Guía práctica de fiscalización de los OCEX

GPF-OCEX 5375 Guía de auditoría de determinados procesos automatizados

Referencia: GPF-OCEX 1315, GPF-OCEX 5340

Elaborado por la CT-OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 01/12/2025

1. Introducción

En los últimos años se ha convertido en una tendencia generalizada en el sector público la introducción de sistemas automatizados de complejidad creciente para mejorar la actuación administrativa y la prestación de servicios e incrementar su eficiencia operativa.

En un entorno donde la automatización y las tecnologías emergentes son cada vez más protagonistas en la gestión pública, los auditores se enfrentan a un panorama en constante evolución. Los sistemas informáticos complejos, las bases de datos integradas y los procesos automatizados han redefinido tanto la forma en que se generan y procesan las actuaciones y procedimientos, así como operaciones del sector público en general.

Estos sistemas utilizan una variedad de tecnologías como la automatización de flujos de trabajo, formularios digitales, la automatización robótica de procesos y la inteligencia artificial, lo que representa un reto para las entidades que los implantan, pero también para los auditores públicos que deben fiscalizar los procedimientos administrativos y los procesos de gestión de las entidades del sector público en los que se utilizan.

Esta transformación exige a los profesionales de la auditoría pública familiarizarse con nuevas formas de trabajar, conceptos y herramientas capaces de analizar dichos entornos y con grandes volúmenes de datos. La interacción con infraestructuras tecnológicas, la revisión de controles automáticos y la comprensión de flujos de información digital adquieren un nuevo grado de complejidad.

Históricamente, los algoritmos utilizados para automatizar procesos de gestión han sido de tipo determinista, es decir, para un input dado producían un output de forma consistente, basado en reglas bien definidas y fácilmente revisables por un auditor. Por ejemplo, la aplicación para elaborar las

nóminas usa distintos automatismos o algoritmos: uno para calcular el tipo de retención de IRPF, otro para calcular las horas extras, otro para calcular el salario neto, etc. La comprobación del correcto funcionamiento de esos algoritmos hace años era sencilla mediante pruebas de detalle con el uso de calculadoras y posteriormente con hojas de cálculo; actualmente se pueden comprobar de forma masiva (el 100% de los elementos) con el uso de herramientas tipo ACL/IDEA.

La auditoría de estos algoritmos y controles "tradicionales", integrados en los procesos de gestión auditados, es ampliamente tratada en las GPF-OCEX existentes.

Conforme la tecnología avanza, los algoritmos se han ido haciendo más complejos y actualmente es habitual en el sector público que los procesos de gestión incorporen **actuaciones administrativas automatizadas, automatizaciones de procesos mediante robotización** y otro tipo de automatizaciones complejas.

En este contexto, resulta indispensable contar, además de con personal especializado en TI, con orientaciones técnicas, procedimientos de auditoría claros y sistemáticos que permitan afrontar estos desafíos con rigor técnico y adaptabilidad que esta guía pretende cubrir.

Además, en los últimos años ha crecido el uso de **tecnologías emergentes**, incluyendo la IA generativa, que, de acuerdo con la IAASB[1], tienen una o más de las siguientes características:

- Opacidad: la lógica de la herramienta o el proceso para tomar decisiones no es transparente (a veces denominado de caja negra).
- No determinismo: los mismos inputs pueden producir resultados diferentes debido a procesos probabilísticos, sensibilidad al contexto u otras influencias impredecibles.
- Adaptabilidad: la herramienta evoluciona con la interacción con el usuario, actualizaciones o reaprendizaje.

Estas tecnologías emergentes, que a los efectos de esta guía agrupamos dentro del concepto de inteligencia artificial (**IA**), tienen unas características disruptivas y exceden su finalidad, es decir, no son objeto de la guía aquellos sistemas, metodologías o herramientas que empleen IA que produzcan resultados no deterministas.

Conscientes de esta realidad, la Comisión Técnica de los OCEX ha elaborado el presente documento que pretende ayudar al auditor de los OCEX a establecer un marco conceptual y metodológico para realizar fiscalizaciones de determinados procesos automatizados.

Los criterios establecidos en esta guía son coherentes con el marco establecido por las GPF-OCEX y las NIA-ES-SP. Con carácter previo a la lectura de esta guía deben leerse y comprenderse las GPF-OCEX 1315 Revisada, 5330, 5340, 5370, 1503, 1957, 1961, 1962, 1964 y 1971, y las NIA-ES-SP 1330 y 1500.

La presente guía se elabora **para complementar las GPF-OCEX existentes** con orientaciones más específicas sobre determinado tipo de automatizaciones.

[1] IAASB Technology Quality Management Roundtables-Briefing Note for Participants, 20/8/2025.

2. Objetivo y ámbito de aplicación de la guía

Esta guía tiene como finalidad proporcionar orientaciones para llevar a cabo auditorías de procesos o sistemas automatizados, que incluyan actuaciones administrativas automatizadas, automatizaciones de procesos mediante robotización software y otro tipo de automatizaciones similares**,** de acuerdo con la metodología recogida en las GPF-OCEX.

Su objetivo es ayudar a:

- Comprender en qué consisten las herramientas y técnicas más frecuentemente utilizadas en la automatización de procedimientos y procesos, así como comprender los conceptos básicos relacionados con estos sistemas.
- Identificar los principales riesgos asociados a los procesos automatizados.
- Identificar los controles internos que hacen frente a estos riesgos.
- Diseñar los procedimientos adecuados para realizar una auditoría de un proceso automatizado.

El ámbito de aplicación de esta guía son las auditorías en las que se revisan procesos de gestión que incluyen:

- **Actuaciones administrativas automatizadas implantadas por las administraciones públicas**
- **Automatizaciones de procesos mediante robotización implantadas por cualquier entidad del sector público.**

En otros procesos automatizados similares que pudieran presentarse en una auditoría se aplicarán los criterios establecidos en esta guía.

No son objeto de la guía aquellos sistemas, metodologías o herramientas que empleen inteligencia artificial que produzcan resultados no deterministas.

3. Definiciones y conceptos básicos

3.1 Definiciones

Debe tenerse en cuenta que determinados conceptos relacionados con las tecnologías emergentes están en continua evolución y no siempre coincide su significado si se consultan distintas fuentes. No obstante, a los efectos de la presente guía, los siguientes términos tienen los significados que se indican:

a) ***Actuación administrativa automatizada (AAA):*** **es un concepto jurídico**, necesita base legal y produce un acto administrativo válido (con firma/sello electrónico); consiste en cualquier acto o actuación administrativa realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público (artículo 41 de la Ley 40/2015).

En la práctica, una AAA puede estar soportada técnicamente por un algoritmo no complejo, por una RPA o por una combinación de ambos.

b) ***Algoritmo***: conjunto limitado de pasos, instrucciones o reglas bien definidas que se utilizan para resolver un problema o realizar una tarea específica. Debe ser preciso, ejecutable y garantizar un resultado en un tiempo determinado. Un algoritmo puede ser leído y entendido por un humano.

Pueden ser **algoritmos no complejos**, que funcionan siguiendo un conjunto limitado de reglas o instrucciones, totalmente predecibles en su comportamiento y no abordan tareas que requieren

razonamiento o aprendizaje, o bien pueden alcanzar un **alto grado de complejidad** incluyendo inteligencia artificial. Últimamente se tiende a utilizar el término "algoritmo" como sinónimo de IA, lo cual no es muy exacto y se debería referir estos casos como "**algoritmo de inteligencia artificial**".

c) ***Analítica de datos***: es el proceso de transformar grandes volúmenes de datos en información útil para la toma de decisiones o para la auditoría.

d) ***Automatización o proceso automatizado:*** acción que ocurre automáticamente dentro de una aplicación informática para hacer que una tarea o un conjunto de tareas se realicen sin necesidad de intervención humana. Hace referencia al desarrollo de código para realizar tareas repetitivas y basadas en reglas. No genera por sí mismo un acto administrativo.

La automatización o proceso automatizado está diseñada mediante un algoritmo, puede ser básica, o puede alcanzar un alto grado de complejidad.

Los términos de algoritmo y automatización suelen ser utilizados indistintamente, aunque son conceptos distintos. El algoritmo indica "qué hacer y cómo", la automatización es "hacerlo automáticamente".

e) ***Automatización cognitiva***: es el siguiente nivel de la automatización tradicional. En lugar de limitarse a tareas repetitivas y estructuradas, esta tecnología permite que los sistemas automatizados interpreten, aprendan y tomen decisiones complejas, imitando ciertas capacidades humanas (escuchar, hablar, ver, leer y comprender el texto). Puede combinar varias tecnologías avanzadas:

- Inteligencia Artificial: para simular el razonamiento humano.
- Aprendizaje automático: para aprender de los datos y mejorar con el tiempo.
- Procesamiento de lenguaje natural: para entender textos, correos, chats, etc.
- Visión por computadora: para analizar imágenes o vídeos.
- Reconocimiento óptico de caracteres: para extraer información de documentos escaneados

Automatización inteligente: este término se utiliza muchas veces de forma indistinta con el de automatización cognitiva por la literatura técnica.

f) ***Big Data:*** conjuntos de datos masivos y complejos que los sistemas tradicionales de gestión de datos no pueden manejar. La llegada de Internet y otras tecnologías conectadas aumentó significativamente el volumen y la variedad de datos disponibles, dando origen al concepto de "Big Data". La ciencia de datos y, más específicamente, el análisis de Big Data ayudan a las organizaciones a dar sentido a los grandes y diversos conjuntos de datos.

Los datos tradicionales y el Big Data difieren principalmente en los tipos de datos involucrados, la cantidad de datos manejados y las herramientas necesarias para analizarlos. Los primeros consisten principalmente en datos estructurados almacenados en bases de datos relacionales que los organizan en tablas claramente definidas, lo que facilita la consulta mediante herramientas estándar como SQL.

El Big Data, por su parte, engloba conjuntos de datos masivos en diversos formatos, incluidos datos estructurados, semiestructurados y no estructurados. Esta complejidad exige enfoques analíticos avanzados, como el *machine learning*, la analítica de datos y la visualización de datos, para descubrir patrones, extraer conocimientos y predecir resultados.

g) ***Código fuente:*** representación/implementación en un lenguaje de programación de un algoritmo con el fin de que un ordenador/sistema realice la tarea o resuelva el problema que el algoritmo especifica. El código fuente es entendible por las máquinas y los humanos.

h) ***Robot o robot software o bot***: programa informático que ejecuta tareas específicas siguiendo un conjunto de instrucciones o reglas predefinidas y cuyo objetivo principal es realizar procesos de forma eficiente, precisa y sin intervención humana directa. Pueden interactuar con interfaces de usuario, bases de datos y otros sistemas para realizar operaciones como la recopilación, procesamiento y transferencia de información.

i) ***Automatización robótica de procesos (RPA por sus siglas en inglés):*** algoritmos para ejecutar tareas repetitivas y estructuradas, como la introducción de datos o la integración de sistemas, simulando acciones humanas en entornos digitales, en sistemas y aplicaciones existentes. Aunque un RPA puede ser creado escribiendo el código directamente, atendiendo a criterios de complejidad, mantenimiento, escalabilidad y compatibilidad, también se pueden utilizar herramientas específicas comerciales.

   Un RPA puede estar integrado y formar parte de una AAA o no.

j) ***Inteligencia artificial (IA):*** aunque no existe una definición formal y universalmente aceptada, la Comisión Europea define la inteligencia artificial como un campo de la informática que se enfoca en crear sistemas que puedan realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento y la percepción. Estos sistemas pueden percibir su entorno, razonar sobre el conocimiento, procesar la información derivada de los datos y tomar decisiones para lograr un objetivo dado.

   El reglamento de IA define ***sistema de IA*** como el sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

k) ***Aprendizaje automático (Machine Learning)***: es una rama de la IA que se centra en que las máquinas aprendan de los datos y puedan tomar decisiones o hagan predicciones sin ser explícitamente programados para cada tarea, mediante el uso de algoritmos y el entrenamiento a partir de conjuntos de datos y con cierto nivel de intervención humana en el aprendizaje.

l) ***Aprendizaje profundo (Deep Learning):*** es un subconjunto del aprendizaje automático que utiliza algoritmos de redes neuronales artificiales para procesar grandes cantidades de datos (incluso datos sin estructura) e imitar el proceso de aprendizaje del cerebro humano, eliminando gran parte de la intervención humana necesaria en el aprendizaje.

m) ***Inteligencia artificial generativa***: rama/subcampo de la IA que se enfoca en la generación de contenido nuevo (textos, imágenes, sonidos, código de programación, etc.) de forma autónoma a partir de datos existentes.

n) ***Agente IA:*** Son programas autónomos basados en inteligencia artificial, capaces de percibir su entorno (con sensores, datos, etc.) y actuar sobre él (con actuadores o decisiones). Buscan cumplir objetivos adaptándose a cambios en el entorno.

o) ***Procesamiento del lenguaje natural (PLN):*** campo de la IA que estudia las interacciones entre computadoras y el lenguaje humano. Emplea técnicas de aprendizaje automático para procesar e interpretar textos y datos.

p) ***Reconocimiento del habla:*** el reconocimiento del habla permite procesar el habla y convertirla en texto legible con un alto grado de precisión, utilizando distintas técnicas de IA.

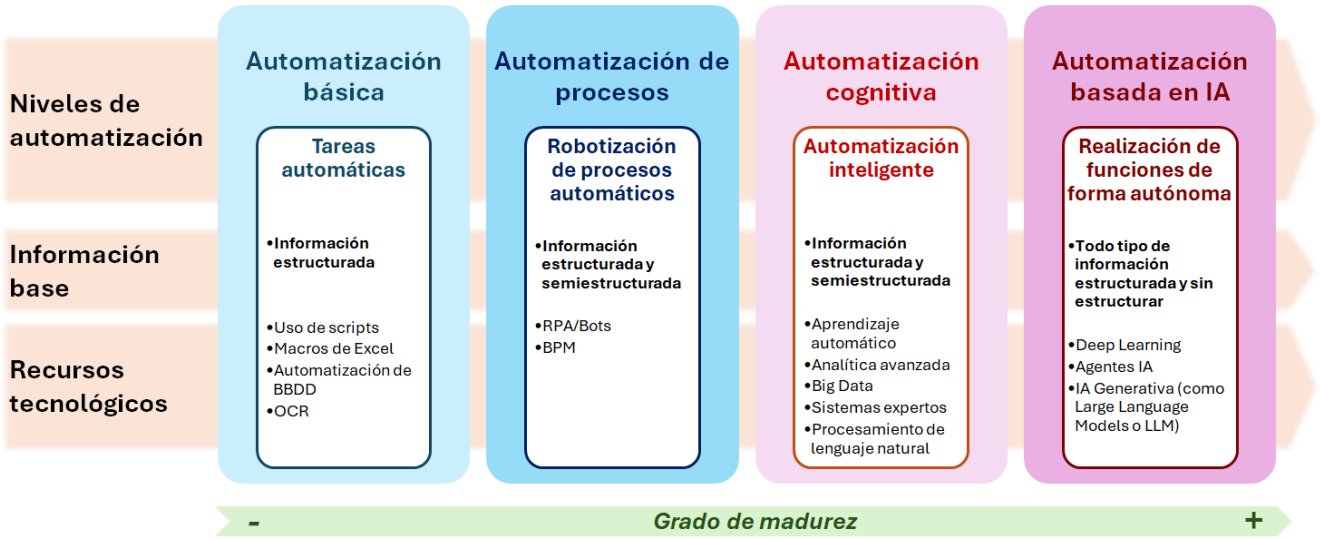
q) ***Sistemas expertos:*** son programas capaces de tomar decisiones y resolver problemas complejos de gran esfuerzo para una persona. Un sistema experto está especializado en dar respuesta a un problema concreto al igual que haría una persona con conocimiento y experiencia de la materia.

r) ***Tratamiento inteligente de documentos (IDP, Inteligent Document Processing)***: esta tecnología permite tratar de forma automatizada los documentos para la extracción y/o cotejo de información, aplicando inteligencia artificial, como el aprendizaje automático para esta tarea.

3.2 Tipos de automatizaciones

Algunos autores han realizado el ejercicio de categorizar los distintos tipos de procesos automatizados o automatizaciones según su grado de avance tecnológico y características. Distinguen cuatro etapas secuenciales que representan un continuo de madurez tecnológica: **automatización básica, automatización de procesos, automatización cognitiva** y, finalmente, **automatización basada en IA**.

Intentando simplificar un panorama complejo, se puede representar gráficamente[2] así:



En el primer grupo, **automatización básica**, se abordan tareas repetitivas mediante el uso de tecnologías simples como macros de Excel, scripts y automatización de bases de datos. Esta etapa opera sobre información estructurada. Las ventajas que ofrece son claras: ahorro de tiempo, reducción de errores, mejora de la eficiencia y estandarización de tareas.

El segundo, **automatización de procesos**, implica una mayor sofisticación técnica mediante la robotización de procedimientos o la gestión de procesos de negocio. Esta automatización es capaz de gestionar información estructurada y semiestructurada. Con estas tecnologías se pueden modelar flujos administrativos completos e integrar distintos sistemas entre sí, por ejemplo, utilizando interfaces de programación de aplicaciones (APIs por sus siglas en inglés), logrando una reducción del tiempo de procesamiento y una mejora de la trazabilidad. Ejemplos típicos incluyen la tramitación automatizada

[2] Vease Javier Requejo García en *La inteligencia artificial al servicio del órgano interventor: casos de uso en el sector local*, Revista Auditoría Pública nº 85 Junio 2025. También Carmen Montserrat Querol expone una clasificación similar en sus cursos sobre *Trabajos de auditoría aplicando herramientas de inteligencia artificial y herramientas avanzadas para optimizar procesos*, citando una presentación de la Agencia Tributaria Catalana. El gráfico está elaborado a partir de ambos autores.

de solicitudes, la integración de expedientes digitales entre plataformas o la validación cruzada de datos entre registros administrativos.

Ambos tipos de automatización comparten una lógica transparente y predecible, lo que facilita su trazabilidad y revisión por parte del auditor. La fiscalización de estos sistemas exige verificar el diseño del algoritmo, los controles de calidad, la documentación técnica y la coherencia normativa del procedimiento automatizado.

El tercero, **automatización cognitiva**, introduce capacidades de análisis y toma de decisiones mediante el uso de aprendizaje automático, Big Data y procesamiento del lenguaje natural. Las ventajas incluyen una mejora en la toma de decisiones, detección proactiva de irregularidades, optimización de recursos y enriquecimiento de los análisis.

La etapa final corresponde a la **automatización basada en IA**, caracterizada por el uso de *deep learning*, grandes modelos de lenguaje LLM y agentes IA. Esta fase no está limitada por el tipo de información.

Las dos primeras fases incluyen herramientas claramente deterministas y las dos siguientes fases del proceso introducen modelos no deterministas.

En la práctica, sin embargo, dado que actualmente existen en el mercado cientos de herramientas, que crecen y evolucionan cada día, podremos encontrarnos herramientas "híbridas" que será difícil encajar en un esquema tan simple como el anterior, o el del apartado 3.2, los cuales tienen una función meramente didáctica. En esos casos habrá que emplear el juicio y escepticismo profesional para determinar frente a qué tipo de herramienta o proceso de automatización nos encontramos y qué consecuencias tiene sobre los riesgos, los procedimientos de auditoría a aplicar y las evidencias de auditorías que se pueden obtener.

Podemos auditar procesos sencillos, como el de concesión de subvenciones, donde puede ser sencillo "clasificar" el tipo de automatización utilizada.

En otros casos, frecuentes, se deberá auditar una entidad que opera un ERP financiero complejo, con múltiples módulos interconectados, formado por cientos de automatizaciones que individualmente consideradas se pueden calificar como "básicas" pero que en conjunto forman un sistema de elevada complejidad. Es probable que alguno de esos módulos disponga, por ejemplo, de procesos de cálculos nocturnos que se encargan de recopilar información, realizar operaciones complejas, emitir un informe y enviarlo a los responsables, que calificaríamos como "automatización de procesos". También podría incluir, cada vez será más frecuente, algún subproceso concreto que incorpore aprendizaje automático para predecir tendencias futuras o algún otro tipo de IA.

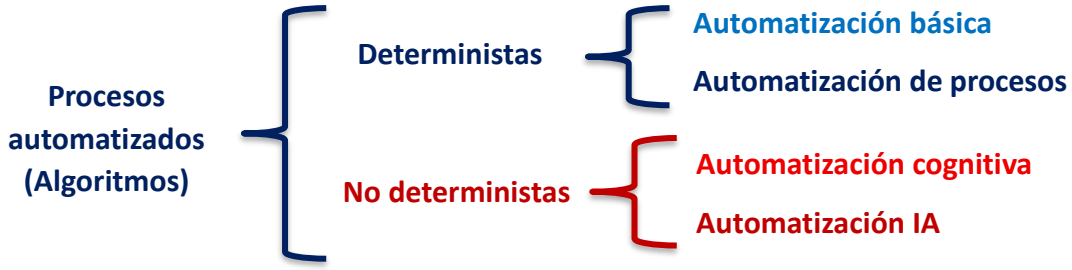
3.3 Diferencia entre la IA generativa y los algoritmos no complejos

La IA generativa es una categoría de sistemas de IA **capaces de producir contenido nuevo**, como texto, imágenes, datos, código o audio, basados en el entrenamiento a partir de grandes volúmenes de datos. A diferencia de las herramientas informáticas tradicionales que siguen reglas codificadas, las herramientas de IA generativa "aprenden" relaciones estadísticas y generan resultados novedosos y adaptables. Estos sistemas a menudo se basan en redes neuronales, particularmente en grandes modelos de lenguaje (LLM), que codifican patrones a partir de datos de entrenamiento y generan respuestas basadas en distribuciones de probabilidad en lugar de reglas deterministas.

La siguiente tabla refleja las diferencias en tres atributos distintivos entre la IA generativa y los algoritmos no complejos:[3]

Características	Herramientas de IA generativa	Algoritmos no complejos
Determinismo	**No determinista**: la misma entrada puede producir diferentes salidas (porque el modelo utiliza procesamiento probabilístico, responde a cambios sutiles de contexto o tiene otras influencias impredecibles).	**Determinista**: la misma entrada produce una salida consistente.
Transparencia lógica	A menudo **opaco** ("caja negra"); La toma de decisiones interna puede ser difícil de interpretar o rastrear: la lógica y las vías de decisión no son completamente visibles o explicables.	**Transparente y basado en reglas**; La lógica se puede documentar y revisar.
Adaptabilidad	**Puede actualizarse o evolucionar** con el tiempo a través del reentrenamiento, las actualizaciones basadas en la nube o las interacciones del usuario con cambios de funcionalidad sin reprogramación explícita.	**Lógica y comportamiento fijos** a menos que se reprogramen explícitamente.

Utilizando el criterio del determinismo se puede visualizar, para mayor claridad, la clasificación de los distintos tipos de automatizaciones como sigue:



Naturalmente, esta es una clasificación básica de las principales herramientas existentes actualmente para distinguir los dos grandes grupos, que tienen riesgos diferentes, y resulta útil para la presente guía.

4. Las actuaciones administrativas automatizadas (AAA)

4.1 Qué son las AAA

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público consolida jurídicamente el concepto de administración electrónica y define el concepto, que ya se regulaba en la Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, de **actuación administrativa automatizada,** señalando en su artículo 41.1 que:

Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.

[3] IAASB Technology Quality Management Roundtables. BRIEFING NOTE FOR PARTICIPANTS, August 20, 2025.

El apartado 2 del mismo artículo añade que *en caso de actuación administrativa automatizada* ***deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.***

Los artículos 41 y 42 de la Ley 40/2015 han sido desarrollados por el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, fundamentalmente en materia de identificación y firma de los distintos agentes.

Adicionalmente, las comunidades autónomas han regulado, para su ámbito competencial, distintos aspectos de la aplicación de las AAA[4]. En esta guía solo mencionaremos aquellos aspectos que tengan un interés general.

No cabrá realizar mediante actuación administrativa automatizada actividades que supongan juicios de valor. Es decir, las AAA se referirán a actos absolutamente reglados, cuya producción es predeterminada a través de un sistema automático, que simplemente comprueba la concurrencia de los supuestos de hecho determinantes de dicha producción.

La actividad administrativa también puede ser de carácter discrecional. La discrecionalidad es una facultad netamente humana, que otorga flexibilidad y adaptabilidad a cada caso, lo que es incompatible con las AAA. La obligación de motivar los actos administrativos impuesta por el artículo 35 de la Ley 39/2015 se ve reforzada para los actos discrecionales, requiriendo un mayor celo para justificar la decisión, que los procesos automatizados no son capaces de hacer.

En síntesis, **las AAA solo pueden implementarse en aquellos procedimientos basados en reglas claramente definidas y transparentes, que generen actos administrativos** que no dejen lugar a la interpretación y donde **la motivación esté predefinida por simples reglas matemáticas**, donde las decisiones son el resultado de la aplicación de criterios previamente establecidos por la Administración. Resultaría muy complicado, o directamente inviable, emitir mediante una AAA un acto de cese de

[4] Por ejemplo, el artículo 40. Actuación administrativa automatizada del DECRETO 54/2025, de 15 de abril, del Consell de la Generalitat Valenciana, establece:

1. La actuación administrativa automatizada permitirá realizar íntegramente actos o actuaciones administrativas por medios electrónicos, sin necesidad de intervención de forma directa de una persona empleada pública.
   Cuando las actuaciones administrativas automatizadas produzcan efectos jurídicos en las personas físicas se garantizará el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado, en los términos previstos en el artículo 22 del Reglamento (UE) 2016/679.
2. Las actuaciones administrativas automatizadas se autorizarán por resolución de la persona titular del órgano administrativo competente por razón de la materia según corresponda, que **se publicará** en la Sede PROP o en la sede electrónica asociada con el siguiente contenido:
   a) El detalle de los actos o actuaciones a automatizar.
   b) El mecanismo de firma a emplear, de entre los recogidos en la Política de identificación y firma electrónica de la Generalitat y el lugar en que poder verificar dicha firma.
   c) El órgano o los órganos competentes para la definición de las especificaciones, la programación, el mantenimiento, la supervisión y el control de calidad.
   d) **El órgano encargado de auditar el sistema de información y su código fuente**.
3. El órgano competente del acto o actuación a automatizar será el responsable ante las eventuales impugnaciones.
4. **Los órganos encargados de auditar las actuaciones administrativas automatizadas serán la Intervención general, en el ámbito de la Administración de la Generalitat, y sus análogos en el resto de las entidades del sector público instrumental**, en los términos de la normativa reguladora en materia de hacienda y sector público.

personal nombrado por libre designación. En estos casos la motivación debe ser muy clara y específica para el caso concreto, lo que hoy por hoy un algoritmo no tiene permitido hacer.

4.2 Auditoría previa de las AAA realizada por las intervenciones generales.

Dentro del ámbito estatal, la Disposición final octava, siete, de la Ley 36/2014, de Presupuestos Generales del Estado para el año 2015, modificó la Ley 47/2003, de 26 de noviembre, General Presupuestaria (LGP) dando nueva redacción al apartado 2 del artículo 142 sobre el control a realizar por parte de la IGAE de la gestión económico-financiera del sector público estatal, que quedó redactado como sigue:

> "2. El control se realizará mediante el ejercicio de la función interventora, el control financiero permanente y la auditoría pública, a que se refieren los capítulos II, III y IV de este título.
>
> No obstante, **cuando de acuerdo con la normativa aplicable, los procedimientos objeto de control se instrumenten y formalicen en resoluciones o actos a través de actuaciones administrativas automatizadas**, …, la Intervención General de la Administración del Estado podrá aprobar las normas necesarias para adaptar los distintos controles previstos en este título a las especialidades derivadas de este tipo de actuaciones, mediante Resolución publicada en el Boletín Oficial del Estado.
>
> En todo caso, **con carácter previo a la aprobación de las normas reguladoras de los citados procedimientos de gestión, se requerirá la realización de una auditoría previa** de la Intervención General de la Administración del Estado, en los términos y forma que determine dicho centro directivo, **para verificar** que el nuevo procedimiento de gestión incorpora l**os controles automatizados de gestión** necesarios a la naturaleza del mismo, satisface**, a efectos de la función interventora, los requerimientos de seguridad** que correspondan a la categoría del respectivo sistema de información, de acuerdo con el **Esquema Nacional de Seguridad vigente en cada momento, y se ajusta a los términos establecidos en el** artículo 39 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (*actualmente artículo 41.2 de la Ley40/2015*).
>
> Cuando del informe de auditoría se derive el **incumplimiento** de las especificaciones del sistema de información o la detección de **deficiencias graves**, estos incumplimientos o deficiencias deberán ser solventados por el órgano u órganos competentes antes de la aprobación de la norma por la que se establezca la actuación automatizada.
>
> Se efectuarán **revisiones de la auditoría inicial**, de acuerdo con lo que se prevea al respecto en los planes anuales de auditorías de la Intervención General de la Administración del Estado. Cuando del resultado de la auditoría se deduzca el incumplimiento de las especificaciones aprobadas o la detección de deficiencias graves, el Interventor General concederá un plazo para su adaptación que, en el caso de no ser atendido, suspenderá la utilización de la aplicación. No obstante, el Interventor General, a la vista de la naturaleza del defecto y de las circunstancias concurrentes, podrá acordar la suspensión inmediata de la utilización de la aplicación a los efectos señalados. Todo ello, sin perjuicio de las actuaciones de revisión de los sistemas informáticos de gestión económico-financiera a desarrollar en el ámbito del control financiero permanente y la auditoría pública."

En relación con el control de las AAA, las comunidades autónomas también han legislado, de forma muy similar, para atribuir esas competencias a sus respectivas intervenciones generales.

En resumen, el artículo 142.2 de la LGP y normativa concordante de las comunidades autónomas configura la auditoría pública como un mecanismo específico de control interno para las AAA, estructurando su aplicación en dos momentos complementarios, mediante la realización de una auditoría previa a la aprobación de las normas reguladoras del procedimiento automatizado, y a través de auditorías posteriores a la puesta en marcha de la actuación automatizada.

4.3 Otras actuaciones de las intervenciones sobre las AAA

A modo solamente de ejemplo, resulta de interés conocer cómo fiscalizan algunas intervenciones generales las AAA:

- La Disposición Adicional 3ª de la Ley 3/2023, de 16 de marzo, de medidas fiscales, financieras, administrativas y del sector público para el 2023 de Cataluña regula la **fiscalización previa automatizada** de la siguiente forma: *En los casos en que los sistemas informáticos den seguridad jurídica a lo establecido por la normativa y a la correspondiente anotación contable puede establecerse la fiscalización previa automatizada, que es la realizada íntegramente por medios electrónicos, y, por tanto, sin la actuación de personal del Cuerpo de Intervención de la Generalitat.*
- También resulta de interés el artículo 102.4 del Texto Refundido de la Ley de Hacienda de Castilla-La Mancha, por el que se autoriza la sustitución de la función interventora por el control financiero permanente en los expedientes de gasto vinculados a la concesión de subvenciones públicas o al reconocimiento de obligaciones derivadas de ellas, **siempre que dichos procedimientos se ejecuten mediante actuaciones administrativas automatizadas**.

4.4 Objetivos específicos de la auditoría del AAA realizada por un OCEX

En determinados casos, un OCEX deberá verificar el buen funcionamiento de una AAA existente en un procedimiento administrativo que esté fiscalizando y el cumplimiento con las normas que lo regulan.

Los objetivos de la auditoría podrán ser los siguientes, que incluyen la verificación del cumplimiento del artículo 41 y 42 de la Ley 40/2015:

1) **Verificar que la AAA incorpora todos los pasos y los controles de gestión necesarios, adecuados a la naturaleza del procedimiento.**

   Para ello se requiere la realización de una auditoría del sistema de información que incluya, entre otros aspectos, un análisis de la AAA y sus controles, para verificar que la AAA se ajusta a las especificaciones técnicas y a la normativa aplicable, de su adecuada implementación y la verificación de la eficacia operativa.

   Por ejemplo, en un procedimiento de ayudas económicas, entre otros aspectos, debe comprobarse que el sistema permita la presentación de solicitudes, el estudio, la calificación o valoración, la verificación del cumplimiento de los requisitos legales y el reconocimiento del derecho, así como la generación de resoluciones automatizadas, su firma electrónica y la corrección de los valores reflejados en ellas. Asimismo, debe permitir evaluar si los controles automatizados identificados garantizan efectivamente el cumplimiento normativo en cada fase del procedimiento, el diseño de los flujos de decisión y del procedimiento administrativo, así como su integración con otros sistemas y fuentes de datos externas (interfaces internas y externas).

2) **Comprobar que la AAA satisface los requerimientos de seguridad que correspondan a la categoría del respectivo sistema de información, de acuerdo con el Esquema Nacional de Seguridad (ENS).**

Se debe evaluar si la AAA satisface los requerimientos de seguridad aplicables en función de la categoría del sistema de información correspondiente, de acuerdo con lo establecido en el ENS. En definitiva, se trataría de una auditoría de sistemas de información focalizada en los controles de seguridad (**CGTI**[5]). Tales comprobaciones podrían sustituirse por la correspondiente certificación del ENS de los sistemas implicados.

En la sentencia del Tribunal Supremo antes citada se indica que la transparencia del algoritmo puede contribuir a la mejora del código y al fortalecimiento de su seguridad puesto que la entrega del código fuente a personas y organizaciones legitimadas para auditarlo permitiría identificar posibles vulnerabilidades y ayudar a su corrección.

3) **Verificar que se ha establecido previamente el órgano u órganos competentes**, según los casos, para (artículo 41 de la Ley 40/2015):
   - la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad,
   - la auditoría del sistema de información y de su código fuente, y
   - ser considerado responsable de la AAA a efectos de impugnación.
4) **Verificar que el sistema de firma para la AAA sea acorde con el artículo 42 de la Ley 40/2015.**
5) **Comprobar si la intervención general correspondiente ha realizado las auditorías previas** de la AAA que establece la normativa y si, en su caso, las recomendaciones realizadas fueron adoptadas.
6) **Comprobar la existencia de trazabilidad completa en el proceso automatizado.** Verificar que el sistema ha sido diseñado para ser auditado y conserva pistas de auditoría suficientes para reconstruir las decisiones automatizadas, así como los datos que sirvieron de base para la toma de esa decisión en registros inalterables.

   Cuando se trate de AAA u otros algoritmos que decidan dar ayudas o beneficiar a unos u otros, deberán ser auditables, ya que la trazabilidad y el acceso al funcionamiento interno del sistema resultan esenciales para garantizar la fiscalización y la defensa de los derechos de la ciudadanía. En esta la línea, la sentencia del Tribunal Supremo del 11 de septiembre de 2025[6] establece que el software utilizado por la Administración constituye información pública a efectos de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
7) **Verificar la vigencia y coherencia de la documentación técnica y funcional y detectar en su caso modificaciones que debieron ser objeto de auditoría previa.** Puede que el documento de especificación de requisitos, modelo de datos o código fuente hayan dejado de ser coherentes con la resolución que regula la AAA o con la propia normativa reguladora del procedimiento.
8) Además, en cada OCEX, se revisará la normativa que en cada caso corresponda.

[5] Será de aplicación la GPF-OCEX 5330.

[6] https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Noticias-Judiciales/ci.El-Tribunal-Supremo-condena-a-la-Administracion-a-facilitar-a-una-Fundacion-Ciudadana-el-codigo-fuente-de-la-aplicacion-informatica-que-acredita-a-los-beneficiarios-del-bono-social-electrico.formato2

4.5 Riesgos de auditoría

En el apartado 9 puede verse un listado de los riesgos más frecuentes que debe considerar el auditor.

4.6 Ejemplos

Entre las funcionalidades que pueden tener las AAA, están todas aquellas actividades que puedan producirse mediante un sistema de información adecuadamente programado sin necesidad de intervención directa de una persona empleada pública en cada caso singular, por ejemplo, las que consistan en[7]:

- La adopción de un acuerdo administrativo mediante la aplicación de fórmulas matemáticas y otros procesos puramente mecánicos en los que se utilicen valores cuantificables y susceptibles de ser expresados en cifras y/o porcentajes.
- La certificación de hechos o datos preexistentes en registros o en sistemas de información, incluso del silencio administrativo.
- La constatación puramente mecánica de requisitos previstos en la normativa aplicable y la posterior declaración, en su caso, de la consecuencia jurídica prevista en la misma.
- La comunicación o declaración de un hecho, acto o acuerdo preexistente a través de su transcripción total o parcial.
- La práctica de las notificaciones electrónicas.

Algunos ejemplos de actividades administrativas automatizadas:

- Gestión de subvenciones: las plataformas digitales permiten que los ciudadanos presenten solicitudes online, pudiendo automatizarse desde validaciones para la comprobación de los requisitos hasta la emisión de la resolución de la subvención.
- Comprobación automática de ciertos requisitos: estar al corriente de obligaciones fiscales y tributarias, comprobación de la cuenta bancaria, etc.
- Alta de terceros para el pago de obligaciones en las administraciones públicas.
- Procedimientos de concesión de pensiones.
- Emisión de certificados administrativos: empadronamiento, certificados de calificación sanitaria, notas en las pruebas de acceso a la universidad, participación en acciones formativas, certificados de la JQCV, certificado COVID Digital UE …
- Publicaciones en tablones electrónicos de anuncios y edictos.
- Generación de liquidaciones tributarias y cartas de pago (cálculo y emisión de tasas y tributos).

[7] Véase el artículo 40 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.

5. La automatización de procesos mediante robotización (RPA)

5.1 Qué son los RPA

La automatización robótica de procesos es una de las tendencias más importantes en la transformación digital, ya que permite cambiar radicalmente la manera en que las organizaciones gestionan sus procesos internos, mejorando la eficiencia, reduciendo costes y permitiendo a los empleados centrarse en tareas de mayor valor.

Es una tecnología de software que utiliza robots para automatizar tareas repetitivas y basadas en reglas que normalmente realizan los seres humanos. Estos robots pueden estar programados para interactuar con personas y con aplicaciones y sistemas de la misma manera que lo haría una persona, ejecutando tareas como la entrada de datos, la generación de informes, el procesamiento de transacciones, entre otras.

Los RPA imitan los pasos que realiza el humano frente a la pantalla del ordenador. Se suelen programar para que realicen los movimientos de ratón, pulsaciones de teclado o copiado y pegado de información con entrenamiento demostrativo, aunque también puede hacerse con programación de código. En el primer caso significa que hay que grabar los movimientos y tareas que se quieren automatizar.

El RPA puede estar programado para interactuar con cualquier sistema o aplicación para realizar tareas digitales repetitivas, como copiar y pegar, extraer datos web, realizar cálculos, abrir y mover archivos, analizar correos electrónicos, iniciar sesión en programas y conectarse mediante interfaces de programación de aplicaciones (API por sus siglas en inglés) u otro tipo de conexiones.

Las primeras versiones de RPA se centraron en la automatización de tareas simples, como los procesos relacionados con la entrada de datos. Con el tiempo, la tecnología ha evolucionado para incluir capacidades más avanzadas lo que permite a los robots realizar tareas más complejas.

Se pueden encontrar los siguientes tipos de RPA:

RPA desatendida: funciona de manera autónoma, sin intervención humana. Se utiliza para tareas repetitivas y predecibles. Los bots desatendidos se activan por eventos específicos o se ejecutan en momentos predeterminados.

RPA asistida: los robots asistidos trabajan junto a los empleados, ayudándoles en tareas que requieren intervención humana. Por ejemplo, un profesional del servicio al cliente puede usar estos robots durante una llamada para procesar información rápidamente. Estos robots se activan por el usuario y pueden requerir decisiones humanas en ciertos pasos.

RPA híbrida: combina elementos de RPA desatendida y asistida. Los robots híbridos pueden trabajar de manera autónoma en ciertas tareas y requerir intervención humana en otras. Este tipo de RPA es útil en procesos complejos que necesitan flexibilidad y adaptabilidad.

5.2 Ventajas del uso de los RPA

La adopción de RPA ofrece una serie de beneficios significativos en la gestión de procesos. A continuación, se detallan algunos de los más importantes[8]:

- Reducción de costes: uno de los principales beneficios de la adopción de la RPA es la reducción de costes laborales. Los RPA pueden realizar tareas que normalmente requerirían varios empleados, lo que permite replantear de las plantillas asignadas a los departamentos.

[8] La automatización robótica de procesos en el Departamento de Intervención de la Diputación de Girona, Nuria Josa Arbones/ Inma Molas Pujol, Revista de estudios Locales - CUNAL 277, 2024.

- Mejora de la eficiencia: los robots de RPA pueden trabajar las 24 horas del día, los 7 días de la semana, sin necesidad de descansos. Esto permite completar las tareas más rápidamente y con una mayor precisión que si fueran realizadas por humanos.
- Eliminación de errores humanos: las tareas repetitivas y basadas en reglas son propensas a errores cuando son realizadas por humanos. Los robots de RPA, por otro lado, pueden realizar estas tareas con una precisión prácticamente perfecta, reduciendo la probabilidad de errores.
- Aumento de la productividad: al automatizar tareas repetitivas, la RPA libera a los empleados para que se concentren en actividades de mayor valor. Esto no solo aumenta la productividad, sino que también mejora el ambiente laboral de los departamentos.
- Escalabilidad: los robots de RPA se pueden escalar fácilmente. A medida que se detectan nuevos procesos a automatizar, se pueden añadir más robots para manejar el aumento de la carga de trabajo sin necesidad de contratar personal adicional.

5.3 Objetivos específicos de la auditoría del RPA realizada por un OCEX

Entre los objetivos de auditoría que pueden plantearse tenemos:

1) Verificar que el RPA incorpora todos los pasos y los controles necesarios, adecuados a la naturaleza del procedimiento.

   Para ello se requiere la realización de una auditoría del sistema de información que incluya, entre otros aspectos, un análisis del RPA y sus controles, para verificar que se ajusta a las especificaciones técnicas y a la normativa interna aplicable, de su adecuada implementación y la verificación de la eficacia operativa.

2) Comprobar que el RPA satisface los requerimientos de seguridad que correspondan a la categoría del respectivo sistema de información, de acuerdo con el Esquema Nacional de Seguridad (ENS).

   Para ello se requiere de una auditoría de sistemas de información focalizada en los controles de seguridad (CGTI[9]). Tales comprobaciones podrían sustituirse por la correspondiente certificación de los sistemas implicados.

3) Verificar que se dispone, y está vigente, la documentación donde se recojan, al menos, lo siguiente:
   - la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad,
   - la auditoría del sistema de información y de su código fuente

4) Comprobar la existencia de trazabilidad completa en el proceso automatizado.

   Comprobar que el sistema ha sido diseñado para ser auditado y conserva pistas de auditoría suficientes para reconstruir las decisiones automatizadas, así como conserva los datos que sirvieron de base para la toma de esa decisión en registros inalterables.

5) Verificar la gobernanza del RPA, segregación de funciones y control del ciclo de vida.

   La falta de separación de entornos y roles incrementa riesgo de cambios no autorizados, errores en producción y fraude. Se pueden revisar políticas y organigrama de responsabilidades; comprobar registros de gestión de cambios, pruebas de integración, firmantes de puesta en producción y control de versiones del código/artefactos.

6) Comprobar cumplimiento de la normativa de protección de datos (RGPD/LOPDGDD): evaluaciones de impacto, minimización, retención y derechos de los interesados aplicados al RPA.

[9] Aplicará la GPF-OCEX 5330.

Los robots procesan grandes volúmenes de datos personales; debe acreditarse una Evaluación de Impacto en la Protección de Datos Personales (EIPD) cuando proceda, medidas de minimización y la trazabilidad de bases jurídicas. Se pueden solicitar evaluaciones de impacto de protección de datos/registro de tratamientos, verificar pseudonimización/anonimización, revisar logs de accesos a datos y políticas de retención.

7) Evaluar la gestión de credenciales, secretos y acceso privilegiado del entorno RPA.

   El acceso de los robots a sistemas críticos suele requerir credenciales privilegiadas —su gestión centralizada y trazada es control clave. Para ello se pueden verificar el uso de gestores de secretos, rotación de credenciales, cuentas por robot nominales, principios de mínimo privilegio y pruebas de acceso y revocación.

8) Verificar monitorización, detección de incidentes, respuesta y continuidad operativa del entorno RPA.

   La resiliencia operativa y la capacidad de detectar y recuperar incidentes en robots es crítica para procesos automatizados a gran escala. Para ello se pueden revisar políticas de monitorización, evidencia de pruebas de recuperación y métricas de disponibilidad; validar registros de incidentes y lecciones aprendidas.

5.4 Riesgos de auditoría

En el apartado 9 puede verse un listado de los riesgos más frecuentes que debe considerar el auditor.

5.5 Ejemplos

En el Anexo 3 se pueden ver los ejemplos 1 y 2 extraídos de informes de fiscalización.

6. Características diferenciales de las AAA y los RPA

Como se ha comentado, una actuación administrativa automatizada (AAA) es un concepto jurídico, donde una administración decide aplicar tecnología para hacer más eficiente un procedimiento administrativo, otorgándole base legal al resultado de este procedimiento y haciéndose responsable éste. La tecnología aplicada puede ser cualquier tecnología determinista, desde un algoritmo simple, un programa informático estándar o una macro en Excel a una más avanzada como una RPA.

En la siguiente tabla se puede ver un resumen de la relación entre estos dos conceptos:

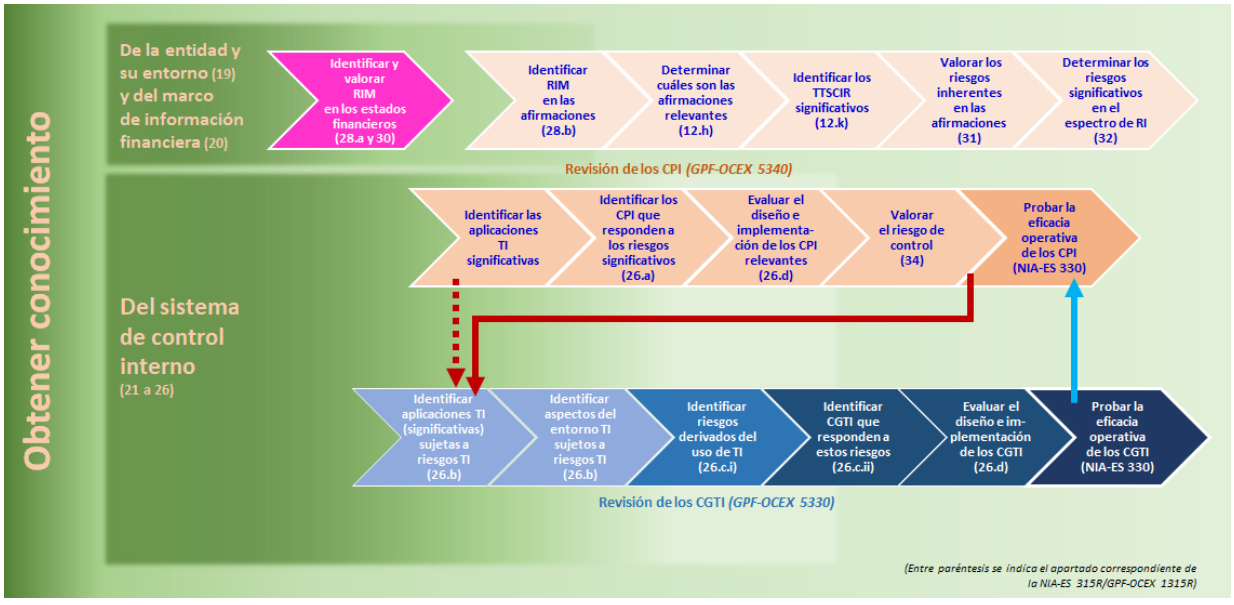
Aspecto	AAA	RPA	Interoperabilidad / Uso combinado
Naturaleza	**Figura jurídica** reconocida en la Ley 40/2015 y en la normativa administrativa	**Tecnología de software** que automatiza tareas repetitivas	Un RPA puede integrarse en una AAA, como parte del flujo técnico previo al acto
Finalidad	Emitir un acto administrativo válido (ej. certificado, licencia, notificación)	Automatizar tareas operativas imitando acciones humanas en sistemas informáticos	El RPA puede preparar datos o validar requisitos que luego se formalizan mediante una AAA o, alternativamente, con intervención humana
Base jurídica	Requiere aprobación previa, sello electrónico o CSV, y trazabilidad normativa	No genera actos jurídicos, pero debe cumplir con normativa de seguridad, protección de datos, etc.	El RPA debe estar alineado con los requisitos legales si se usa en procedimientos administrativos

Aspecto	AAA	RPA	Interoperabilidad / Uso combinado
Valor jurídico	Efectos jurídicos reconocidos conforme a la normativa. Acto administrativo plenamente válido, revisable y con efectos jurídicos	Valor técnico y operativo, no tiene reconocimiento jurídico directo, ni garantías administrativas	El valor jurídico lo aporta AAA o la resolución del órgano administrativo, el RPA es soporte técnico sin capacidad jurídica directa
Intervención humana	No hay intervención humana directa en la emisión del acto, aunque sí en su diseño y supervisión	Sustituye tareas repetitivas, pero requiere configuración y supervisión humana	El RPA ejecuta tareas, AAA o el órgano formaliza el resultado
Ejemplo	Sistema que valida automáticamente requisitos y emite un certificado administrativo	Robot software que extrae datos de formularios y los transfiere a una base de datos o Excel	El robot recopila datos, el sistema AAA o el órgano los valida y emite el certificado sin intervención humana

7. Aspectos generales de la auditoría

La auditoría de un proceso de gestión que incluya una AAA o un RPA no difiere sustancialmente de cualquier auditoría en un entorno de administración electrónica avanzada que, por definición, está formado por múltiples procesos y controles automatizados que el auditor debe conocer y revisar con la metodología establecida en las GPF-OCEX. La circunstancia de que uno de esos procesos o controles automatizados sea un RPA o una AAA no cambia la forma de trabajar, **la metodología de auditoría será la misma**, simplemente habrá que adaptar las pruebas a realizar a las características de la automatización examinada; pero esto hay que hacerlo siempre.

La guía GPF-OCEX 5340 explica la metodología establecida en las NIA-ES-SP y en la GPF-OCEX 1315 Revisada con todo detalle y lo resume en el siguiente flujograma:



Si se va a auditar el área de tesorería o la gestión de las subvenciones, por ejemplo, se utilizarán también las GPF-OCEX 1957 o 1964 respectivamente.

Por tanto, **un resumen del plan de trabajo aplicado para la revisión de un proceso que incluya automatizaciones, con carácter general,** de acuerdo con las GPF-OCEX, sería el siguiente:

a) Obtener **conocimiento** del proceso de gestión que se va a auditar, específicamente las AAA o RPA utilizadas, las aplicaciones y el entorno TI que les dan soporte. (Ver apartado 8).

d) Identificar y valorar los **riesgos** de incorrección material específicos asociados al uso de estas automatizaciones. (Ver apartado 9).

e) Identificar y revisar los **controles de procesamiento de la información** asociados a estos riesgos y diseñar los procedimientos de auditoría para analizar el diseño, la implementación y la eficacia operativa de estos controles. (Ver apartado 10).

f) Identificar y revisar los **CGTI** (controles generales de tecnologías de la información) relevantes relacionados con las AAA o RPA. (Ver apartado 11).

g) Diseñar y ejecutar los **procedimientos posteriores de auditoría** que se consideren precisos de acuerdo con los objetivos de la auditoría (financiera, de cumplimiento u operativa) y con los riesgos identificados y valorados. (Ver apartado 12).

h) Analizar los hallazgos, **extraer conclusiones y recomendaciones**, y elaborar el **informe**. (Ver apartado 13).

i) **Documentar** todos los pasos anteriores.

En la planificación de la auditoría deberá recogerse claramente la metodología que se utilizará para abordar la auditoría del proceso automatizado.

Equipo de auditoría multidisciplinar

Para la realización de fiscalizaciones en entornos de administración electrónica avanzada, con procesos de gestión soportados por aplicaciones informáticas altamente automatizadas, que además cada vez incluyen más frecuentemente el uso de AAA y RPA, será necesario contar con auditores que tengan la formación y experiencia adecuada, formando **equipos de auditoría con perfiles multidisciplinares**, que integre auditores financieros y/o de cumplimiento y auditores especializados en auditoría de sistemas de información, con el fin de obtener una visión completa y que plantee el análisis del proceso desde distintas perspectivas, funcional, legal y tecnológica. **Este aspecto es clave para el éxito de estas auditorías**.

Por tanto, al planificar la auditoría se deben determinar los recursos necesarios para llevarla a cabo, incluyendo tanto el equipo de auditoría como las herramientas necesarias. Si no se dispone de recursos propios se ha tendrá en cuenta la conveniencia o no de contar con personal externo experto para aquellos temas especializados que lo requieran.

8. Obtención de conocimiento del proceso de gestión donde se integra la AAA o el RPA

El auditor ha de obtener una comprensión clara de las áreas en las que se implementa la automatización. También es importante identificar y analizar el nivel de automatización de los procesos, es decir, si se ha implementado una automatización parcial o completa.

Este conocimiento permitirá al auditor identificar los riesgos asociados con la automatización. Por ejemplo, en el caso de una automatización parcial, el auditor deberá evaluar tanto los controles automatizados como los manuales, ya que ambos tipos de controles son importantes para la integridad del proceso. Este conocimiento es esencial para que el auditor determine los procedimientos de

auditoría adecuados y pueda adaptar su enfoque de auditoría de manera efectiva, garantizando así una evaluación exhaustiva y precisa de los controles y procesos de la organización.

En esta etapa, en la que se debe conocer el proceso automatizado y su infraestructura tecnológica, se han de revisar, entre otros, el flujo del proceso automatizado, la plataforma en la que se instala y la integración con las distintas bases de datos, portales web y otros sistemas con los que se relaciona.

El auditor ha de ejecutar procedimientos de valoración del riesgo, que incluirán, entre otras acciones:

- Verificar la existencia de un plan estratégico institucional que contemple la automatización.
- Evaluar el cumplimiento de la normativa aplicable respecto al uso de las AAA y RPA (en particular los artículos 41 y 42 de la Ley 40/2015, el articulado básico del RD 203/2021, ENS y RGPD).
- Evaluar la gobernanza en TI de la entidad fiscalizada y la alineación del proceso fiscalizado con los objetivos institucionales.
- Identificar la cadena de suministro que incluye a los terceros involucrados (proveedores de software, servicios en la nube, etc.).
- Identificar todos los componentes del RPA o la AAA.
- Identificar las aplicaciones TI que le dan soporte, prestando especial atención a los flujos de información y las interfaces existentes entre distintos sistemas.
- Analizar la arquitectura del sistema, incluyendo la infraestructura donde se despliega.
- Revisión del contrato en caso de subcontratación de algún componente del proceso auditado.

Se debe solicitar y analizar los documentos que describen dichos procesos ya que proporcionarán una visión detallada de cómo se ha planificado y llevado a cabo la automatización y son fundamentales para comprender su alcance y efectividad.

El tipo de documentación que podemos encontrar durante una fiscalización se detalla en el Anexo 1.

El análisis de estos documentos ayuda a identificar posibles áreas de riesgo y a evaluar la robustez de los controles implementados. Por ejemplo, el auditor puede examinar cómo se gestionan las excepciones y los errores en los procesos automatizados, así como la existencia de mecanismos de supervisión y mantenimiento continuo de la automatización.

Tras el análisis de la documentación se deben mantener reuniones con los responsables del proceso de gestión en las que se analice de manera detallada el proceso automatizado. En esta etapa será de utilidad la guía *GPF-OCEX 1511 Cómo realizar y documentar las **pruebas paso a paso***. En el Anexo 2 se incluye un cuestionario de ejemplo que se puede utilizar convenientemente adaptado a cada caso.

En resumen, solicitar y analizar los documentos que soportan el proceso de automatización, incluyendo las guías de definiciones y validaciones, es una etapa fundamental de la auditoría. Esto permite al auditor obtener una comprensión profunda de la automatización implementada y evaluar su efectividad y conformidad con la normativa y los estándares establecidos.

Al final, el conocimiento adquirido se debe **documentar** mediante un memorándum o narrativa y mediante un flujograma.

Para realizar el flujograma se puede utilizar la GPF-OCEX 1512. En el Anexo 3 se pueden ver dos ejemplos (el 3 y el 4) de cómo elaborar un flujograma para documentar un proceso de subvenciones.

9. Identificación y valoración de riesgos

Los distintos tipos de automatizaciones ofrecen beneficios claros en términos de eficiencia, pero también riesgos, que difieren según el tipo de herramienta de que se trate, que el auditor debe identificar y valorar siguiendo la metodología establecida en las GPF-OCEX.

A continuación, se detallan una serie de riesgos relacionados con la utilización de automatizaciones en general, incluyendo AAA y RPA, que se encuentran más frecuentemente, agrupados por áreas, y las preguntas que debe hacer el auditor cuando realice el análisis de la documentación y el conocimiento del proceso al realizar la prueba paso a paso, que se han mencionado en el apartado anterior.

Área de riesgo	Riesgos	Preguntas del auditor
Riesgos en la programación, infraestructura y software	- Errores en la programación - El software en el que se instala la automatización presenta vulnerabilidades - Los proveedores de la automatización no están homologados - No se ha actualizado el soporte donde se instala la automatización - Inseguridad en la infraestructura que soporta la automatización - Acceso a datos confidenciales durante las pruebas	- ¿Existen revisiones de código o validaciones antes de pasar a producción? - ¿Se realizan análisis de vulnerabilidades en el software? - ¿Los proveedores de la automatización cuentan con homologación o certificación? - ¿La infraestructura tecnológica y los sistemas operativos cuentan con parches y actualizaciones vigentes? - ¿Los datos para las pruebas son datos reales?
Análisis y diseño de los procedi-mientos	- ¿Se ha realizado y documentado el correspondiente análisis funcional? - No existe una estrategia definida o la automatización no está alineada con el objeto de negocio - Falta de definición o formalización de los procedimientos - La estrategia y /o procedimientos pueden estar definidos y no cumplirse o no funcionar - No se han definido procedimientos en caso de qué hacer si la automatización no funciona, analizando como proceder	- ¿Se ha realizado un análisis exhaustivo del proceso antes de la automatización (diagrama de flujos, técnicas de mapeo de procesos)? - ¿Está documentada una estrategia de automatización alineada con los objetivos del negocio? - ¿Se encuentran definidos y aprobados los procedimientos asociados a la automatización? - ¿Existen evidencias de que los procedimientos definidos se aplican en la práctica? - ¿Se han establecido planes de contingencia y pasos a seguir en caso de fallo en la automatización?
Riesgo de controles	- No se han definido controles de evaluación o seguimiento - No se ha definido formalmente cómo se debe realizar el seguimiento de las incidencias, así como la comunicación de las mismas - La implantación del software de la automatización ha implicado reducir o eliminar algunos controles de seguridad (segregación de funciones...)	- ¿Se han definido y establecido controles para evaluar la efectividad de la automatización? - ¿Se han establecido mecanismos de supervisión de los controles? - ¿Se realizan pruebas periódicas para evaluar la eficacia de los controles establecidos? - ¿Existe un procedimiento formal para registrar, clasificar y dar seguimiento a las incidencias? - ¿El acceso a modificar o detener la automatización está restringido y segregado adecuadamente?
Riesgo derivado de la gestión del cambio	- Posibles errores por parte de los empleados por la dificultad del cambio - Implementación errónea del cambio en la automatización - Posible afectación a la interrupción del sistema durante el cambio	- ¿Se realizan pruebas y comprobaciones antes de implementar cambios en la automatización? - ¿Existe un procedimiento formal de gestión de cambios aprobado por un comité o responsables? - ¿Se forma al personal sobre los cambios implementados para reducir errores de operación? - ¿Se han analizado los posibles impactos en la disponibilidad de sistemas durante el cambio?

Área de riesgo	Riesgos	Preguntas del auditor
Riesgo de fiabilidad de los datos	- Baja fiabilidad (exactitud y completitud) de los datos utilizados - Errores de lectura de los documentos que se incorporan en proceso	- ¿Se verifican los orígenes de los datos para garantizar su fiabilidad (exactitud y completitud)? - ¿Existen controles para detectar errores en la lectura o interpretación de documentos? - ¿Se realizan verificaciones posteriores para asegurar la fiabilidad de los datos procesados?
Riesgos de trazabilidad y evidencias	- El sistema automatizado se ha dado de baja y no se han guardado debidamente los registros - El almacenamiento de los ficheros log se ha guardado de forma manipulable - Uso de usuarios genéricos que reducen o eliminan la trazabilidad correcta de los procesos - Falta de registro de las evidencias o de su dispersión y falta de correlación - Falta de evidencia de quién modifica los datos	- ¿Existen mecanismos para asegurar la conservación y no manipulación de registros y logs? - ¿Se audita periódicamente el uso de usuarios genéricos o compartidos? - ¿El sistema registra quién, cuándo y qué cambios realiza sobre los datos? - ¿Se almacenan evidencias de manera centralizada y con correlación adecuada?
Riesgos de incumplimiento	- No se cumple con la normativa aplicable y con las políticas establecidas - En caso de AAA no cumple con lo establecido en artículo 41 y 42 de la Ley 40/2015, y otra normativa estatal o autonómica aplicable - No se tienen en cuenta los cambios establecidos en las normas y políticas - La automatización no se adapta a los manuales establecidos - No se cumple con la normativa del ENS y del RGPD	- ¿Se revisa periódicamente el cumplimiento de la automatización frente a normativas aplicables (ENS, RGPD, etc.)? - ¿Se revisan los cambios en normas y políticas internas y se actualizan los procesos? - ¿Existen procedimientos que aseguren que la automatización cumple con los manuales de operación internos?
Otros riesgos	- La automatización no está incluida en los planes de recuperación ante desastres - Falta o inexistencia de monitorización del rendimiento (en cuanto a aspectos como velocidad, recursos, etc) - Dependencia de personal especializado clave. - Dependencia externa	- ¿Está incluida la automatización en los planes de continuidad del negocio y recuperación ante desastres? - ¿Se monitorea el rendimiento del sistema (tiempos de respuesta, uso de recursos, caídas)? - ¿Qué grado de dependencia existe del personal especializado para el mantenimiento y soporte? - ¿Se evalúan los riesgos asociados a la dependencia de proveedores externos?

10. Identificación y revisión de los controles de procesamiento de la información (CPI)

Durante la etapa de conocimiento de la entidad y de su sistema de control interno, se realizará la identificación, análisis y evaluación de los CPI que la entidad ha implementado para prevenir, detectar y corregir errores, en las automatizaciones examinadas, para ello:

a) El auditor ha de ejecutar procedimientos de valoración del riesgo (ver apartado anterior) para identificar los CPI implantados, incluyendo la revisión de manuales de procedimientos y su correspondencia con el sistema automatizado.

b) Identificará políticas de segregación de funciones.

c) Identificará controles de aprobación y validación en los procesos automatizados.

d) Identificará si existen controles compensatorios cuando se requieran.

e) Verificará la trazabilidad de las operaciones dentro del sistema.

A continuación, se indican algunos ejemplos de aspectos que se podrían analizar:

- Comprobar si existen mecanismos de control interno que incluyan la función de revisar el trabajo realizado por la gestión, supervisando, entre otras, la correcta aplicación de la normativa y procedimientos.
- Comprobar si se ha realizado un documento formal en el que se elabore un análisis de los riesgos que pueden afectar a la gestión, definiendo las áreas y evaluando y valorando los mismos, así como un plan de medidas tomadas para dar respuesta a los riesgos de forma que se puedan evitar o minimizar.
- Analizar si existen procedimientos establecidos para que cada unidad administrativa comunique internamente información pertinente y de calidad para la consecución de los objetivos y el cumplimiento de la normativa aplicable.
- Verificar si hay establecidos procedimientos de realización y planificación de la supervisión de las tareas que se realizan.
- Comprobar si se deja evidencia de la supervisión de estas tareas.

Es importante identificar y comprender los CPI establecidos, así como las validaciones automáticas y manuales. Se puede utilizar como base la **GPF-OCEX 5340**, que detalla la revisión de los CPI en un entorno de administración electrónica. Según dicha guía, los CPI son controles relacionados con el procesamiento de la información en aplicaciones de TI o procesamientos manuales de la información en el sistema de información de la entidad que responden directamente a los riesgos para la integridad de la información (es decir, la completitud, exactitud y validez de las transacciones y otra información) y el cumplimiento de la legalidad. Actúan en diferentes momentos del flujo de procesamiento: entrada, transformación/procesamiento, salida, datos maestros, interfaces, etc.

11. Identificación y revisión de los CGTI relevantes

Se puede utilizar como base la **GPF-OCEX 5330**, que detalla la revisión de los controles generales de tecnologías de información (CGTI) en un entorno de administración electrónica. Según dicha guía, los CGTI son los controles de los procesos de TI de la entidad que apoyan el funcionamiento continúo apropiado del entorno de TI, incluido el funcionamiento continuo efectivo de los controles de procesamiento de la información y la integridad de la información (es decir, la completitud, exactitud y validez de la información) en el sistema de información de la entidad.

Por tanto, será necesario recopilar información sobre los recursos tecnológicos existentes en la entidad, como hardware, software, redes y sistemas de comunicación, que afectan al entorno automatizado.

El auditor deberá evaluar la fortaleza de los CGTI relevantes del proceso de gestión en el que se incorpora la AAA o el RPA. Esta revisión se efectuará de acuerdo con la metodología recogida en la GPF-OCEX 5330, seleccionando los CGTI más relevantes de acuerdo con los objetivos de la auditoría y los riesgos valorados.

Relacionados con los AAA y RPA, se debe prestar especial atención a:

- **GPF-OCEX 5332 Gestión de cambios**: en particular los relacionados con el diseño del algoritmo y/o sus parámetros y la posterior implementación de estos cambios en la automatización, así como comprobar si se prueban adecuadamente los cambios antes de pasarlos a producción, lo que permitirá evitar errores o resultados inesperados.
- **GPF-OCEX 5333 Operaciones de los sistemas de información**: habrá que determinar si se monitoriza la ejecución del algoritmo, se gestionan errores, excepciones o fallos, y se realizan copias de seguridad.

- **GPF-OCEX 5334 Controles de acceso**: determinar quién tiene acceso para definir, modificar, ejecutar, supervisar el algoritmo, si está el acceso basado en el principio de necesidad de conocer y debidamente segregado. Son críticos los controles sobre usuarios con privilegios de administración.
- **GPF-OCEX 5335 Continuidad del servicio**: en el caso de que se trate de un proceso automatizado crítico, habrá que tener en cuenta el plan de continuidad aprobado.

Se analizará también el cumplimiento de los requisitos que se establecen en el Esquema Nacional de Seguridad, aplicando la parte correspondiente de la GPF-OCEX 5314 y en Reglamento General de Protección de Datos (RGPD), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

12. Procedimientos posteriores de auditoría

Estos procedimientos, de acuerdo con la NIA-ES-SP 1330, incluyen las pruebas de controles y los procedimientos sustantivos (procedimientos analíticos y pruebas en detalle).

Tras identificar los controles relevantes (CPI y CGTI) se debe revisar su eficacia operativa que incluirá pruebas de cumplimiento y de detalle para asegurarse de que los controles funcionan como se espera.

Se utilizará como base del trabajo la GPF-OCEX 5340 y la GPF-OCEX 5330. Algunos de los aspectos a revisar pueden ser los siguientes:

- Verificar que se han establecido controles en todo el ciclo de vida de la automatización que permitan garantizar la efectividad de estos controles en todas las fases (alta, actualización, gestión de cambios, baja…)
- Evaluar la frecuencia y alcance de revisiones realizadas por el gestor del sistema.
- Sobre la automatización:
  - Se comprobará que el mapa de procesos se ajusta al objetivo de la automatización.
  - Verificar la correcta configuración de reglas y validaciones establecidas dentro del sistema.
  - Realizar pruebas de entrada y salida en el sistema para validar lógica automática, preferiblemente en un entorno de pruebas.
  - Verificar que los resultados de las pruebas sustantivas sobre el proceso automatizado son los esperados. Para ello, elaborar, si es posible, una prueba de recorrido verificando y reproduciendo los aspectos relativos al proceso que realiza el sistema automatizado (si lo permite la producción, realizar en un entorno de pruebas la reproducción del funcionamiento del sistema automatizado). Dicha prueba implica seguir el rastro de una operación desde su inicio hasta su finalización, de forma que se observe y evalúe cómo se aplican los controles, si las validaciones son realizadas correctamente, o si hay brechas o debilidades en los controles internos.
  - Cuando lo exija la normativa se comprobará si el código fuente está accesible y cumple con los requisitos establecidos.
- Pedir las evidencias de las verificaciones realizadas por el ente fiscalizado respecto a los controles, monitoreo del desempeño y disponibilidad del sistema y revisarlas.
- Solicitar la base de datos de producción para analizar la validez e integridad de su información.
- Verificar la existencia de procedimientos de respaldo y recuperación de datos.
- Comprobar si se han realizado capacitaciones al personal respecto a la automatización fiscalizada.

- Revisar los registros de reuniones de control o seguimiento del sistema.

13. Elaboración de informes

Dependiendo del tipo de auditoría que se haya realizado, por ejemplo:

a) auditoría específica, operativa o de cumplimiento, sobre una AAA o RPA,

b) auditoría de cumplimiento sobre un proceso de gestión (subvenciones, por ejemplo) que incluye en alguna de sus fases una automatización, o

c) auditoría financiera de cuentas anuales, en las que en algún momento se ha utilizado una RPA o un AAA en la gestión,

se utilizará un modelo u otro de informe de los previstos en las GPF-OCEX.

En el caso b) tendrán más o menos relevancia los aspectos relacionados con la automatización en función de los riesgos y hallazgos de la auditoría. En el caso c) probablemente ni se mencione en el informe, salvo que se haya detectado alguna incorrección material o deficiencia significativa relacionada al revisar el control interno.

Se exponen a continuación **ejemplos** de **debilidades** de forma que puedan ayudar al auditor durante la elaboración del informe:

Relativas a la estrategia definida y las políticas establecidas

1. No disponer de una estrategia para la implantación del sistema automatizado acorde con las expectativas y aprobada por la Dirección.
2. No se han establecido políticas y normas asociadas que sirvan como requisitos mínimos para el uso de sistemas automatizados a nivel global.

Relativas al sistema automatizado

1. No existe un Plan de pruebas, o evidencia de las mismas, realizado en preproducción sobre el sistema automatizado y validado por los responsables funcionales.
2. Existencia de validaciones que ha realizado el sistema automatizado y que no se han ejecutado de forma correcta.
3. Existencia de validaciones que el sistema automatizado ha realizado de forma correcta, detectando la falta de cumplimiento de requisitos y, aun así, se ha continuado con el trámite del procedimiento teniendo como consecuencia posibles incumplimientos.
4. El sistema no ha leído de forma correcta los documentos procesados.
5. No existe trazabilidad en el sistema informático que garantice quién ha realizado la validación.
6. No se muestran los cambios en el estado de la validación durante la tramitación.
7. No se puede garantizar que los datos de las validaciones registradas en el sistema informático se encuentren actualizados y conformes con el resultado obtenido.
8. Existencia de validaciones que han dado errores y finalmente se realizan de forma manual, con los consiguientes riesgos de errores.
9. Errores en el cálculo de una subvención.

De acuerdo con la GPF-OCEX 1735 es importante incluir en el informe **recomendaciones** que puedan ser útiles y constructivas para el auditado. Algunas sugerencias de recomendaciones podrían ser las siguientes:

1. Dejar evidencia de la trazabilidad de quién ha ejecutado las validaciones, el sistema automatizado o una persona, con la finalidad de poder realizar el seguimiento de las mismas, así como de los errores que se produzcan.
2. Revisar todas las validaciones que debe realizar el sistema automatizado para evitar que se produzcan errores y así asegurar su correcto funcionamiento.
3. Asegurar la disponibilidad y salvaguarda del fichero con el registro de las evidencias de todas las comprobaciones que se realizan por el sistema automatizado.
4. Dejar evidencia de las pruebas que se han realizado sobre el sistema automatizado en el entorno de preproducción.
5. Establecer un plan para mitigar el riesgo de dependencia del conocimiento de la automatización concentrado en la empresa desarrolladora o en una sola persona de la entidad.

14. Bibliografía

- **La automatización en las Administraciones públicas: cómo auditar un sistema RPA**, Sandra Barrio Carvajal y Lucía Silóniz Fernández-Shaw, Revista Auditoría Pública nº 84, noviembre 2024.
- **Actuaciones administrativas automatizadas y automatización robótica de procesos en la gestión de personas**, Pedro Padilla Ruiz, Revista Vasca de Gestión de Personas y Organizaciones Públicas, nº 24, 2023.
- **Auditoría de las actuaciones administrativas automatizadas sobre ayudas públicas,** Eloy Sánchez Genicio, Revista El Consultor de los Ayuntamientos, septiembre de 2025.
- **La automatización robótica de procesos en el Departamento de Intervención de la Diputación de Girona,** Josa Arbones, N. / Molas Pujol, l., Revista de estudios Locales - CUNAL 277, 2024.
- **Actuación automatizada, robotizada e inteligente**, Agustí Cerrillo Martínez, en Manual de Derecho administrativo, Marcial Pons, 2025.
- **Chatbots, automatización y actuaciones administrativas automatizadas: gobernanza de la inteligencia artificial para la modernización administrativa,** Luis Feijoo García y Luis María Bautista Ortega, en Kit básico para la implantación de la Inteligencia Artificial en el Sector Público, El Consultor de los Ayuntamientos, 2025.
- **Requisitos para Auditorías de Tratamientos que incluyan IA**, Agencia Española de Protección de Datos (AEPD), enero 2021.

Anexo 1: Ejemplo de documentación a solicitar durante la planificación

Área	Documento a solicitar	Finalidad
Administrativa	Estrategia de la automatización	Comprobar que existe una estrategia y los pasos que se han seguido
	Documento de aprobación del proceso automatizado	Verificar la existencia de base legal y aprobación formal
	Descripción del procedimiento automatizado	Comprender el flujo, actores y controles
	Registro de actividades de tratamiento	Identificar datos personales tratados y base legal
Diseño y planificación	Especificaciones técnicas: Definición de requisitos funcionales y no funcionales.	Entender objetivos, funcionalidades y alcance del sistema
	Diagramas de flujo de procesos: Representación gráfica del flujo de trabajo y toma de decisiones.	Identificar infraestructuras, bases de datos y flujos
	Plan de desarrollo e implantación	Comprobar planificación, responsables y plazos
Seguridad y protección de datos	Documento de seguridad del sistema	Conocer las medidas de protección y gestión de accesos
	Análisis de riesgos de seguridad	Evaluar riesgos detectados y medidas adoptadas
	Evaluación de impacto en protección de datos, si corresponde	Verificar medidas ante riesgos de tratamiento de datos sensibles
Operativa y funcionamiento (usuarios)	Manual de usuario	Revisar facilidad de uso y operatividad
	Manual de administración técnica	Comprobar gestión técnica y mantenimiento
	Plan de contingencia y continuidad	Asegurar planes de actuación ante incidentes
Control y trazabilidad	Matriz de controles automáticos	Identificar controles internos programados
	Logs de trazabilidad	Verificar registro de actuaciones, accesos y decisiones
	Informes de auditoría interna o controles previos	Conocer evaluaciones internas previas
	Indicadores de desempeño	Comprobar medición de eficacia y calidad
Validación y calidad	Planes de pruebas (test plan)	Verificar que se hayan realizado pruebas técnicas y funcionales
	Actas de validación y aceptación del sistema	Confirmar que el sistema fue revisado y aceptado formalmente
	Certificaciones técnicas (si aplica)	Comprobar cumplimiento de estándares técnicos o de ciberseguridad
Documentación Complementaria	Informe de Evaluación de Riesgos	Para la identificación y análisis de riesgos potenciales.

Anexo 2: Ejemplo de cuestionario

A continuación, a modo de ejemplo, se indican una serie de preguntas tipo para revisar y que pueden ayudar para la realización del programa de trabajo.

Preguntas para analizar un proceso automatizado

¿Se ha realizado un análisis exhaustivo de la viabilidad del proceso antes de la automatización (diagrama de flujos, técnicas de mapeo de procesos)?

¿Se ha realizado un estudio de la necesidad de sistemas automatizados o RPA para el caso de uso en cuestión?

¿Se ha elaborado un Plan de desarrollo de la automatización o documento equivalente?

¿Se ha implementado un sistema de registro de las actividades objeto de la automatización?

¿Se han instaurado controles que permitan monitorear en tiempo real la automatización y alerten sobre posibles disfuncionalidades o desviaciones?

¿Se realizan auditorías periódicas de los registros de actividades para asegurar su integridad y precisión?

¿Se han implementado controles de acceso basados en roles bien definidos?

¿Existe una política de identificación, autenticación y acceso y se aplica?

¿Se ha diseñado teniendo en cuenta la escalabilidad, usando arquitecturas orientadas a servicios que permitan alcanzar un mayor volumen de la automatización, según las nuevas necesidades, sin afectar al rendimiento?

¿Se ha establecido un plan de mantenimiento y soporte para asegurar que se siga operando correctamente cuando los sistemas subyacentes evolucionen?

¿Se han implantados controles automáticos que identifiquen y notifiquen sobre posibles errores o inconsistencia en los datos?

¿Se han implementado procedimientos y reglas que permitan adaptarse a las actualizaciones en la normativa aplicable?

¿Se ha realizado una evaluación de la capacidad asegurando que la infraestructura sea capaz de soportar una carga adicional a la inicialmente estimada?

¿Se han realizado pruebas exhaustivas de integración entre la automatización y el resto de los sistemas para garantizar una comunicación eficaz, sin errores y fluida?

¿Se han establecido mecanismos de respaldo, para minimizar el impacto en caso de fallos de integración?

¿Dispone de un plan de pruebas antes de pasar a producción para comprobar el correcto funcionamiento de la aplicación?

¿El plan de pruebas incluye criterios de seguridad como requisito para el paso a producción?

¿Se requiere de la aprobación del responsable funcional en las pruebas previas al paso a producción?

¿Se realizan las pruebas en un entorno aislado, independiente y seguro o en el entorno de producción?

¿Se utilizan APIs u otro tipo de interactuación con otros sistemas durante el proceso de automatización? En caso afirmativo, indicar cuales

¿Se ha realizado un estudio sobre la adecuación de la tecnología RPA en lugar de otras tecnologías alternativas, como por ejemplo APIs para integrar sistemas?

¿Se dispone del código fuente o de garantías contractuales que aseguren acceso al mismo en caso de incidencias o discontinuidad del servicio?

¿El contrato con la empresa proveedora de la automatización, si es el caso, cubre cláusulas sobre mantenimiento, escalabilidad y cumplimiento normativo?

Anexo 3: Ejemplos de informes

Ejemplo 1 RPA

Fiscalización de las subvenciones concedidas a establecimientos hoteleros afectados por el COVID Cámara de Cuentas de Andalucía, febrero 2025

*En esta **fiscalización de cumplimiento**, uno de los procedimientos destacados en el apartado 4.1. Objetivos y alcance del trabajo de fiscalización ha sido la revisión del subproceso ejecutado por un RPA:*

21 Además de la muestra de expedientes seleccionados, como parte del control interno, se han revisado las validaciones realizadas por el RPA sobre el total de la población de expedientes de subvenciones concedidas, a partir del fichero facilitado por el gestor. De dicho análisis se han detectado incumplimientos que han sido reflejados en el apartado de salvedades y de control interno (§A.7).

En el informe se recoge los resultados de la revisión del control interno relacionado con el RPA:

6.2. Análisis del entorno informático y del RPA

46 Estas subvenciones han sido tramitadas durante la fase de concesión mediante tecnología RPA, que ha realizado la comprobación de requisitos exigidos para tener derecho a la subvención hasta que se emite la resolución de concesión. Para la gestión de los expedientes de las subvenciones se utiliza la aplicación INCENTIVA.

Como parte del análisis del control interno se ha revisado, por un lado, el entorno informático, y, por otro lado, el correcto funcionamiento del RPA.

Se debe destacar que, en la fecha en la que se han realizado los trabajos por parte de la Cámara de Cuentas, el RPA ya no estaba operativo. No se ha dispuesto de las evidencias originales de todas las comprobaciones que se efectuaron en el momento de la tramitación de las subvenciones, por lo que, para la elaboración del trabajo, se ha utilizado un fichero, de fecha 16 de mayo de 2023, con réplicas de algunas de las validaciones que ejecutó el robot. Se han obtenido las consultas relativas a la Agencia Estatal de la Administración Tributaria, Ministerio de Hacienda y Administración Pública, Tesorería General de la Seguridad Social y la Dirección General de la Policía Nacional (en el Apéndice 9.4 se detallan las validaciones).

48 Con respecto al funcionamiento del RPA, se han analizado:

- Las validaciones que ha realizado el robot y que no se han ejecutado de forma correcta.
- Las validaciones en las que el RPA ha detectado la falta de cumplimiento de requisitos y, aun así, las subvenciones han sido concedidas.

De dicho análisis se han detectado las siguientes **debilidades** generales:

- Durante el proceso de verificación de los requisitos, los documentos pdf incluidos no han podido ser leídos de forma correcta, ya que se han producido errores que han conllevado que la validación se haya tenido que realizar de forma manual.
- No existe una trazabilidad en INCENTIVA que garantice quién ha realizado la validación, si ha sido el RPA o una persona.
- No se muestran los cambios que se han producido en el estado del expediente durante el proceso de las validaciones.
- No se puede garantizar que los datos de las validaciones registradas en INCENTIVA se encuentren actualizados y conformes con el resultado obtenido.
- No se puede asegurar que los datos que se han remitido a la BDNS sean los correctos, ya que se han detectado errores en el cruce de ayudas recibidas por minimis, y datos de expedientes que no se incluyen en la BDNS (§30 y 38).

Las validaciones realizadas se muestran en el gráfico nº1. (§A.13):

En el informe se profundiza en esta materia:

8.6.2. Análisis del entorno informático y del RPA

A.12 Para realizar la robotización que ha comprobado el cumplimiento de los requisitos en la tramitación de las subvenciones se ha elaborado un contrato de servicios informáticos con una empresa, mediante el procedimiento de emergencia, al no contar con los medios propios necesarios para la realización de las comprobaciones necesarias. Dicho contrato se ha otorgado a través del Acuerdo del Consejero de Turismo, Regeneración, Justicia y Administración Local por el que se declara la emergencia de la contratación del servicio informático necesario para la tramitación robotizada de las solicitudes de subvención al amparo del Decreto-ley 6/2021, de 23 de marzo, por el que se

establecen medidas extraordinarias y urgentes para el sector turístico como consecuencia de la situación ocasionada por el coronavirus (covid-19).

El contrato tiene como objeto proceder a la verificación con la mayor celeridad posible, del cumplimiento de los requisitos establecidos en el Decreto-ley 6/2021, para lo cual se considera oportuno incorporar a la tramitación de las ayudas la tecnología RPA, que permite efectuar de forma robotizada la mayor parte de las comprobaciones descritas en el citado Decreto-ley 6/2021, mecanizando la consulta a las plataformas de intercambio de datos con la Seguridad Social y la Administración Tributaria, la consulta de datos en páginas web como la Base Nacional de datos de subvenciones (BDNS) o las consultas a determinados Registros como el Registro de Licitadores del Estado, el Registro Público Concursal o el Registro de Turismo de Andalucía. Asimismo, esta tecnología permite efectuar de un modo automatizado la lectura de documentos en pdf que se encuentren normalizados, como es el caso de las declaraciones trimestrales de IVA o las declaraciones del Impuesto de Sociedades.

Se ha elaborado una guía de diseño de la robotización para la implementación en los sistemas de información usados en la tramitación de las subvenciones al amparo del Decreto-ley 6/2021. Se describe, formalmente y a nivel de usuario, la lógica global del sistema en el tratamiento de las solicitudes presentadas, indicando las actuaciones, secuencias lógicas de las distintas transiciones que sufren los expedientes de subvención, así como cada uno de los procesos o comportamientos del sistema de información para la verificación de cada uno de los requisitos, de forma que tal descripción ayude a identificar la adecuada pista de auditoría.

Se han diseñado un total de 40 validaciones para comprobar los requisitos, que se han plasmado en la citada guía (Anexo 9.4).

El siguiente flujograma del informe muestra cómo se han utilizado RPA para gestionar las subvenciones. Las flechas rojas no son del informe.

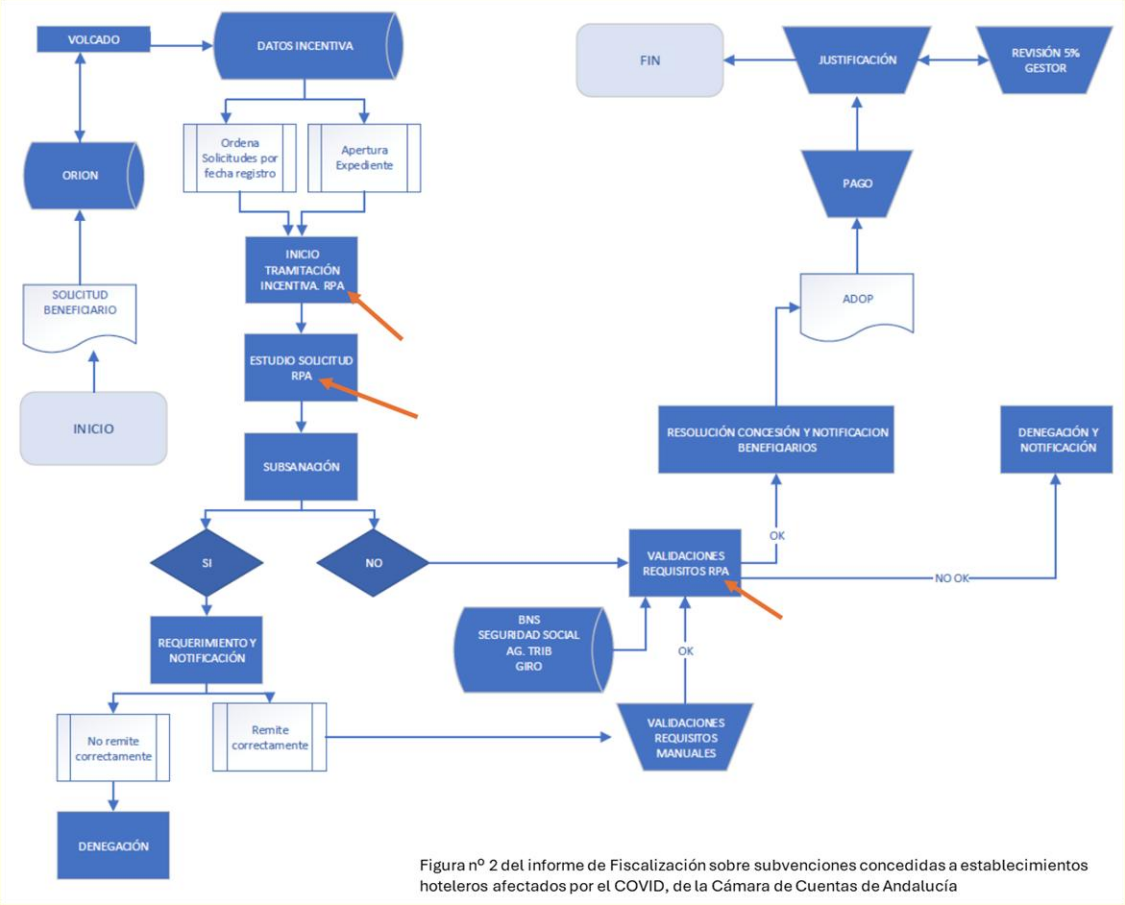


Figura nº 2 del informe de Fiscalización sobre subvenciones concedidas a establecimientos hoteleros afectados por el COVID, de la Cámara de Cuentas de Andalucía

Ejemplo 2 RPA

Fiscalización operativa del Bono Alquiler Joven en Andalucía
Cámara de Cuentas de Andalucía, junio 2025

*Esta **fiscalización operativa** no tenía como objetivo específico auditar el RPA, ya que esta herramienta solo era una más entre las utilizadas en el proceso fiscalizado, pero resulta interesante ver qué tareas tenía encomendadas dicho RPA según se describe en el informe:*

8. La gestión de las ayudas del BAJ se realiza a través de la herramienta informática de la Consejería utilizada para ayudas al alquiler (Alquila) y la plataforma de tramitación electrónica de la Junta de Andalucía (PTw@ndA). En el anexo 3 se ofrece un mapa del proceso de tramitación.

   Las solicitudes se presentan de forma exclusivamente electrónica por la Ventanilla Única de la Administración de la Junta de Andalucía (VEAJA), como punto de encuentro entre solicitantes y Administración. La sincronización y comunicación entre VEAJA y Alquila se realiza mediante la interacción de un **RPA (Robotic Process Automatic)** o Robot encargado de la incorporación de los formularios de solicitud, subsanación o modificación (Anexo I y Anexo I-BIS), de alegaciones y desistimiento (Anexo II), y de justificaciones (Anexo III), y documentación complementaria o voluntaria presentada. Asimismo, permite la grabación de la información de presentación (fecha y código de registro) y todos los campos de cada solicitud presentada, facilitando el cálculo de la subvención.

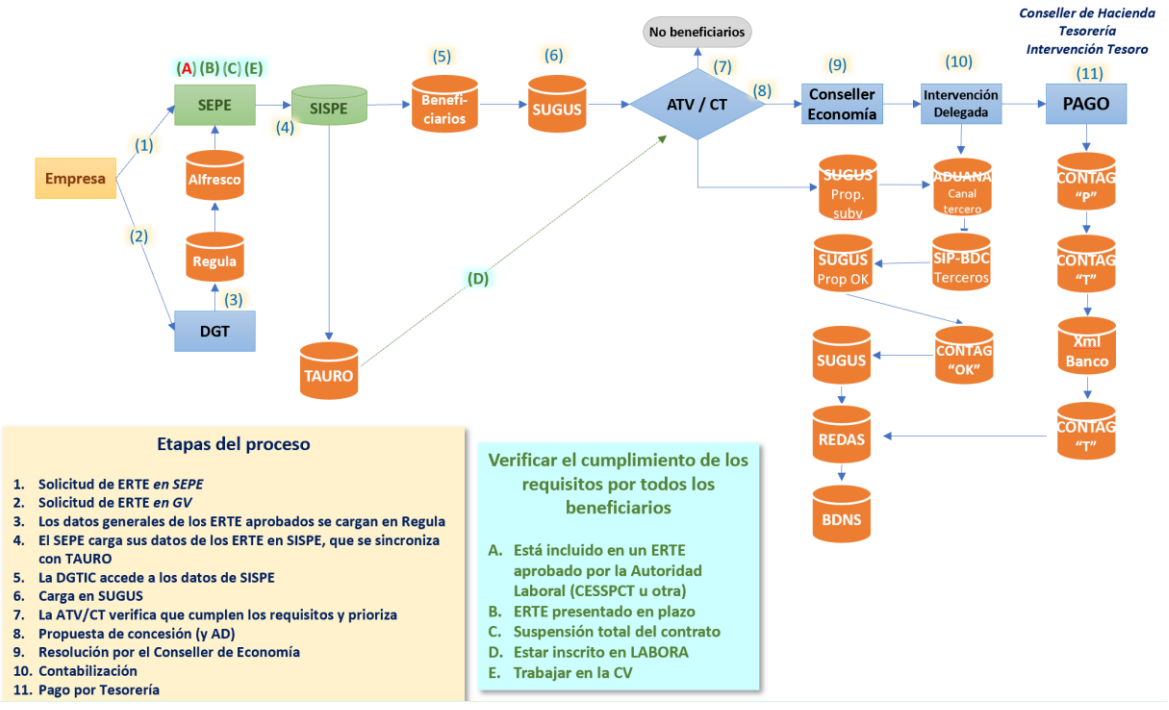
   El Robot lleva a cabo una serie de acciones para la comprobación del cumplimiento de determinados requisitos previstos en las bases reguladoras[(6)] siempre que no exista oposición a las consultas SCSP por parte de las personas solicitantes.

   (6) Los requisitos objeto de verificación son: titularidad de otra vivienda; residencia habitual y permanente; nacionalidad y/o residencia; edad; hallarse al corriente con la Seguridad Social, con la Agencia Tributaria Estatal y con la Agencia Tributaria de Andalucía; ubicación de la vivienda en la provincia a que se dirige la solicitud; límite de renta de la vivienda; no percepción de otras ayudas o subvenciones; no incursión en circunstancias del art.13 Ley 38/2003, de 17 de noviembre; datos bancarios; acreditación representación legal; fuente regular de ingresos; y límite ingresos.

Ejemplo 3 Automatización

Informe especial. Auditoría de las ayudas a personas con rentas bajas afectadas por un ERTE como consecuencia de la COVID-19 reguladas en el Decreto Ley 3/2020 y en el Decreto 54/2020
Sindicatura de Comptes de la Comunitat Valenciana, junio 2021

La figura nº 1 del informe muestra el flujograma del proceso de gestión de las ayudas:



Anexo 4: Matriz de auditoría

A continuación, a modo de resumen, se incluye una matriz con las distintas fases y pruebas a realizar durante el trabajo de campo:

Fase	Objetivo	Prueba de auditoría	Evidencia esperada	Posibles hallazgos
Conocimiento del entorno	Conocer el contexto institucional y tecnológico del sistema.	- Revisar el plan estratégico institucional y verificar mención del sistema automatizado. - Evaluación de la gobernanza de TI.	- Copia del plan estratégico con objetivos relacionados al sistema.	- Desalineación entre sistema automatizado y misión institucional.
		- Verificar normativa vigente sobre TIC.	- Certificaciones, etc.	- Incumplimientos normativos.
		- Identificar la cadena de suministro.	- Contratos, convenios para verificar la adecuación de su clausulado.	- Riesgos de terceros no controlados. - Información esencial en la nube sin control.
Análisis del control interno	Evaluar mecanismos internos de control sobre procesos automatizados.	- Revisar manuales de procedimiento y flujogramas.	- Manuales y diagramas actualizados.	- Inconsistencias entre práctica y documentación.
		- Evaluar la segregación de funciones.	- Matriz de funciones por usuario.	- Concentración de funciones críticas en un solo rol sin que haya procedimientos alternativos compensatorios.
Controles de cambios	Verificar acciones de gestión y monitoreo del sistema.	- Comprobar controles de autorización dentro del sistema.	- Capturas del sistema mostrando validaciones o flujos de aprobación.	- Ausencia de controles automáticos.
		- Verificar si se ha llevado a cabo un control de versiones que permita rastrear y gestionar los cambios en el código fuente (GPF 5332, apartado B.2.2)	- Documento que acredite las versiones de la automatización, así como los cambios introducidos en cada una de ellas y la fecha en la que se ha generado.	- Falta de control de versiones. - El control de versiones no recoge las fechas. - No están documentados los cambios introducidos en las versiones.
Seguridad	Evaluar las medidas o controles para proteger la información.	- Identificación de los componentes relacionados con el algoritmo que sean críticos y las copias de respaldo.	- Procedimiento de copias de seguridad y evidencias de pruebas de restauración.	- Ausencia de copias de seguridad y pruebas de restauración no realizadas.
		- Validar cumplimiento normativo de protección de datos personales.	- Evaluaciones de cumplimiento, diagnósticos legales.	- Incumplimiento de leyes como GDPR o leyes locales de protección de datos.

Fase	Objetivo	Prueba de auditoría	Evidencia esperada	Posibles hallazgos
Automatización	Validar la lógica y consistencia de los procesos automatizados.	- Comparar resultados del sistema con operaciones históricas o manuales. - Revisar los entornos disponibles. - Revisar validaciones configuradas en el sistema. - Comprobar los casos de prueba utilizados.	- Reportes del sistema vs. registros físicos o anteriores. - Entornos de desarrollo, pruebas y producción diferenciados. - Capturas/configuraciones de validaciones automatizadas. - Casos de pruebas y para cada caso los resultados obtenidos (registros de base de datos, documentos generados).	- Resultados inconsistentes, errores de cálculo o lógica de negocio. - No existe entorno de pruebas. - Validaciones no parametrizadas adecuadamente. - Inexistencia de los casos probados - Que en una AAA no se genere un acto administrativo válido.
	Validar las integraciones con otros sistemas.	- Revisar y realizar pruebas de integridad de las interfaces y APIs. - Revisar los controles sobre las interfaces.	- Reportes de los resultados con las integraciones vs resultados obtenidos por el operador.	- Resultados diferentes según el mecanismo de obtención de datos de otros sistemas.
	Comprobar que algoritmo funciona de manera fiable, continua y precisa.	- Verificar la existencia de herramientas automáticas para la monitorización, o comprobaciones manuales, frecuencia.	- Procedimientos de monitorización operativa, gestión de incidencias/errores, ficheros de log, políticas de retención de logs.	- Ausencia de monitorización y gestión de incidencias - Inexistencia de logs o períodos de retención muy cortos que no permiten cumplir con los requisitos de auditoría o investigación de incidentes.
		- Revisar logs de actividad de la ejecución del algoritmo.	- Ficheros o registro de la base de datos de logs, política de retención de logs, informes de permiso de acceso.	- Logs insuficientes, no protegidos (lo que permitiría su modificación) y período de retención inadecuado/insuficiente.
	Si se trata de una automatización crítica: verificar que existen planes y capacidades para asegurar su **continuidad** y/o **recuperación** en un plazo aceptable tras una interrupción y/o desastre.	- Identificación de los componentes relacionados con el algoritmo que sean críticos y las copias de respaldo. - Revisión del Análisis de impacto del negocio (BIA) y comprobar que la automatización está incluida.	- Procedimiento de copias de seguridad y evidencias de pruebas de restauración. - Documento BIA en el que establezca el Tiempo objetivo de recuperación (RTO)/Punto objetivo de recuperación (RPO)para la automatización. - Actas de reuniones en los que se haya discutido y, en su caso, aprobado la criticidad.	- Ausencia de copias de seguridad y pruebas de restauración no realizadas. - Inexistencia del BIA o RTO/RPO no definidos - Criticidad no evaluada formalmente.
		- Existencia de Planes de continuidad de negocio (BCP) o Plan de Recuperación ante desastres (DRP).	- Documento BCP/DRP.	- Inexistencia del BCP o DRP o no incluyen la recuperación de la automatización.
		- Pruebas del plan de recuperación que incluyan la automatización.	- Plan de pruebas. - Informes de resultados de las pruebas y/o actas. - Planes de acción que permitan subsanar o corregir las deficiencias identificadas tras la realización del plan de pruebas.	- Ausencia o insuficientes pruebas. - Resultados de pruebas no satisfactorias sin acción correctora.