Auditoría Pública nº 64 (2014), pp. 51 - 60

Julio García Muñoz
Auditor interno
Universidad de Castilla-La Mancha
Luis Álvarez Arderius
Técnico de auditoría
Audiencia de Cuentas de Canarias

Controles informáticos para la fiscalización de la nómina

Una guía de trabajo para complementar el tradicional control interno de legalidad

RESUMEN/ABSTRACT:

El presente artículo pretende resaltar la necesidad que presentan interventores, tesoreros y auditores internos para complementar la función tradicional del control interno de la gestión económico-financiera de las administraciones públicas, con el establecimiento gradual de controles y pruebas sobre los sistemas de información que soportan dicha gestión.. En la actualidad, la fiscalización interna de la gestión económico financiera del sector público se efectúa a partir de los datos obtenidos de las aplicaciones informáticas, en ocasiones sin cuestionarse si son correctos o no, sin probar previamente su validez o el correcto funcionamiento de la aplicación que los produce… Este escenario puede mejorarse implementando sencillos controles en el sof ware de gestión económica, de manera que los profesionales del control interno pueden, identificar y mitigar los riesgos de funcionamiento de estos sistemas, así como, en su caso, corregir errores en la información.

En concreto, el artículo propone una sencilla guía de trabajo para complementar la revisión de los programas informáticos que las administraciones públicas emplean para la gestión de sus retribuciones, resaltando asimismo los beneficios que aporta este enfoque de control interno para la mejora del alcance y efectividad de las actuaciones de los órganos de control externo.

T is article aims to highlight the need for public internal auditors and controllers of complementing the traditional Spanish Public Bodies' control on legal & economic management, with gradual introduction of internal controls on the information systems that support such management. Nowadays, the classic economic and financial control technics are largely done as of data, neither questioning at first whether data is correct or not, nor the validity of sof ware or the proper functioning of the IT system that produces the datasets… Such situation could be enhanced by applying easy to make trials on economic management sof ware, so that internal controllers can both identify and mitigate the IT system risks, and detect and correct likely data errors or inaccurate information.

Specifically, the article proposes a simple work guide to implement a step-by-step checking framework on Public Institutions payroll sof ware, also pointing out the value added benefits of a suitable internal control, in boosting improvements on the ef ectiveness of External Control Bodies' actions.

PALABRAS CLAVE/KEYWORDS:

FISCALIZACIÓN DE NÓMINA, RETRIBUCIONES PÚBLICAS, AUDITORÍA INFORMÁTICA, CONTROL INTERNO, CONTROL EXTERNO
SALARY AUDIT, PUBLIC REMUNERATION, COMPUTER AUDITING, INTERNAL CONTROL, EXTERNAL CONTROL

1. SITUACION ACTUAL DE LA FISCALIZACION DE RETRIBUCIONES EN LAS ADMINISTRACIONES PÚBLICAS

Los **gastos del personal al servicio de las administraciones públicas** representan, el desembolso más importante de cualquier Administración Pública y ref ejan asimismo la relevancia que tienen las retribuciones del personal en la configuración y posterior ejecución de sus **presupuestos**.

En cualquier administración, **la gestión de estos gastos se considera como elemento esencial o crítico**, tanto para aquellos que ostentan responsabilidades como para aquellos que se ocupan de procesos más técnicos, sobre todo teniendo en cuenta la **importancia** que tienen actualmente los **sistemas de información que soportan los procesos de gestión**, a la hora de administrar los recursos públicos.

Idéntica criticidad presentan los gastos de personal desde el **punto de vista del control** de la actividad económico-financiara del sector público, tanto en el ámbito del control interno como en el ámbito externo.

Cualquier administración pública necesita un **sistema de control interno adecuado** y capaz de proporcionar la suficiente seguridad con respecto a la salvaguarda de los activos o de los recursos corporativos, la fiabilidad de los registros contables y, en definitiva, de garantizar el buen funcionamiento de la organización.

A su vez, el examen y la evaluación del sistema de control interno constituye la base sobre la cual el **control externo** determina el nivel de fiabilidad de dicho sistema y, en consecuencia, establece el alcance y los procedimientos de control/fiscalización a llevar a cabo.

Obviamente, la **adecuación del sistema de control interno** de cualquier organización contribuye así a una **mejora en la gestión de los recursos públicos**.

En el contexto anterior, diversas variables contribuyen a que los **controles internos establecidos sobre los sistemas de información que soportan su gestión** adquieran una **importancia muy significativa**, variables tales como el volumen presupuestario que este tipo de gastos representa, el considerable número de perceptores, así como la diversidad de los puestos de trabajo vinculados a los mismos y la complejidad de la normativa que regula el personal de las administraciones, complejidad ésta última, a la que se suma la de los sistemas y el *so*f *ware* que soportan el proceso de gestión de este tipo de gastos.

La revisión de la **eficacia de los sistemas de información que soportan la gestión de la nómina** de cualquier administración para su fiscalización **no es, por tanto, una opción, sino una necesidad** que los responsables del control interno deben afrontar como complemento a los controles "tradicionales" que hasta ahora se vienen aplicando. Los responsables del control interno en cualquier administración deben "familiarizarse" con el entorno de las tecnologías de la información y las comunicaciones (TIC) y ser capaces de "enfrentarse" a procesos y sistemas de información.

Si bien la denominada "resistencia al cambio" puede condicionar cuándo comenzar con este enfoque del control, las posibles responsabilidades legales para los profesionales del sistema de control interno de cualquier administración pública (en materias tales como fraudes, pérdidas económicas, privacidad y confidencialidad de la información, revelación de secretos, suplantación de identidades, etc.), derivadas de la omisión del ejercicio de una parte de sus funciones, constituyen un argumento más que suficiente para tomar conciencia de la importancia de este tipo de controles.

¿Cómo arrancar sin experiencia previa o sin una formación informática al efecto? El presente artículo pretende aportar una sencilla guía de trabajo cuyos objetivos son:

1. Avanzar de una manera sencilla hacia **controles internos de naturaleza informática que complementan al tradicional control financiero o de legalidad**.
2. Aportar una mayor **seguridad** en la **legalidad** de la gestión de retribuciones públicas, evitando con ello incurrir en **responsabilidades** –contables, patrimoniales, penales, disciplinarias-.
3. Potenciar una **gestión eficiente de los recursos públicos destinados al control** interno de la gestión económico-financiera de las administraciones públicas, **evitando duplicidades** a través de una adecuada coordinación de los **órganos de control interno y externo**.

2. FISCALIZACION TRADICIONAL DE LEGALIDAD, ¿QUÉ DEJAMOS FUERA?

Si a día de hoy en su entidad no se ha realizado una **auditoría interna del sistema de información** (ASI) o **controles informáticos semejantes**, las fiscalizaciones de nómina mensuales que está realizando cuentan con una **significativa y constante limitación al alcance**: tener que **aceptar los riesgos existentes y confiar en la validez de "los datos"** que le suministra "la aplicación", sin realizar pruebas previas que evaluen la fiabilidad, integridad y seguridad del sistema de información de la organización, en general, y de la aplicación informática de retribuciones (en adelante, AIR), en particular.

Con independencia de quién y cómo aplique el control sobre la gestión de retribuciones, sea éste interven-

tor o auditor, a la hora de realizar un **control tradicional** de la nómina centrada en aspectos económicos o de legalidad, la siguiente figura podría sintetizar visualmente qué alcance controlamos y qué dejamos fuera.

SISTEMA DE INFORMACIÓN

De este contexto se deriva un verdadero *acto de fe* que se realiza sobre la validez de los datos, sin evaluar previamente los riesgos vinculados a la gestión de los mismos y sin realizar pruebas sobre la eficacia de los sistemas informáticos, el adecuado funcionamiento de los procesos de la aplicación de gestión de retribuciones o la integridad de las comunicaciones realizadas por las redes. **¿Podemos permitírnoslo? ¿Cómo podemos mejorar la eficiencia y calidad en la fiscalización interna de la nómina?**

Es necesario transformar el enfoque tradicional del control interno hacia un enfoque integral del sistema de control interno, a partir de la previa evaluación de los riesgos, que permita a los responsables del control interno, analizar también la relación entre los procesos de gestión (en este caso de la nómina) y los procesos y activos de las TIC.

Con este propósito, se plantea necesario, el diseño y realización de unos **controles internos informáticos**, con el **triple objetivo**:

a) **Validez/eficacia de resultados de control**: Asegurar **la validez de los resultados de las fiscalizaciones de nómina** que se realicen, en cuanto a de la información que contengan. No realizar "actos de fe" y determinar la confianza que concedemos a su control interno[1].

b) **Eficiencia del control interno. Reducir la carga de pruebas sustantivas a realizar por el interventor/tesorero/auditor interno**. Una vez se incremente el nivel de confianza en el Sistema de Información mediante pruebas de procedimiento, se empleará **menos tiempo en el control de la nómina y los recursos podrán ser optimizados** orientándolos hacia otras fiscalizaciones.

c) **Eficiencia del control externo. Mejorar la seguridad en el sistema de control interno de la administración pública de cara a facilitar (*suavizando*) las fiscalizaciones externas de las Instituciones de Control Externo (de las Comunidades Autónomas, del Tribunal de Cuentas de España y/o también del Tribunal de Cuentas Europeo).**

Resumiendo:

Δ Seguridad/Fiabilidad Sistema Control Interno AIR →▽ Alcance y Extensión Pruebas Externas

Resulta evidente por tanto que, ante una única tarea de control aparece más de un beneficiario: Órgano de Control Interno e Instituciones de Control Externo, evitando duplicidades de control.

3. UN PASO MÁS, FISCALIZACION DEL *SOFTWARE* DE RETRIBUCIONES. UN PROGRAMA DE TRABAJO PARA NO INFORMATICOS

Expuestas las razones por las que implementar controles informáticos en la AIR y ventajas generadas para el control interno y el control externo, **corresponde ahora abordar el cómo, el procedimiento y programa de trabajo** para implementar el control.

Las preguntas iniciales son evidentes **¿está preparado el interventor/tesorero/auditor interno tradicionalmente, centrado en controles de legalidad, economía y eficiencia, para una auditoría informática?** en la mayoría de los casos no….

Para ello, se propone a continuación un **programa de trabajo** para que el responsable del control interno, **sin experiencia** en auditorias informáticas, complemente **el control/la fiscalización de la nómina** a través de **sencillos puntos de control sobre la aplicación**

[1]De acuerdo con el punto 5.2. (Control Interno) de las Normas de Auditoría del Sector Publico de la IGAE (Res. 01.09.1998).

informática que soporta la gestión de retribuciones.

Paso a paso:

Como **planteamiento general**, nos encontramos las 3 fases clásicas presentes en toda organización de una actividad fiscalizadora.

3.1. Planificación: autoevaluacion del control interno y análisis de riesgos.

El objetivo de esta etapa inicial es realizar una (Auto) evaluación del sistema de control interno y análisis de riesgos, para concretar el universo de auditoría interna.

Si es la primera vez que el responsable del control interno afronta la realización de su primer control informático sobre la AIR, lo primero es, como en toda actividad fiscalizadora/auditora, realizar una **evaluación del sistema de control interno y un análisis de riesgos**. Ponernos en situación, para lo que es fundamental la **recopilación de toda la información y documentación** existente que sea de relevancia, solicitando al servicio de informática:

1. Manual de usuario de la AIR. Nos aporta información sobre los permisos de los distintos tipos de usuarios así cómo qué acciones/procesos pueden realizar.
2. Listado de las auditorias informáticas (o trabajos técnicos de control semejantes) que se hayan realizado sobre la AIR, tanto por la empresa propietaria del *sof ware* (si el soporte esta externalizado), como por los servicios informáticos de nuestra entidad.
3. Historial de actualizaciones relevante, fecha y su motivación. La frecuencia con la que se realizan modificaciones aportará información sobre la robustez y estabilidad de la AIR. En el ámbito retributivo público es frecuente que recurrentemente disposiciones legales alteren porcentajes de retención fiscal por IRPF, descuentos a percibir por maternidad, edad de los familiares a cargo, etc. Deberemos centrar el foco en aquellas que consideremos críticas para verificar que antes y después de los cambios, las transacciones de nómina eran correctas.
4. Historial de incidencias que tengan registrado los servicios TIC. (fecha, detalle, motivo, criticidad, etc.).

Una vez evaluada la información aportada y observado "el historial clínico del paciente", es momento de pasar de la planificación a la acción, esto es, diseñar e implementar controles y pruebas, verificando la existencia y el adecuado funcionamiento de los puntos clave que afectan a la AIR.

3.2 Ejecución de los controles

Por su tipología, podemos diferenciar entre **controles generales del sistema y controles específicos de la aplicación de gestión de retribuciones**.

3.2.1 Revisión de los Controles Generales del entorno informático.

Presentan una importancia capital, puesto que son el **primer punto de control que "frena" potenciales errores y acota las vulnerabilidades** del sistema en su conjunto. Si éstos no existiesen o no funcionasen de manera efectiva, los controles específicos que la AIR pudiera tener, presentarían una mayor exposición al fallo o a prácticas fraudulentas[2].

A modo de ejemplo, dos **sencillos controles** que podemos realizar consistirían en **identificar y describir** los siguientes puntos.

[2]En línea con lo señalado por la Sindicatura de Comptes de la Comunidad Valenciana, Minguillón Roy, Antonio. (2010) *La auditoría de sistemas de información integrada en la auditoría financiera. La perspectiva del sector público*. Pág. 153.

1. Controles de organización y dirección. ¿Tiene la organización una política formal de seguridad informática? ¿Existe designado un responsable de seguridad? ¿Existen incidencias de manera frecuente en el área TIC? ¿Qué repercusión y alcance tienen (pérdidas económicas, de datos,…)? ¿Cómo son gestionadas las caídas del sistema? ¿existe un protocolo de recuperación o respaldo de datos?

2. Política de contraseñas. Longitud de la clave, robustez por la obligatoriedad de uso combinado de letras y números, mayúsculas, minúsculas y caracteres especiales, frecuencia de cambio, seguridad física y lógica de los servidores donde se almacenan y recuperan las contraseñas olvidadas o bloqueadas por el sistema ante intentos fallidos o ataques de *so*f *ware* malicioso…

3.2.2 Revisión de los Controles Específicos sobre la AIR

El objetivo de estos controles consiste en garantizar que **todas las transacciones son autorizadas y registradas, y que son procesadas de forma completa, adecuada y oportuna**[3].

3.2.2.1 Roles y permisos. Segregación de funciones

Un factor esencial para el adecuado control de todo proceso de gestión corporativa, informático o en papel, es la existencia de la debida **segregación de funciones clave**. Nos centraremos en identificar cuáles son los roles y las funciones críticas ejecutadas en el servicio de informática/TIC (procesos y trabajos *backo*f *ce* o *backend*) respecto a la AIR y que, al igual que los ordenadores de gasto y pago, deben estar perfectamente separadas.

El principal punto de atención debe recaer sobre **los roles de programador y operador**[4] del *so*f *ware*. De cara a incrementar la prevención de posibles fraudes, dichas funciones deben recaer sobre responsables diferentes. Es frecuente que, debido a la falta de personal, recursos y/o capacidades de las plantillas de las administraciones públicas, se produzca una concentración de funciones en una persona o en una unidad determinada, pudiendo explotar y modificar la AIR con fines malintencionados o intereses particulares.

Llegado este punto, debemos observar la **postulación de ISACA**[4] respecto de cómo entender la segregación de funciones operador-programador, señalando que **"no debería limitarse solo a los puestos ocupados, sino que debería extenderse a los conocimientos y/o habilidades"**.

Respecto a los roles y permisos, el interventor/tesorero/auditor deberá establecer un **control interno permanente que permita la trazabilidad posterior respecto a los accesos lógicos**. Sugerimos la solicitud del **historial de roles y permisos de usuarios (Externos e Internos)** con un alcance de 3-4 años[5] para tener una cierta perspectiva inicial. **El modelo que aportamos** contendría los **parámetros de control básicos** a nivel de usuario.

Historial de roles y permisos de usuarios
Objetivo de la prueba: Correcta segregación de funciones como garantía de un adecuado Sistema de Control Interno.

FECHA EVENTO	TIPO DE ROL O PERMISO	DESCRIPCIÓN DEL PERMISO	INICIO CONCESIÓN	FIN CONCESIÓN	USUARIO	EXTERNO O INTERNO
Alta/Baja/Modificación de permiso					Nombre Apellidos	

Obtenida la panorámica que nos aporta este modelo descriptivo, deberemos **evaluar y concluir sobre la adecuación de la segregación de funciones en la AIR y el control de accesos lógicos a la misma**. La experiencia señala que frecuentemente existe un determinado número de personas que tendrán permisos sobre todos los procesos/tareas que conforman el ciclo de gestión y pago de la nómina...

3.2.2.2 Las pruebas sustantivas como refuerzo

Al partir de la consideración de que no somos fiscalizadores con capacidades informáticas, existe una dificultad adicional para implementar pruebas de procedimiento sobre el *software*, ya que el uso de técnicas de análisis de datos mediante herramientas informáticas[7], tratamiento mediante procesos de negocio, registros de transacciones de la AIR, etc., serán

[3]Misma referencia bibliográfica que nota anterior, pág. 159.
[4]ISACA, *Information Systems Audit and Control Association*.
[5]De la evaluación previa de riesgos pueden desprenderse eventos que requieran un alcance temporal distinto o incluso poner el foco en un periodo específico (por ejemplo, una migración de una aplicación a otra, si ha habido una actualización crítica con incidencias de relevancia, etc.).
[6]CAATs (*Computer Assisted Audit Techniques*). ACL e IDEA, como *so*f *ware* más extendido.
[7]Vidal Barberà, Albert y Chico Martínez, Francisco Julián (2010). Cómo tomarse el capítulo I como algo personal y no morir en el intento. *Auditoría Pública* nº 50

conceptos de más difícil manejo para el Interventor/Tesorero o Auditor Interno tradicional. Por ello, el programa de trabajo propuesto lo hemos centrado en pruebas sustantivas. En nuestro caso de estudio, las retribuciones públicas, recomendamos específicamente las siguientes.

- **Errores por entrada manual de datos**. Revisión en detalle de aquellos datos que deben introducirse manualmente o cuya captura no sea automatizada o semiautomatizada, sino que se efectúa mediante una transacción/procedimiento aislado con el subsiguiente incremento del riesgo de errores en la captura de datos. Habremos de valorar la probabilidad de ocurrencia de fallos y el posible impacto económico.
- **Retribuciones variables no periódicas en su devengo**. Por su especial riesgo e incidencia se debe prestar atención a los pagos por productividad, pagos extraordinarios por prestación de servicios fuera del horario habitual, encomiendas de servicios extraordinarios no directamente vinculados con las tareas de un puesto de trabajo, etc. Se revisará el procedimiento de cálculo de cuantía, la documentación soporte que justifique su percepción...
- **Sistema de alertas e incidencias relevantes**. Creación de alertas automáticas para aquellas retribuciones que superen un determinado importe determinado por normativa o contrato (posteriormente revisadas como control permanente). En el foco: indemnizaciones por razón del servicio, asistencias, ayudas sociales particulares, compatibilidades para segundos puestos de trabajo.

  Un segundo punto de atención, sobre controles específicos para las **incidencias más relevantes**[7] **del área de retribuciones y establecer puntos de control en la aplicación**:
  - Percepción de retribuciones indebidas, sin justificar.
  - Errores en el prorrateo de las pagas extraordinarias y cobros indebidos de éstas por parte de cargos electos con dedicación.
  - Retribuciones por incentivos o productividad no vinculadas al cumplimiento real de objetivos o por un importe fijo prorrateado mensualmente.
  - Percepción de indemnizaciones o finiquitos improcedentes y cláusulas indemnizatorias que no se ajustan a la normativa.
  - Utilización de cheques al portador para realizar pagos de gratificaciones.
  - Retención incorrecta o falta de retención del IRPF.
- **Totalizaciones**. Revisión, para uno o varios meses, de que la retribución mensual ordinaria y periódica en su devengo (la *nómina*), basada en cálculos automáticos, se totaliza de manera exacta para el conjunto de perceptores.
- **Existencia de copias de seguridad o *backups* y respaldo del sistema**. El primer punto a verificar es su existencia. Si no se realizan copias de los datos críticos para abonar las retribuciones mensuales estaríamos ante un serio indicador de riesgo. Si los *backups* existen, la disponibilidad, accesibilidad (tiempo y facilidad) a los datos para su recuperación y la frecuencia de almacenado serían variables a estudiar.

3.3. Informe de fiscalización y establecimiento de controles periódicos

El objetivo de esta fase consiste en plasmar por escrito las principales conclusiones que hemos evidenciado durante la ejecución de los controles, contemplando de una manera constructiva aquellas deficiencias que necesitan subsanarse para evitar la incurrencia en riesgos económicos por la realización de pagos no ajustados a legalidad.

Dichas conclusiones preliminares o reparos, serán trasladados a los responsables de gestión para que aporten las **alegaciones** que consideren oportunas. Transcurrido este trámite, el **informe de control alcanza el estado de definitivo** y se deberá trasladar al responsable jerárquico.

En este punto, para **dotar nuestro trabajo de un verdadero valor añadido**, cada conclusión o corrección a realizar deberá llevar asociada una **recomendación** para subsanarla, no debiendo olvidar los aspectos clave de su **contenido**:

1. Una propuesta realista de acciones.
2. Valoración económica del riesgo que se evita.
3. Nombramiento de un responsable.
4. Plazo para su ejecución.
5. Recursos necesarios.

Se deberán **priorizar** las recomendaciones atendiendo a su importancia o **criticidad**. Asimismo, trascurrido el tiempo asignado, deberemos realizar un **seguimiento** para verificar su adecuada implementación.

¿Ya está? Aún podemos sacar más jugo a los resultados del trabajo realizado y dando un pequeño paso más seremos capaces de establecer una estructura de control permanente. Nuestra propuesta consiste en que, finalizada la primera fiscalización en la que se incorporen controles internos informáticos, el

interventor/tesorero/auditor interno realice una **circularización periódica al responsable de la AIR** o al Jefe de Servicio TIC. De esta manera **no tendrá solo la foto estática** que aporta un informe, **sino que el control** sobre cambios e incidencias importantes que atañan a la AIR será **continuo y dinámico**. Para ello os sugerimos el empleo de diversas herramientas:

1. Cuestionario para la evaluación **anual** de la fiabilidad de la AIR.
2. Cuestionario para la evaluación **mensual** (o frecuencia diferente, pero inferior a la anual) de la fiabilidad de la AIR.
3. Cuestionario/revisión del procedimiento de autorización y asignación de permisos y responsabilidades (véase modelo en apartado 3.2.2).

Recordemos, la mayoría de nosotros no somos expertos, ni auditores informáticos: el camino más fácil es preguntar y analizar. Usemos una circularización periódica para revisar el estado de los principales puntos de control. En los dos primeros casos, los extremos de la AIR a verificar incluirían una revisión similar a la detallada en el Anexo 2, cuyos parámetros principales serían:

1 Actualizaciones.
2 Soporte y mantenimiento.
3 Compatibilidad con el resto de los sistemas de información.
4 Seguridad de la información.
5 Integridad de la información empleada para el pago de la nómina.

Recomendamos una **frecuencia anual mínima**. Asimismo, en función de los resultados obtenidos en la primera fiscalización de la AIR, el responsable del control interno determinará si son necesarias circularizaciones semestrales, trimestrales,… La **situación ideal** que aportaría mayores garantías de control al pago de retribuciones públicas sería contar, **mensualmente** y antes de pagar la nómina, con un cuestionario de control remitido al servicio de control y/o tesorería que hubiera sido cumplimentado por el responsable de la aplicación.

Habremos pasado de realizar actos de fe a fiscalizar los gastos de personal, basándonos en procedimientos técnicos y contando con garantías acerca del adecuado funcionamiento del sistema informático y de la aplicación de gestión de retribuciones.

4. CONCLUSIONES

Tal y como se ha venido señalando a lo largo del artículo, los responsables del control interno de cualquier administración pública deben ser capaces de enfrentarse a la necesidad de identificar los riesgos existentes en los sistemas de información y revisar la eficacia de los procesos que soportan su gestión económico financiera, en general, y la de las retribuciones públicas, en particular.

Como conclusión, queremos señalar cómo con un mínimo esfuerzo de control, casi sin necesidad de una formación específica, el interventor, tesorero o auditor interno, tradicionalmente centrado en controles de legalidad o económico-financieros, tiene a su alcance la posibilidad de dar pasos hacia controles internos informáticos, ampliando así fácilmente su alcance y revisando:

1. Funciones y obligaciones del usuario gestor de la AIR.

2. Segregación de funciones en roles y responsabilidades.
3. Identificación y autenticación de usuarios.
4. Registro de incidencias y control de acceso lógico.

De cara a futuro, las fiscalizaciones y trabajos de control interno venideros verían su **evolución natural** focalizándose en aspectos tales como:

A. Gestión de soportes de servicios e infraestructuras TIC, a través de auditorías operativas/informáticas sobre la eficiencia y seguridad de la gestión interna o de los contratos externalizados vinculados a las TIC.

B. Revisiones internas integrales de los procesos de gestión, que permitan evaluar la eficacia y la eficiencia de los Sistemas de Información.

C. Revisiones específicas de los sistemas de información que soportan los procesos de gestión, tales como aquellos vinculados al **sistema de gestión de la seguridad de la información** (SGSI). Indicativamente se podría comenzar por la inclusión de controles internos informáticos en el documento de seguridad de los sistemas de información de la entidad y la concreción de un responsable de su gestión.

5. BIBLIOGRAFIA

Minguillón Roy, Antonio (2010). La auditoría de sistemas de información integrada en la auditoría financiera. La perspectiva del sector público. Sindicatura de Comptes de la Comunidad Valenciana.

Piattini, Mario Gerardo. y Del Peso Navarro, Emilio (1998). Auditoría Informática. Un Enfoque Práctico. Ed. RA-MA.

Piattini, Mario Gerardo, Del Peso Navarro, Emilio y Del Peso Ruiz, Mar. (2008). Auditoría de Tecnologías y Sistemas de Información. Ed. RA-MA.

ISACA (2009). Marco para la Auditoría de los Sistemas de Información. Asociación de Auditores y Auditoría y Control de Sistemas y Tecnologías de la Información y las Comunicaciones. Madrid.

Instituto de Auditores Internos de España (2014). Cobertura del Riesgo Tecnológico: hacia una Auditoría Interna de TI Integrada.

The Institute of Internal Auditors (2012). Normas Internacionales para el ejercicio profesional de la Auditoría Interna.

Intervención General de la Administración del Estado IGAE (1998). Normas de Auditoría del Sector **Público.**

Órganos Públicos de Control Externo del Estado Español. Principios y Normas de Auditoría del Sector Público.

Vidal Barberà, Albert y Chico Martínez, Francisco Julián (2010). Cómo tomarse el capítulo I como algo personal y no morir en el intento. *Auditoría Pública* nº 50.

ANEXOS

I. Programa de trabajo. Fiscalización informática AIR.

PROGRAMA DE TRABAJO		
SISTEMA DE INFORMACION Y APLICACIÓN DE RETRIBUCIONES		
DESCRIPCIÓN DEL TRABAJO		**Refª P.T.**
1. Definición de **objetivos** perseguidos	Asegurar un grado de control razonable respecto a la **integridad, fiabilidad y seguridad**, tanto del **Sistema de Información** General de la Institución (entorno informático), como de la. **Aplicación de Gestión de Retribuciones**.	

FASE DEL TRABAJO		PRUEBAS/FASE	Refª P.T./ Doc Soporte
A. PLANIFICACIÓN	EVALUACIÓN DEL **SISTEMA DE CONTROL INTERNO** Y ANÁLISIS DE **RIESGOS**	1. Manual de usuario de la AIR. 2. Listado de las Auditorias Informáticas (o trabajos técnicos de control semejantes) que en se hayan realizado sobre la AIR. 3. Historial de actualizaciones relevante, fecha y su motivación. 4. Historial de incidencias que tengan registrado los Servicios TIC. (Fecha, detalle, motivo, criticidad, etc.).	Documentación analizada
	CONTROLES GENERALES DEL SISTEMA INFORMÁTICO	5. Controles de organización y dirección. 6. Política de Contraseñas. (frecuencia de cambio, longitud mínima.	Directrices, Manuales y Políticas de la Dirección/Dirección TIC
B. EJECUCIÓN DE LOS CONTROLES	**CONTROLES ESPECÍFICOS** SOBRE LA APLICACION	7. Roles y permisos. Segregación de funciones. 8. Pruebas Sustantivas. 1.1. Errores por entrada manual de datos. 1.2. Retribuciones variables no periódicas en su devengo. 1.3. Sistema de Alertas e Incidencias Relevantes. 1.4. Totalizaciones. 1.5. *Backups* y respaldo del sistema. 9. Control de accesos lógico: Identificación y autenticación de usuarios. 10. Registro de incidencias.	Manuales, Papeles de Trabajo, Listados de Accesos e Incidencias.
C. CONCLUSIÓN E INFORME	INFORME PROVISIONAL ALEGACIONES INFORME DEFINIFIVO	11. Se elabora informe provisional que contiene las incidencias más relevantes detectadas en la revisión efectuada, y se da traslado de las mismas a los responsables administrativos de las unidades correspondientes. 12. Se concede un plazo para la presentación de alegaciones (de acuerdo con lo dispuesto en la normativa o directrices de la Unidad). 13. Una vez recibidas las alegaciones, en su caso, se contestan las mismas, procediendo a su modificación (parcial o total) en el informe provisional, en caso de que sean consideradas suficientes por la Unidad de Control Interno. 14. Una vez expirado el plazo de presentación de alegaciones, se elabora el informe definitivo, donde se recoge copia de las alegaciones presentadas, en su caso. 15. Se supervisa el informe definitivo por parte del responsable de la Unidad. al/los órgano/s competente/s, junto con un escrito resumen con las conclusiones y recomendaciones más significativas.	Informe de Controles Informáticos que soportan y garantizan la integridad y validez de los datos de fiscalización de nómina
D. SEGUIMIENTO Y MEJORA	DE RECOMENDACIONES	16. A los seis meses siguientes de emitido el informe, se realiza un seguimiento de recomendaciones. La frecuencia debe establecerse en función de la relevancia y tiempo de implementación requerido de las recomendaciones.	Informe de Seguimiento de Recomendaciones
	PUNTOS DE CONTROL PERMANENTES	17. Cuestionario para la evaluación anual de la fiabilidad de la *app*. 18. Circularización periódica (mensual/trimestral/…) previa a la fiscalización de la nómina (sobre eventos/controles informáticos).	Cuestionario Modelo de Circularización

II. Modelo de cirularizacion al servicio TIC

Servicio de Intervención/Tesorería/Control Interno **Fecha**

Sr. Director del Área de Tecnología y Comunicaciones,

Asunto: Solicitud Mensual de Información sobre la aplicación informática de gestión de retribuciones.

Estimado/a….

Con motivo de la fiscalización mensual de la nómina de los trabajadores que ordinariamente lleva a cabo este servicio, es necesario que antes del día…., para poder proceder al pago de la misma, remita la información que se le solicita, relativa a la integridad y seguridad de la información de la aplicación informática que gestiona las retribuciones (AIR) de esta institución.

#	PREGUNTA	SI	NO	OBSERVACIONES
1	Han existido **actualizaciones** de la AIR. En caso afirmativo, detállelas y valore su efecto.			
2	Los trabajos de **soporte y mantenimiento** de la AIR se han desarrollado sin incidencias.			
3	La **compatibilidad** de la AIR con el resto del Sistema de Información			
4	La **seguridad de la información** de la AIR, así como aquellas otras fuentes que integran sus datos en la misma, no se ha visto comprometida por en el periodo considerado.			
5	En la AIR han existido **incidencias** significativas que han podido afectar a la **integridad** de la información empleada para el pago de la nómina. En caso afirmativo, detállelas y valore su efecto.			
6	**Otros aspectos/eventos** de relevancia que afecten a la AIR para el pago de la nómina. Detalle y valórelos.			

Toda la información aportada se refiere al periodo INICIO-FIN

Fecha y Firma del Responsable/Director del Servicio de Tecnología y Comunicaciones

Sin otro particular, y agradeciendo su colaboración, reciba un cordial saludo.

Atentamente, El Interventor/El Tesorero/El Director del Servicio de Control Interno