basan en riesgos e incluyen, entre otras, auditorías sobre sistemas y procesos informáticos, ciberseguridad, gestión de datos e información, gestión de terceros y seguridad física.

La función de Auditoría Interna responde ante el Auditor General, y tiene acceso no restringido y comunicación con el jefe de la administración tributaria. Los resultados de auditoría se reportan al Auditor General con carácter trimestral, y al Comisionado cada semestre.

Las auditorías de procesos que afectan al EOI comprenden la revisión de los registros y su monitoreo e integridad, especialmente el acceso a información de los contribuyentes para garantizar que se aplican controles y procedimientos y que estos funcionan según lo previsto para prevenir el acceso no autorizado.

4. Disposiciones de cumplimiento y procesos para abordar las infracciones de confidencialidad (Requisito Principal 3.3)

Aun cuando se adopten marcos de GSI y controles de seguridad adecuados, la posibilidad de acceso no autorizado o violaciones de datos no puede descartarse. Por ello, para fortalecer el marco GSI y la capacidad de una administración tributaria para prevenir futuras infracciones es fundamental contar con disposiciones de cumplimiento efectivas y procesos bien definidos para gestionar las violaciones de confidencialidad y aprender de ellas.

Por lo tanto, el RP 3.3 requiere que las jurisdicciones tengan disposiciones de cumplimiento y procesos de para abordar las violaciones de la confidencialidad. Este requisito principal se divide en dos REs (véase la Figura 20):

- RE 3.3.1: Las jurisdicciones deben imponer multas o sanciones adecuadas por el uso o la divulgación indebidos de información.
- RE 3.3.2: Las jurisdicciones deben aplicar procesos adecuados para abordar incumplimientos supuestos o reales, que incluyen la aplicación efectiva de sanciones.

REQUISITO ESPECÍFICO 3.3.1: SANCIONES POR LA DIVULGACIÓN O EL USO INDEBIDOS DE INFORMACIÓN DEL CONTRIBUYENTE

A fin de garantizar la aplicación efectiva de las disposiciones jurídicas en materia de confidencialidad y el uso adecuado de información del contribuyente, incluida la información intercambiada, la ley debe imponer sanciones suficientemente claras y severas para

FIGURA 20. **Componentes fundamentales para abordar las violaciones de la confidencialidad**

Recuadro 43. **Ejemplo de sanciones por la divulgación o el uso no autorizados de información del contribuyente**

La Ley del Impuesto sobre la Renta (LIR) de la Jurisdicción A establece sanciones pecuniarias y penales, en función de la gravedad del delito, para cualquier persona, incluido el personal y los contratistas externos, que viole la confidencialidad de la información del contribuyente con arreglo a la LIR. Las infracciones se sancionan con una multa de hasta EUR 15 000 o hasta tres años de prisión.

Bajo el Código de Conducta de la administración tributaria de la Jurisdicción A, la divulgación o el uso no autorizados de información del contribuyente, incluida la información intercambiada, constituye una falta grave sancionada con el despido. Además del despido, el manejo indebido accidental o negligente de información del contribuyente puede motivar la adopción de medidas disciplinarias, que incluyen advertencias, suspensión temporal y degradación de categoría profesional.

desincentivar las infracciones y violaciones.

Las sanciones pueden estar contenidas en la legislación tributaria, de administración pública o penal, o en una combinación de todas ellas. Lo importante es que se tengan debidamente en cuenta multas o sanciones administrativas, civiles y/o penales, que cubran una amplia gama de violaciones de la confidencialidad o uso indebido de información.

La gravedad de las sanciones (p. ej. amonestación, suspensión de funciones, sanción pecuniaria o prisión) dependerá por lo general de la gravedad y el impacto de la conducta que motivó su aplicación.

Las sanciones deben ser aplicables a todo tipo de personas que pueden tratar información del contribuyente y cometer una infracción:

- El personal, tanto trabajadores fijos (p. ej. funcionarios de carrera) como temporales (contratos temporales, nombramientos de duración limitada).
- Los contratistas externos, incluidas las personas físicas y jurídicas.

Las sanciones deben aplicarse también a infracciones cometidas por personal y contratistas pasados, es decir, después de que cesen sus funciones con respecto a la información de los contribuyentes. El Recuadro 43 ofrece un ejemplo de sanciones aplicadas en caso de divulgación no autorizada de información del contribuyente.

REQUISITO ESPECÍFICO 3.3.2: PROCEDIMIENTOS PARA ABORDAR VIOLACIONES U OTROS INCUMPLIMIENTOS SUPUESTOS O REALES, INCLUIDA LA APLICACIÓN EFECTIVA DE SANCIONES

Las disposiciones sancionadoras deben ir acompañadas de procesos y recursos necesarios para garantizar su aplicación efectiva. También es necesario adoptar procesos que prevean qué sucede desde que se produce o se sospecha una infracción o se incumplen las políticas, hasta el momento en que se adopta la decisión de aplicar una sanción adecuada (o hasta que la situación sea resuelta de otro modo, sin necesidad de aplicar una sanción).

La violación de la confidencialidad del contribuyente puede proceder de un acto involuntario, deficiencias en los sistemas y procedimientos que protegen la confidencialidad de la información, o puede ser consecuencia de acciones intencionadas en beneficio personal por parte de una o más personas (por ejemplo, en caso de corrupción).

Ya sea resultado de acciones intencionadas o involuntarias, cualquier violación de la confidencialidad debe tomarse en serio y abordarse de inmediato. Deben adoptarse medidas adecuadas en función de las circunstancias de la infracción. Si se debe a un acto intencionado para obtener un beneficio personal, por lo general sería adecuado remitir el asunto a los agentes de la ley para que presenten posibles cargos penales.

La planificación y preparación previa frente a las violaciones de la confidencialidad –es decir, la existencia de procesos para gestionarlas– permite a las jurisdicciones manejar situaciones derivadas de las infracciones de manera más rápida y eficaz. Un sistema de gestión de infracciones eficaz requiere procesos que definan los procedimientos de reporte, elevación a un nivel superior, de investigación y disciplinarios, así como las funciones y responsabilidades de los actores interesados en cada una de las fases. Los procesos deben prever distintos escenarios de infracción de distinta gravedad. Asimismo, los procesos deben revisarse y actualizarse cuando sea necesario, en base a la experiencia derivada de su aplicación.

Conforme al RE 3.3.2, deben establecerse cuatro tipos distintos de procesos con respecto a las infracciones, incluidas aquellas que involucran información intercambiada, tal como se representa en la Figura 21.

El Foro Global ha preparado y puede ofrecer a las jurisdicciones, previa petición, orientaciones más precisas sobre buenas prácticas de gestión de violaciones de datos y los requerimientos del RE 3.3.2.

RE 3.3.2.1. Procesos cuando se sospecha o se produce una infracción, para garantizar el reporte e investigación

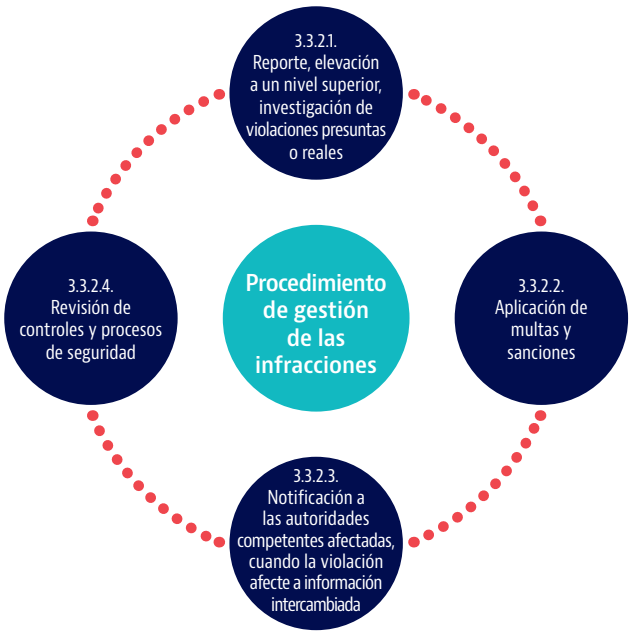
El RE 3.3.2.1 requiere que las jurisdicciones tengan procesos a seguir cuando se sospeche o produzca un acceso, uso o divulgación no autorizados, los que deben garantizar que estos problemas se reporten e investiguen. Estos aspectos se analizan a continuación.

Procesos de reporte

Los procesos de las administraciones tributarias deben establecer que el personal notifique las violaciones presuntas o reales de información confidencial, incluida la información intercambiada, y los pasos para reportar, registrar y elevar un incidente. Los procesos deben documentarse y estar a disposición del personal para facilitar su consulta, de modo que el personal conozca la cadena de reporte o elevación. También debe impartirse capacitación al respecto. A menudo, el departamento de seguridad de la administración tributaria es el encargado de recibir los reportes.

A modo de ejemplo, los procesos podrían establecer que el personal deba reportar por escrito una violación de información presunta o real al superior inmediato, o a un funcionario responsable designado quien, en caso de necesidad y en función de la gravedad del incidente, elevará el asunto a la dirección, p. ej. al jefe de la administración tributaria.

FIGURA 21. **Elementos principales de la gestión de las violaciones de la confidencialidad**



El proceso también puede prever que el funcionario responsable designado realice pesquisas iniciales con las personas denunciantes y denunciadas y/o sus superiores, antes de decidir si debe activar formalmente un procedimiento de gestión de infracciones, incluyendo una investigación formal.

El proceso puede requerir que el personal denunciante reporte toda información o prueba relevante que tenga en su poder que respalde su sospecha o conocimiento de una infracción. El proceso también puede prever un procedimiento de seguimiento con el personal denunciante, para obtener cualquier información adicional en relación con la infracción reportada.

Procesos de investigación

Si un incidente reportado necesita ser investigado, debe iniciarse una investigación lo suficiente exhaustiva para determinar:

- Las circunstancias que llevaron a la violación o incumplimiento.
- La persona o personas responsables.
- Cuando sea posible, la causa de la infracción.

Por tanto, los procesos de las administraciones tributarias deben comprender también los procedimientos de investigación y recopilación de hechos que permitan conocer el alcance y la gravedad de una infracción reportada. La investigación no debe retrasar ninguna medida inmediata que pueda tomarse para minimizar el impacto de la infracción, p. ej. la revocación del acceso de un supuesto infractor a los sistemas de información o el aislamiento de los entornos físicos o informáticos en los que se conservan los datos comprometidos.

Los procesos de investigación cubrirán normalmente los siguientes aspectos:

- **Investigación preliminar para determinar la gravedad de una infracción**. La investigación preliminar permite determinar el tipo de infracción (p. ej. ciberataque, datos robados por un infiltrado, documentos o medios de almacenamiento perdidos), la magnitud de los datos violados (pocos datos o un conjunto completo de datos), el tipo de datos afectados (p. ej. datos de contribuyentes nacionales, datos de AEOI o EOIR), o cualquier jurisdicción con la que se intercambie información que se vea afectada.
- **Identificación de la(s) persona(s) encargada(s) de la investigación y de los actores internos y externos que deben estar involucrados**. Los funcionarios encargados

de la supervisión y coordinación de las investigaciones deben estar claramente identificados. Los procedimientos podrían establecer también qué tipo de coordinación entre departamentos se necesitará en caso de que un incidente sea lo suficientemente grave como para que requerir una investigación exhaustiva (p. ej. departamento de TI, departamento de auditoría interna y las unidades de negocio relevantes tales como la unidad de EOI). También pueden regular la necesaria coordinación con actores externos (p. ej. contribuyentes afectados, proveedores de datos, la autoridad de protección de datos, la policía y las autoridades competentes de otro país, si la infracción afecta a información intercambiada). En caso de infracciones muy graves, podría requerirseo presentar una denuncia ante la policía.

- **Procedimientos de recopilación de evidencias**. La evidencia es un elemento esencial del proceso de investigación, pues ayudará a determinar la(s) persona(s) responsable(s) e informa la prevención de infracciones similares en el futuro. La evidencia será esencial para la debida aplicación de sanciones, incluidas las de carácter penal, cuando esté justificado. Por lo tanto, deben existir procedimientos claros para la realización de indagaciones y la recopilación de evidencias, p. ej. por los departamentos de auditoría o disciplinario y, cuando proceda, en colaboración con las autoridades de cumplimiento de la ley.

- **Medidas provisionales**. Mientras las investigaciones están en curso, los procedimientos podrían permitir la adopción de medidas administrativas adecuadas, como el traslado o la suspensión de la(s) persona(s) sospechosa(s) o efectivamente responsable(s) de la infracción, a fin de garantizar investigaciones justas y transparentes.

Una vez concluida la investigación, debe prepararse un reporte para la gerencia que incluya recomendaciones para la adopción de medidas o sanciones contra la(s) persona(s) responsable(s) (las autoridades de cumplimiento de la ley pueden intervenir en caso de que se sospeche que la divulgación ha sido intencionada).

RE 3.3.2.2. Recursos, procesos y procedimientos para adoptar medidas correctivas y aplicar sanciones adecuadas cuando se identifiquen problemas

Los procesos de las administraciones tributarias deben garantizar también la imposición efectiva de multas o sanciones en base al marco jurídico, que se aborda en el RE 3.3.1.

Por tanto, el RE 3.3.2.2 establece que las jurisdicciones deben, con el respaldo de recursos, procesos y procedimientos administrativos adecuados, garantizar que se adopten medidas correctivas cuando se identifiquen problemas reales, con la imposición en la práctica de multas o sanciones adecuadas a los empleados, contratistas y otras personas que vulneren las normas de confidencialidad, las políticas de seguridad o los procedimientos, para disuadir a otros de cometer infracciones similares.

Los procesos deben describir los pasos administrativos para la imposición de sanciones disciplinarias y administrativas tales como amonestación, suspensión, degradación de categoría profesional, reducción salarial o despido, en función de la gravedad y seriedad de la infracción.

Normalmente existirá una autoridad dentro de la administración tributaria, o en otro ámbito dentro del sector público, responsable de la aplicación de sanciones administrativas o disciplinarias. Dicha autoridad tendrá normalmente conferidas las competencias necesarias para imponer las sanciones correspondientes, o poner los hechos en conocimiento de la policía u otra autoridad encargada de velar por el cumplimiento de la ley, según proceda. Los procesos para denunciar los hechos a la policía a fin de que inicie una investigación y un procedimiento penal deben estar documentados. Las disposiciones legales aplicables que puedan invocarse para la imposición de multas administrativas, civiles o económicas, o para solicitar la incoación de actuaciones penales, también podrán documentarse con el fin de facilitar su consulta.

RE 3.3.2.3. Notificación a autoridades competentes extranjeras acerca de violaciones de la confidencialidad de información intercambiada

Si una violación de la confidencialidad afecta a información intercambiada, un aspecto esencial de la gestión y respuesta a dicha infracción es la comunicación con los socios de intercambio.

Bajo los acuerdos internacionales de intercambio de información, las jurisdicciones suelen estar obligadas a informar inmediatamente a las autoridades competentes de los socios de intercambio que suministraron la información que ha sido divulgada o usada sin autorización, a fin de que puedan formular medidas de respuesta adecuadas con arreglo a su marco jurídico interno y los acuerdos aplicables.[21] Las comunicaciones

21. En el caso de algunos acuerdos multilaterales, la autoridad competente de la jurisdicción en la que se produzca una violación de información intercambiada debe notificar a la Secretaría del Órgano de Coordinación del acuerdo, que a su vez notificará a otras autoridades competentes con las que esté en vigor un acuerdo multilateral para asegurarse de que estén informadas. Véase, por ejemplo el Acuerdo Multilateral de Autoridades Competentes (MCAA) sobre el Estándar Común de Reporte (CRS), sección 5(2), y el MCAA sobre intercambio de reportes país por país, sección 5(3).

por parte de la jurisdicción en la que ha ocurrido la infracción son también importantes para dar a los socios de intercambio la seguridad de que las causas se investigarán rápida y exhaustivamente, y de que se adoptarán medidas correctivas. Estos aspectos son esenciales para mantener la confianza en el intercambio internacional de información fiscal.

Por lo tanto, el RE 3.3.2.3 requiere que las jurisdicciones apliquen procesos para notificar a otras Autoridades Competentes las violaciones de la confidencialidad o el fallo de las medidas de protección, así como las sanciones y acciones correctivas impuestas en consecuencia.

Por lo general, se espera que la notificación a las autoridades competentes extranjeras incluyan los siguientes aspectos:

- Dónde ocurrió la infracción (p. ej. en qué organización, división o sistema de una administración tributaria).
- El tipo de infracción (p. ej. ciberataque, datos robados por un infiltrado, documentos o medios de almacenamiento perdidos).
- El tipo de datos afectados (p. ej. archivo de EOIR o datos de AEOI).
- Las medidas adoptadas para contener, erradicar y analizar la situación.
- El punto de contacto central en la administración tributaria y otros puntos de contacto relevantes.

Tras la notificación inicial, podría ser recomendable que la administración tributaria continúe en contacto con el o los socios de intercambio en cuestión con el fin de facilitar que adopten medidas adecuadas en su jurisdicción (tales como el cumplimiento de obligaciones legales internas de notificar a los contribuyentes afectados y a las autoridades de protección de datos). En ciertos casos puede ser recomendable emitir comunicados públicos.

La Figura 22 describe los posibles pasos de comunicación que pueden emprenderse cuando tiene lugar una violación de información intercambiada.

RE 3.3.2.4 Revisión de controles de seguridad y de los procesos de monitoreo y cumplimiento en respuesta a infracciones

Es esencial aprender de los incidentes y las infracciones, con el fin de mejorar continuamente los procesos y controles dirigidos a vigilar, prevenir y gestionar los que puedan producirse en el futuro.

Por tanto, el RE 3.3.2.4 establece que las jurisdicciones deben revisar los procesos de monitoreo y de cumplimiento en respuesta a infracciones, y la alta dirección debe asegurarse de que las recomendaciones de cambios se aplican en la práctica.

FIGURA 22. **Acciones comunicativas generales en caso de una infracción que afecte a información que ha sido intercambiada**

Colaborar con los socios de intercambio	Una jurisdicción debe ponerse en contacto oportunamente con el o los socios de intercambio afectados por una violación de información intercambiada. La Secretaría del Foro Global puede ayudar a una jurisdicción proporcionándole orientación relativa a las obligaciones generales de notificación de acuerdos internacionales de intercambio de información y facilitar las comunicaciones con autoridades competentes extranjeras (en todos estos casos, sin acceder a información específica de los contribuyentes).
Abordar los requisitos legales para notificar a las personas y autoridades afectadas	De conformidad con la legislación interna en materia de protección de datos y privacidad, puede ser necesario informar a los contribuyentes afectados acerca de la violación de sus datos. Puede solicitarse la cooperación de las autoridades competentes socias, cuando proceda, p. ej. en casos en los que las personas afectadas no sean residentes en la jurisdicción en la que ha tenido lugar la infracción.
Mantener informados a los socios de intercambio a medida que se desarrolla el caso	Puede ser necesario mantener informados a los socios de intercambio acerca de los resultados de las investigaciones y las medidas adoptadas para contener y remediar una infracción, así como los resultados de esas medidas, p. ej. las sanciones impuestas y, si los intercambios se suspendieron con carácter preventivo, si la jurisdicción está lista para reanudar los intercambios.
Informar a los actores externos y al público cuando proceda	Puede ser conveniente informar al público cuando sea necesario para disipar la preocupación pública acerca de una violación de datos, así como para prevenir la desinformación.

Esto significa que las administraciones tributarias deben revisar en general sus procesos de monitoreo, cumplimiento y gestión de infracciones, así como los controles de seguridad relevantes, no solo de forma rutinaria como se contempla en el RE 3.2.6 relativo a la gestión de las operaciones, sino también en base a las lecciones aprendidas de infracciones específicas.

Para apoyar estas revisiones, los informes elaborados al concluir una investigación de una infracción pueden recomendar, además de una sanción adecuada a la(s) persona(s) responsable(s):

- Medidas para minimizar las repercusiones de la infracción.
- Futuras acciones para evitar infracciones o incidentes similares.
- Posibles mejoras (de ser necesario) de los procesos de reporte, de investigación, disciplinarios o administrativos para aplicar sanciones.

Las lecciones aprendidas de incidentes concretos también deben alimentar las revisiones periódicas (p. ej. anuales o bianuales) destinadas a:

- Identificar estrategias a más largo plazo para reducir aún más la probabilidad de reiteración de las infracciones.
- Mejorar el proceso de gestión de las infracciones.

La autoridad investigadora, las personas encargadas de la seguridad de la información y la confidencialidad en la administración tributaria (p. ej. el OSI), y/o la alta dirección deben ser responsables de realizar el seguimiento para garantizar que se implementen las recomendaciones de mejora derivadas de una infracción concreta o una revisión de procesos.

La revisión de los controles de seguridad y de los procesos de monitoreo o cumplimiento podría dar como resultado:

- La aplicación de medidas correctivas del proceso en el que se produjo la infracción.
- La revisión de procesos de selección o contratación de personal (empleados y contratistas externos).
- La implementación de programas de formación periódica para el manejo seguro de datos confidenciales y la promoción de la sensibilización en materia de seguridad.
- La revisión y mejora de los controles de GSI, p. ej. los derechos de acceso.
- La realización más frecuente de simulacros de respuesta ante violaciones de datos.

Véase el Recuadro 44 para ver un ejemplo de proceso dirigido a tratar las violaciones de información confidencial.

Recuadro 44. **Resumen de un ejemplo de política de gestión de las infracciones**

Bajo la Política de Notificación de Infracciones de la Confidencialidad e Incidentes de Seguridad de la administración tributaria de la Jurisdicción B, todos los empleados y los contratistas externos deben reportar por escrito al Oficial de Seguridad de la Información (OSI) las violaciones de la confidencialidad o incidentes de vulneración de las políticas de seguridad de la información, presuntos o reales. La Política establece las funciones y responsabilidades de los distintos miembros del personal durante todo el proceso de reporte e investigación.

Cuando concluya la investigación, el gerente de línea del proceso de negocio afectado debe elaborar un informe, asesorado por el OSI, que documente el incidente, una evaluación de su gravedad y sus causas probables. Dependiendo de la naturaleza, magnitud y gravedad del incidente, el gerente de línea puede decidir elevar el incidente a la Agencia de Protección de la Información y/o derivar el incidente a la policía.

Bajo la Política, deben aplicarse medidas correctivas a fin de remediar el fallo que causó la infracción. Si la infracción afecta a información intercambiada, el incidente debe reportarse también a el o los socios de intercambio relevantes y, cuando proceda, a la Secretaría del Órgano de Coordinación del acuerdo multilateral de intercambio de información aplicable.

El informe del gerente de línea debe recomendar las medidas disciplinarias adecuadas que deben adoptarse contra la(s) persona(s) responsable(s). Estas medidas pueden comprender la advertencia, el despido, la suspensión, la degradación de rango y el recorte salarial.

Una vez se haya subsanado el incidente y se haya cerrado la investigación, el OSI debe preparar un informe para el directorio de la administración tributaria indicando si se recomienda medidas para mejorar las políticas, procesos o controles de seguridad relevantes.

Anexos

Anexo A. Glosario de conceptos

CONCEPTO	DESCRIPCIÓN	RE
Acceso físico	Un acceso a zonas específicas de las instalaciones.	**3.2.3**
Acceso lógico	Un acceso a sistemas mediante procesos de identificación, autenticación y autorización.	**3.2.3**
Actividad de registro	La actividad de registro se refiere al registro y seguimiento por las administraciones tributarias de todo acceso a datos protegidos, incluido el acceso a instalaciones y áreas en las que se conservan los datos, y en particular a sistemas que contienen registros y otra información sensible de los contribuyentes.	**3.2.6**
Activo	Todo elemento de valor involucrado en el desarrollo de procesos y en la generación de resultados. Los activos pueden ser información, personas, servicios, equipos, sistemas, etc.	**3.2.1**
Acuerdo de Nivel de Servicio	Acuerdo que establece un nivel de servicio mínimo que debe cumplir una entidad que presta un servicio.	**3.2.4**
Acuerdo de no divulgación	Declaraciones o contratos formales en los que se establecen las reglas para la no divulgación de información confidencial a terceros.	**3.2.2**
Autenticación	Cuando un usuario accede a los sistemas informáticos, el proceso de autenticación asegura y confirma la identidad de dicho usuario de manera irrefutable.	**3.2.3**
Autoridad competente	La(s) autoridad(es) competente(s) es(son) la(s) persona(s) o autoridad(es) gubernamental(es) designada(s) por una jurisdicción como competente(s) para intercambiar información con arreglo a cualquier acuerdo internacional de intercambio de información.	**3.1.1, 3.2.5**
Autorización	Una vez se haya identificado a un usuario en un sistema, el usuario estará autorizado a acceder a los recursos según los principios de necesidad y de mínimo privilegio.	**3.2.3**
Centro de Operaciones de Seguridad	Un Centro de Operaciones de Seguridad es un equipo de profesionales y sistemas especializados para el monitoreo y análisis continuo de la situación de seguridad de la administración tributaria.	**3.2.6**
Cifrado	El cifrado es un mecanismo de protección aplicado a datos para que sean accesibles únicamente cuando se facilite la clave de descifrado adecuada.	**3.2.5**
Clasificación de información	Proceso dirigido a identificar los tipos de información en poder de las administraciones tributarias y determinar el nivel de protección que deben recibir.	**3.2.5**

Anexos

CONCEPTO	DESCRIPCIÓN	RE
Concesión de acceso	Otorgamiento efectivo del acceso a información a través de la creación de cuentas de usuario, administración de contraseñas y de la asignación a los usuarios de derechos de acceso específicos y autorizaciones.	**3.2.3**
Controles	Véase Prácticas.	**3.2.1**
Controles básicos	Conjunto de controles de seguridad mínimos que una administración tributaria aplica a ciertos riesgos, con independencia de su gravedad.	**3.2.4**
Controles de acceso	Controles de seguridad que garantizan que el acceso a la información, los espacios físicos y los sistemas esté basado en la necesidad de saber y los derechos mínimos.	**3.2.3**
Control de seguridad de TI	Medida administrativa, técnica o física implantada para mitigar un riesgo de TI.	**3.2.4**
Externalización	Recurrir a un proveedor externo para el suministro de bienes y servicios.	**3.2.4**
Firewall	Equipo instalado en puntos estratégicos de una red (normalmente frente al acceso externo o interno y zonas internas divididas) que permite o bloquea el tráfico en base a ciertas reglas.	**3.2.4**
Formación	Medidas dirigidas a que el personal de la administración tributaria (empleados y contratistas) adquiera y desarrolle los conocimientos, aptitudes y competencias clave necesarias para integrar la confidencialidad y la seguridad en los procesos tributarios.	**3.2.2**
Función de auditoría	Revisiones exhaustivas e imparciales para evaluar el cumplimiento de los procesos de sistemas de GSI establecidos en las políticas y procedimientos. Las conclusiones y resultados de la auditoría deben comunicarse directamente al jefe de la administración tributaria.	**3.2.6**
Gestión de activos	Proceso que garantiza que los activos de la administración tributaria se identifiquen y rastreen desde su creación o adquisición hasta su destrucción o eliminación.	**3.2.4**
Gestión de incidentes	Implica la identificación, documentación y gestión de incidentes de seguridad, tanto en ámbitos de informáticos como no informáticos.	**3.2.6**
Gestión del acceso	Políticas, procesos y procedimientos, de los que son responsables los cargos directivos y no únicamente la función informática de la administración tributaria, que rigen el acceso físico y lógico, así como los procesos efectivos para la concesión y la auditoría del acceso lógico y para la identificación y autenticación de los usuarios.	**3.2.3**
Gestión del cambio	Se refiere a la gestión controlada del desarrollo de nuevos sistemas y servicios, así como la realización de cambios importantes sobre los ya existentes.	**3.2.6**
Gestión de la continuidad del negocio	Proceso de gestión dirigido a asegurar la continuidad de las operaciones en el escenario de un evento que altere su curso normal.	**3.2.1**

CONCEPTO	DESCRIPCIÓN	RE
Gestión de proveedores	Proceso basado en el riesgo que garantiza que un proveedor externo que acceda a los datos o instalaciones de una administración tributaria no ponga en riesgo la confidencialidad y seguridad.	**3.2.4**
Gestión de registros	Se refiere a los procesos y políticas colectivos que se utilizan para administrar y facilitar la generación, transmisión, análisis, almacenamiento, archivo y eliminación final de grandes cantidades de datos del registro generados en un sistema de TI.	**3.2.6**
Gestión de vulnerabilidades	Se refiere a los procesos y procedimientos de identificación y gestión de vulnerabilidades.	**3.2.6**
Identificación	Un proceso utilizado en los sistemas informáticos para identificar únicamente a los usuarios que disponen de un derecho de acceso.	**3.2.3**
Ingeniería social	Consiste en explotar de forma malintencionada la confianza del personal para obtener información que puede utilizarse en beneficio propio. Esta actividad se conoce también como "piratería de personas".	**3.2.2**
Malware	Software malicioso. Programa creado para explotar una vulnerabilidad en un sistema seleccionado con el fin de dañarlo o sustraer información.	**3.2.4**
Marco GSI	Un marco de GSI comprende las estructuras organizativas y los principios generales sobre seguridad de la información, que guían a las administraciones tributarias para alcanzar sus objetivos en GSI, siguiendo un enfoque basado en riesgos. La responsabilidad última sobre el marco GSI debe recaer en los funcionarios de mayor jerarquía dentro de la administración tributaria.	**3.2.1**
Mínimo privilegio	Principio de gestión del acceso que establece que el acceso legítimo debe restringirse a las funciones específicas mínimas que el usuario necesita para desempeñar sus tareas.	**3.2.3**
Mitigación del riesgo	Consiste en adoptar activamente medidas para reducir el impacto o la probabilidad de que se produzca un riesgo.	**3.2.1**
Necesidad de saber	Principio de gestión del acceso que establece que solo debe acceder a la información del contribuyente el personal con un fin de negocio legítimo para ello.	**3.2.3**
Nomenclaturas	Reglas que establecen cómo debe designarse la información para que sea claramente identificable.	**3.2.1**
Período de conservación	Requisito legal para conservar información durante un período determinado aun cuando la información deje de ser necesaria para cumplir los fines de la actividad tributaria.	**3.2.5**
Phishing	Tipo de estafa online que consiste en el envío de mensajes fraudulentos de correo electrónico que aparentan proceder de una fuente legítima y engañan al destinatario para que envíe información confidencial, como sus credenciales de acceso a los sistemas.	**3.2.2**

Anexos

CONCEPTO	DESCRIPCIÓN	RE
Política	Una política es una declaración documentada de la administración tributaria en relación con la implementación de procesos, procedimientos y controles en un ámbito determinado. Una política responde a la pregunta "¿qué se debe hacer?". Debe existir una jerarquía entre las políticas. Por ejemplo, una política sobre identificación y autenticación para el acceso a los sistemas de TI estará subordinada a la política global sobre la gestión del acceso. También debe existir una política de GSI general en la que se enumeren los principios generales de seguridad aplicables a todas las políticas.	**3.2.1**
Política de escritorio limpio/despejado	Una política de escritorio limpio/despejado (CDP, siglas en inglés de *clean/clear desk policy*) especifica cómo deben dejar su espacio de trabajo los empleados cuando abandonan sus escritorios o salen de la oficina, a fin de garantizar la confidencialidad de la información.	**3.2.5**
Política de uso aceptable	Conjunto de normas que establecen las prácticas permitidas y prohibidas en relación con los sistemas de información que contienen información confidencial.	**3.2.5**
Política GSI	Una política de GSI expresa la postura de la administración tributaria sobre la forma en cómo plantea la seguridad de la información. La política de GSI debe establecer el alcance del sistema de GSI y los objetivos generales de gestión de la seguridad de la información a los que habrán de ajustarse todas las demás políticas específicas.	**3.2.1**
Prácticas o controles	Un control o una práctica es una medida específica utilizada para gestionar el riesgo para la seguridad de la información (es decir, para mitigar o eliminar el riesgo). Los controles pueden ser procesos y procedimientos, así como programas, herramientas, técnicas, tecnologías y dispositivos. En ocasiones, los controles también se denominan como salvaguardas o contramedidas en relación con un riesgo identificado.	**3.2.1**
Procedimiento	Un procedimiento es una serie documentada de pasos y actividades para implementar políticas de seguridad. Un procedimiento responde a la pregunta "¿cómo se debe hacer y quién lo hace?". El término procedimiento suele aparecer asociado al término proceso – procesos y procedimientos –, porque un procedimiento suele ser una representación más detallada de cada uno de los pasos de un proceso. Con frecuencia, puede haber más de un procedimiento para cada paso de un proceso. Por ejemplo, un proceso puede referirse a la presentación de una declaración de impuestos; pero como pueden existir distintas formas de realizar esa presentación, existirán procedimientos diferentes para cada forma de presentación.	**3.2.1**
Proceso	Un proceso es una secuencia repetible de acciones con un resultado medible. El concepto de proceso es crucial en la GSI. Medir los resultados y actuar en función de ellos constituye la base para mejorar los procesos y la seguridad. Un proceso puede ser de cualquier tipo, desde un proceso tributario, como la presentación y la evaluación de declaraciones de impuestos, hasta la actualización de programas informáticos. Toda acción que no forme parte de un proceso determinado representa por definición un riesgo para la seguridad, ya que no hay garantía de repetibilidad ni de que se midan y mejoren sus resultados.	**3.2.1**
Pruebas de penetración	Las pruebas de penetración simulan las acciones de un pirata informático contra la organización.	**3.2.4, 3.2.5**

CONCEPTO	DESCRIPCIÓN	RE
Recuperación	Se refiere a la restauración de servicios y operaciones en caso de fallo grave.	**3.2.4**
Registro	Un registro, en un contexto informático, es la documentación automática y con indicación del momento en que se producen, de los eventos relevantes para un sistema informático concreto. También pueden llevarse registros manuales para actividades no informáticas.	**3.2.6**
Resiliencia	Se refiere a la mitigación del riesgo de interrupción del servicio y la garantía de tolerancia a los fallos en los servicios, proporcionando la continuidad del servicio hasta cierto punto.	**3.2.4**
Riesgo para la seguridad de la información	Posibilidad de que una amenaza determinada explote vulnerabilidades de un activo o un grupo de activos, causando un perjuicio a la organización.	**3.2.1**
Saneamiento de medios	El saneamiento es el proceso por el cual se tratan datos conservados en medios de almacenamiento con el fin de reducir la probabilidad de recuperación y restauración hasta un nivel aceptable.	**3.2.5**
Seguridad de la información	Se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información.	**3.2.1**
Sensibilización	La sensibilización consiste en exponer periódicamente a los empleados a mensajes de seguridad que les alertan de amenazas y riesgos en materia de TI o de otras amenazas y riesgos para la seguridad; estos mensajes suelen comunicarse a todos los empleados a la vez, tanto en una determinada área de trabajo como en el conjunto de la administración tributaria, e incluso a terceros externos.	**3.2.2**
Sistema GSI	Por sistema de GSI se entiende el conjunto de políticas, procedimientos y controles en ámbitos específicos que permiten implementar el marco de GSI. La responsabilidad última sobre el sistema de GSI debe recaer en los funcionarios de seguridad con mayor jerarquía dentro de la administración tributaria.	**3.2.1**
Usuario legítimo	Usuario que obtiene un derecho de acceso específico en base a los principios de necesidad de saber y de mínimo privilegio.	**3.2.3**
Vulnerabilidad	Deficiencia en el diseño o en la naturaleza de un activo o debilidad derivada de la falta de mantenimiento de un activo.	**3.2.1, 3.2.6**

Nota: Puede haber definiciones oficiales de estos conceptos en las fuentes de referencia relevantes, pero estas son definiciones que usamos para los fines de la guía práctica de GSI.

Anexo B. Recursos de utilidad

Información relevante relativa a estándares internacionales de transparencia fiscal e intercambio de información

- Modelo de Acuerdo entre Autoridades Competentes contenido en el Estándar AEOI: https://www.oecd.org/tax/exchange-of-tax-information/estandar-para-el-intercambio-automatico-de-informacion-sobre-cuentas-financieras-segunda-edicion-9789264268074-es.htm

- Estándar para el Intercambio de Información Previa Petición: https://www.oecd.org/tax/transparency/documents/global-forum-handbook-2017-spanish.pdf

- Plan de Acción del Foro Global para la Participación de Países en Desarrollo en el AEOI: https://www.oecd.org/tax/transparency/documents/plan-of-action-AEOI-and-developing-countries.pdf

- Términos de Referencia del proceso de revisión de pares del Intercambio Automático de Información: https://www.oecd.org/tax/transparency/documents/AEOI-terms-of-reference.pdf

- Foro Global sobre Transparencia e Intercambio de Información con Fines Fiscales: http://www.oecd.org/tax/transparency/

- Intercambio de Información Previa Petición: http://www.oecd.org/tax/transparency/what-we-do/exchange-of-information-on-request/exchange-of-information-on-request-peer-review-process.htm

- Intercambio Automático de Información: http://www.oecd.org/tax/automatic-exchange/

  https://www.oecd-ilibrary.org/taxation/estandar-para-el-intercambio-automatico-de-informacion-sobre-cuentas-financieras-segunda-edicion_9789264268074-es

- Estándar Común de Reporte: https://www.oecd.org/tax/automatic-exchange/common-reporting-standard/

- Asistencia técnica disponible del Foro Global sobre Transparencia e Intercambio de Información con Fines Fiscales: https://www.oecd.org/tax/transparency/what-we-do/

- Guía de la OCDE sobre la Protección de la Confidencialidad de la Información Objeto de Intercambio con Fines Fiscales: https://www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe-report.pdf

Modelos de acuerdos de intercambio internacionales

- Modelo de Convenio Tributario sobre la Renta y sobre el Patrimonio de la OCDE: https://www.oecd-ilibrary.org/taxation/modelo-de-convenio-tributario-sobre-la-renta-y-sobre-el-patrimonio-version-abreviada-2017_765324dd-es

- Modelo de Acuerdo sobre Intercambio de Información en Materia Tributaria de la OCDE: https://www.oecd.org/tax/exchange-of-tax-information/2082215.pdf

- Convención modelo de las Naciones Unidas sobre la doble tributación entre países desarrollados y países en desarrollo: https://www.un-ilibrary.org/content/books/9789210474047

- Convención de Asistencia Administrativa Mutua en Materia Fiscal: https://read.oecd-ilibrary.org/taxation/the-multilateral-convention-on-mutual-administrative-assistance-in-tax-matters_9789264115606-en

OCDE
MEJORES POLÍTICAS
PARA UNA VIDA MEJOR

Para más información:

www.oecd.org/tax/transparency

gftaxcooperation@oecd.org

@OECDtax | #TaxTransparency