1. Introducción y objetivos de la guía

Las Normas Técnicas de Auditoría (ver MFSC-1310) tienen implícito un concepto fundamental: el auditor, al planificar una auditoría, debe identificar y valorar los riesgos de auditoría que pueden existir al ejecutar el trabajo y emitir su informe; teniendo en cuenta ese análisis se debe diseñar un conjunto equilibrado de procedimientos de forma que los riesgos queden reducidos a un nivel aceptable a la hora de emitir el informe de auditoría.

Muy esquemáticamente, las etapas de una auditoría ejecutada con el enfoque basado en el análisis de los riesgos son:

- Conocimiento de la entidad
- Análisis de las cuentas anuales auditadas: Identificación de los saldos, transacciones y clases de transacciones significativas. Identificación de las actividades, de los procesos de gestión significativos, de las aplicaciones que los soportan y de los flujos de datos relacionados.
- Valoración de los riesgos tanto a nivel global como de las afirmaciones e identificación de las áreas significativas.
- Revisión de los controles generales.
- Adquisición de un conocimiento de los procesos de gestión significativos, de las aplicaciones significativas y de las principales interfaces.
- Identificación de los riesgos y de los controles clave de los procesos y de las aplicaciones de gestión significativas.
- Realización de pruebas de recorrido o paso a paso y evaluación del diseño de los controles.
- Realización de pruebas del funcionamiento de los controles clave.
- Realización de procedimientos sustantivos.
- Análisis de los hallazgos, elaboración de las conclusiones y del informe.

El gasto de personal de una entidad es el resultado de la agregación de un gran número de transacciones de importes relativamente poco significativos, que de ordinario se gestionan con sistemas de información complejos y cada vez más automatizados e integrados. En estas situaciones, especialmente en las entidades **de tamaño mediano o grande llegar a una conclusión de auditoría (positiva o negativa) sólo con pruebas sustantivas es, en la práctica, imposible**, siendo preciso confiar en cierta medida en los controles internos existentes en los procesos de gestión y, por tanto, deben hacerse pruebas de auditoría sobre el eficaz funcionamiento de los mismos.

Los **objetivos** de la presente Guía de fiscalización del área de personal son ayudar al auditor a:

- Comprender los procedimientos (proceso de gestión) establecidos por la entidad para iniciar, autorizar, registrar, procesar e informar (en las cuentas anuales) de las clases de transacciones significativas relacionadas con la gestión de personal, desde que se formaliza la necesidad de aumentar la plantilla, hasta el pago de la nómina y el cumplimiento de las obligaciones legales relacionadas.
- Identificar y valorar los riesgos de auditoría existentes en el proceso de gestión de personal/nóminas.
- Comprender los controles que la entidad auditada ha establecido en el proceso de gestión, analizarlos, y determinar cuáles de ellos pueden considerarse controles relevantes o controles clave (los que contribuyen a reducir el riesgo de auditoría).
- Diseñar las pruebas de auditoría más adecuadas para probar la eficacia del diseño y el funcionamiento de los controles clave.
- Establecer los procedimientos mínimos recomendados para la fiscalización del área de gastos de personal, incluyendo un contenido orientativo del programa de auditoría.
- Documentar los procedimientos ejecutados, la evidencia obtenida y las conclusiones alcanzadas.

La adecuada comprensión de esta guía requiere el conocimiento previo de las secciones 1310, 1315 y 1330 del MFSC.

2. Ámbito subjetivo de aplicación

Esta guía está diseñada para la fiscalización de empresas y fundaciones públicas que aplican el PGC así como para la fiscalización del capítulo 1 de entes públicos con contabilidad presupuestaria.

3. Ámbito objetivo de aplicación

La guía es aplicable a la fiscalización/auditoría de las áreas comprendidas en el ciclo que abarca los procesos de presupuestación, gestión[1] de personal (puestos y personas), elaboración de la nómina, su pago, reintegros y contabilización, y de los acreedores y deudores relacionados. En particular las cuentas a las que son de aplicación las orientaciones de la presente guía son:

De carácter financiero:

a) Gastos de personal

   64 Gastos de personal

b) Otras cuentas a pagar

   46 Personal
   47 Otras deudas con las administraciones públicas

c) Deudores comerciales y otras cuentas a cobrar

   46 Personal

De carácter presupuestario:

a) Capítulo 1 de gastos

Hay que tener presente que las cuentas de gastos personal están íntimamente relacionadas con las de deudas con administraciones públicas por las retenciones a cuenta del IRPF y las de organismos de la Seguridad Social Acreedores por las cotizaciones sociales, de forma que la evidencia de auditoría que respalde las primeras también sirve para soportar las segundas y viceversa. Por esta razón la planificación y ejecución de la auditoría de estas áreas debe realizarse siempre de forma conjunta y coordinada.

Cuando el alcance de una fiscalización esté limitado a la auditoría de los gastos de personal, aunque no se diga expresamente, se debe entender incluido en ese alcance la auditoría de las cuentas de activo y pasivo relacionadas, sus saldos y movimientos de cargo y abono.

---

[1] **Definiciones (ver también MFSC-1310):**

Un **proceso de gestión** (proceso de negocio) consiste en una serie de actividades, operaciones o funciones (manuales, semiautomáticas o automatizadas) llevadas a cabo por una entidad, que sirven para llevar a cabo su misión y desarrollar su actividad (la elaboración de productos o el suministro de servicios) o el tratamiento de la información. Un proceso tiene un punto de inicio y otro de finalización claros y generalmente intervienen varios departamentos de la entidad.

Un **subproceso** o función es un subconjunto de actividades o tareas, realizadas por un empleado o funcionario para llevar a cabo una parte de sus responsabilidades, que producen un resultado u output.

Por **procesos de gestión significativos**, a los efectos de la auditoría, se entiende los principales procesos que tienen una influencia directa sobre el flujo de tratamiento contable y la formación o valoración de componentes significativos de las cuentas anuales.

Una **aplicación de gestión** (o aplicación de negocio) es una combinación de hardware y software usada para procesar información de la actividad de la entidad. Puede dar soporte a uno o varios procesos de gestión.

Una **aplicación significativa** a los efectos de la auditoría financiera es aquella que procesa transacciones agregadas superiores al nivel de importancia relativa fijado en la memoria de planificación o si respalda un saldo contable significativo de las cuentas anuales auditadas. El auditor también puede identificar aplicaciones contables como significativas basándose en consideraciones cualitativas. Por ejemplo, sistemas que respaldan la planificación financiera, los informes de gestión y actividades presupuestarias; sistemas que gestionan y proporcionan datos e información de costes; y sistemas que gestionan aspectos relacionados con el cumplimiento de la legalidad (contratación, subvenciones, etc.).

Una **interfaz** es una conexión entre dos dispositivos, aplicaciones o redes, mediante la que se intercambia información. Incluso los entornos ERP (Enterprise Resource Planning) muy integrados a menudo requieren complicadas interfaces para intercambiar información con otras aplicaciones distribuidas.

El riesgo de incorrección material (**RIM**), es el riesgo de que las cuentas anuales contengan incorrecciones materiales antes de la realización de la auditoría.

4. Objetivos de la auditoría

La finalidad u objetivo global de la auditoría del área de gastos de personal consiste en obtener evidencia suficiente y adecuada sobre si las cuentas de gastos de personal reflejan de forma razonable el gasto realmente devengado durante el periodo de acuerdo con las normas contables o presupuestarias aplicables y si la gestión se ha realizado de conformidad con la normativa aplicable[2].

Dicho de otra forma, debemos evaluar si las afirmaciones que subyacen en cada componente o cuenta señalada en el apartado 3 anterior son válidas.

Las afirmaciones son el elemento central para la identificación de los riesgos y de los controles y para seleccionar los procedimientos de auditoría más eficaces en la obtención de esa evidencia.

Los **objetivos** de auditoría para el área de **gastos de personal** relacionados con las **afirmaciones** son:

Objetivos de auditoría del área de gastos de personal	Afirmaciones[3]
A. Los procedimientos de contabilidad aplicados están operando de forma efectiva como para presentar adecuadamente el coste de personal devengado en el período.	Existencia Integridad Fiabilidad
B. Los gastos de sueldos y salarios del período son autorizados, revisados y calculados correctamente por el personal responsable.	Fiabilidad
C. Los gastos por sueldos y salarios y otros beneficios sociales están correctamente contabilizados en cuanto a importe, naturaleza y período.	Fiabilidad
D. Las altas y bajas de personal, sus funciones y retribuciones, son conformes con la normativa aplicable.	Legalidad
E. Los procedimientos de gestión y las normas de control interno definidas por la dirección son adecuados para asegurar un control efectivo de la gestión de los asuntos de personal, cálculo de la nómina, contabilización y pago, y han funcionado adecuadamente en el periodo auditado[4].	Existencia Integridad Fiabilidad Legalidad

La conclusión global de auditoría del área debe ser inequívoca, debe expresar la opinión profesional (basada en la evidencia obtenida tras todas las pruebas de auditoría realizadas) sobre si la cifra de gastos personal que reflejan las cuentas anuales es correcta y si la gestión ha sido conforme con la normativa.

[2] Objetivos coincidentes con los establecidos en el artículo 8.3 de la Ley 6/1985 de Sindicatura de Comptes (MFSC-1).

[3] MFSC-1315.5: Las afirmaciones ayudan a comprender al auditor los riesgos que se pueden materializar partiendo de la base de que las afirmaciones son las declaraciones que un tercero interesado esperaría encontrar en los estados financieros.

Teniendo en cuenta lo anterior, el auditor debe esperar que la información financiera cumpla con las siguientes afirmaciones dentro la gestión de personal/nómina para que la preparación y publicación de información financiera sea confiable y para el cumplimiento con las leyes y normas aplicables.

Afirmación combinada	Afirmación	**Descripción** (afirmaciones relacionadas con los gastos)
Existencia	Acaecimiento (*ocurrencia*)	Las transacciones y hechos registrados han ocurrido y corresponden a la entidad
Integridad	Integridad	Se han registrado todos los hechos y transacciones que tenían que registrarse
Fiabilidad	Exactitud	Las cantidades y otros datos relativos a las transacciones y hechos se han registrado adecuadamente
	Corte de operaciones	Las transacciones y los hechos se han registrado en el período contable correcto
	Clasificación	Las transacciones y los hechos han sido registrados en las cuentas adecuadas
Legalidad	Legalidad	Se ha cumplido la legalidad vigente en la gestión de los gastos.

[4] Ver artículo 58 del RRI de la Sindicatura (MFSC-2).

Los **objetivos** de auditoría para el área de **otras cuentas apagar** y las afirmaciones relacionadas son:

Objetivos de auditoría del área de Otras cuentas a pagar	Afirmaciones relacionadas[5]
A. Las otras cuentas a pagar (46 y 47) están adecuadamente incluidas en el período al que corresponde de acuerdo con el principio de devengo.	Existencia Integridad Derechos y obligaciones
B. Las cuentas a pagar están descritas y clasificadas en forma adecuada y las revelaciones necesarias están incluidas en las cuentas anuales y en las notas correspondientes de la memoria.	Derechos y obligaciones Valoración

5. Adquirir una comprensión de los procedimientos de gestión del personal

a) Introducción

Para poder diseñar pruebas de auditoría eficaces, que permitan alcanzar el objetivo pretendido al auditar los gastos de personal, es necesario conocer los procedimientos de gestión de personal que tenga implantados la entidad fiscalizada.

No se puede auditar algo cuyo funcionamiento se desconoce.

Por tanto, una de las primeras tareas de la auditoría del área consistirá en adquirir un conocimiento de la entidad que permita comprender:

- Los procedimientos, tanto manuales como automatizados, mediante los que las transacciones relacionadas con la gestión del personal son iniciadas, autorizadas, procesadas e incorporadas a las cuentas anuales.
- Cómo se resuelven los procesamientos incorrectos de transacciones.
- Cómo se reconcilian los saldos detallados *(auxiliares)* con el mayor general.
- Los archivos contables relacionados con la gestión de personal, tanto manuales como digitales (bases de datos), la información soporte y las cuentas específicas que guardan relación con el inicio, la autorización, y el procesamiento de las transacciones.
- La aplicación informática que soporta el proceso de gestión de personal/nóminas.

En cada entidad habrá ligeras variaciones, pero básicamente nos interesa conocer el proceso de gestión de personal o recursos humanos y de elaboración de las nóminas hasta su pago. Debemos conocerlos de forma clara para identificar dónde puede haber algún riesgo que afecte a las cuentas anuales y así poder centrar nuestras pruebas de auditoría en esos riesgos.

[5] Las afirmaciones ayudan a comprender al auditor los riesgos que se pueden materializar partiendo de la base de que las afirmaciones son las declaraciones que un tercero interesado esperaría encontrar en los estados financieros.

Teniendo en cuenta lo anterior, el auditor debe esperar que la información financiera cumpla con las siguientes afirmaciones sobre los saldos acreedores relacionados para que la preparación y publicación de información financiera sea confiable y para el cumplimiento con las leyes y normas aplicables.

Afirmación	**Descripción** (afirmaciones relacionadas con cuentas de balance)
Existencia	Los activos, pasivos y patrimonio neto existen.
Integridad	La entidad posee o controla los derechos de los activos y los pasivos son obligaciones de la entidad.
Derechos y obligaciones	Se han registrado todos los activos, pasivos e instrumentos de patrimonio neto que tenían que registrarse
Valoración e imputación	Los activos, pasivos y el patrimonio neto se muestran en las cuentas anuales por sus importes adecuados y cualquier ajuste de valoración o imputación resultante está debidamente registrada
Legalidad	Se ha cumplido la legalidad vigente en la gestión de los gastos.

b) Memorándum/narrativa

Para facilitar la adquisición del conocimiento de los procedimientos de gestión se puede utilizar el formulario modelo que se adjunta como MFSC-2861.1, pero también puede utilizarse un memorándum o narrativa alternativa a ese modelo que sea lo suficientemente claro y descriptivo.

Si la entidad dispone de procedimientos formalizados por escrito, la narrativa a realizar por el auditor será tanto más breve cuanto más completos y claros sean aquéllos, que serán archivados completos en el Archivo Permanente de la entidad y un resumen (tan extenso como se considere necesario) también en el Archivo Corriente (TeamMate), y estarán adecuadamente referenciados.

Debe entrevistarse a las personas responsables de las distintas tareas y realizar pruebas de recorrido para confirmar que nuestra comprensión de los procedimientos aplicados es correcta, es decir, que la descripción se corresponde con los procedimientos ejecutados en la práctica por la entidad.

c) Descripción gráfica

En cualquier caso, se recomienda vivamente complementarlos con diagramas de flujo y tablas de riesgos y controles. Cuando se trata de procesos de gestión complejos como el que estamos estudiando, se empezará dibujando el mapa del proceso o flujograma general (como el del ejemplo siguiente), señalando los principales subprocesos o funciones que posteriormente se han de describir con mayor detalle.

Para hacer el análisis de los riesgos y controles con mayor precisión conviene disponer cuanto antes de un flujograma del proceso de gestión analizado.

El proceso de gestión de personal y nóminas está siempre soportado por aplicaciones informáticas que pueden abarcar todas las actividades relacionadas, desde la solicitud interna de contratación de personal, selección, contratación, funciones del puesto a cubrir y retribución, control de presencia, etc. Es habitual que la aplicación de nóminas sea independiente de las aplicaciones de gestión de gestión económica y contable, por lo que habrá que tener especial cuidado al analizar la interfaz que relaciona ambas aplicaciones.

La gestión de la nómina consiste en ejecutar cálculos periódicos del coste de los salarios de los empleados, elaborar las nóminas individuales y proporcionar la información para su contabilización y pago.

La elaboración de la nómina solo será exacta si: a) se utiliza información de los ficheros maestros que sea completa y exacta; b) si la información de altas y bajas (y tiempo trabajado) ha sido correctamente capturada; y c) si todas las deducciones han sido correctamente calculadas.

El interés individual de los empleados proporciona un informal pero efectivo control sobre el riesgo de infravaloración de los importes de nómina, ya que los perceptores son los primeros interesados en comprobar que no se les ha pagado menos de lo que les corresponde.

El subproceso de Pago consiste en aprobar los listados de nómina a pagar a los empleados y ordenar el pago a los beneficiarios.

El pago normalmente se efectúa utilizando una aplicación de banca electrónica instalada en una terminal segura. La información de la nómina en el sistema de la entidad se traspasa mediante una interfaz automática al software bancario o bien se descarga manualmente de la aplicación de nómina y se carga en el software bancario.

En el subproceso de pago, deben considerarse dos controles clave:

- El archivo utilizado para transferir la información desde la aplicación de nómina al banco debe archivarse en una carpeta de acceso restringido de la intranet y transmitirse de forma segura.

- El sistema de firmas electrónicas autorizadas para el pago debe ser mancomunado.

d) Identificar las aplicaciones informáticas de gestión y las interfaces

Para identificar las aplicaciones de gestión y las interfaces existentes (fundamentalmente con contabilidad y con el sistema de pagos) se podrá contar con la colaboración de la UASI. Se documentará detalladamente la aplicación de gestión utilizada por la entidad.

6. Identificación de los riesgos del proceso de gestión y de los controles existentes.

Al analizar el proceso se deben identificar los riesgos existentes en cada fase, valorar los riesgos de incorrecciones materiales (RIM) y posteriormente identificar los controles internos que ha implantado la entidad para mitigarlos. Se debe realizar o discutir este análisis en equipo (ver MFSC-1315.4 y MFSC-1315.5).

Cuando se aborda el análisis de los riesgos de un determinado proceso de gestión el enfoque principal consiste en responder, tanto con carácter general, como en cada uno de los subprocesos analizados, a la pregunta:

¿Qué puede ir mal en el proceso de gestión que pueda afectar significativamente a las cuentas anuales o al cumplimiento de la legalidad?

También se puede formular la pregunta así:

¿Qué podría ocurrir en esta fase que pudiera afectar negativamente en la consecución de los objetivos del proceso? ¿Representaría esto un RIM en las CCAA?

Se deben repetir estas preguntas en cada una de las etapas del proceso.

La lista de riesgos potenciales puede hacerse, en cada caso, tan larga como se desee. Para facilitar el trabajo se pueden establecer listas previas sistematizadas y ordenadas, como la del siguiente cuadro de ejemplo, en la que se señalan algunos de los principales riesgos inherentes a cada función o subproceso y el objetivo de control correspondiente.

Funciones	Ejemplos de riesgos inherentes	Objetivo de control interno
1. Presupuestación	R111 Las previsiones de gasto calculadas no son ajustadas a las necesidades.	El presupuesto del ejercicio es una estimación razonable del gasto de personal esperado.
1. Presupuestación (FMR)	R112 Los datos del FMR (fichero maestro de retribuciones) se introducen o modifican incorrectamente o sin autorización. *La introducción de datos incorrectos sobre las retribuciones puede originar cálculos incorrectos del presupuesto y/o pagos excesivos no autorizados.*	Las retribuciones que se aplican en el presupuesto, en la proyección de la nómina y en las nóminas son las legalmente establecidas.
2. Gestión de puestos (FMP)	R121 Los datos del FMP (fichero maestro de puestos) son inexactos o inseguros *Los datos* de las tablas maestras de puestos *pueden ser incorrectamente o indebidamente introducidos o modificados, lo que puede originar pagos indebidos.*	Todos los cambios en el FMP deben estar debidamente autorizados y soportados por la documentación correspondiente.
3. Gestión de personal (FME)	R131 Los datos del FME son inexactos *Los datos del empleado pueden ser incorrectamente introducidos o modificados, lo que puede originar pagos duplicados, pagos indebidos, errores en las deducciones o en las contribuciones, o cambios no autorizados en la asignación de roles y privilegios en los sistemas.* R132 Los datos del FME no son seguros *Usuarios no autorizados pueden acceder y modificar datos sensibles del personal, comprometiendo la confidencialidad de los datos personales y pudiendo originar pagos de nómina fraudulentos*	Los cambios en el FME se realizan de forma completa, autorizada y oportuna para proporcionar información exacta y completa de los empleados para la elaboración de la nómina.
3. Gestión de personal (Altas y bajas)	R133 Empleados inexistentes o duplicados se añaden a la nómina *Los empleados "fantasma" o duplicados en la nómina originan pagos excesivos o fraudulentos.* R134 Los finiquitos o liquidaciones por despidos o bajas por finalización de contrato no se calculan correctamente *Las liquidaciones incorrectas provocan pagos indebidos*	La captura y el mantenimiento de la información de altas y bajas de los empleados es adecuada, exacta y oportuna.

Funciones	Ejemplos de riesgos inherentes	Objetivo de control interno
	R135 Cuando causa baja un empleado no se le cancela en el sistema. *Si el empleado no se ha marcado como "baja" en el sistema puede continuar cobrando la nómina. Si la baja en el FME está conectado con la gestión de usuarios podría continuar teniendo acceso a la red/sistemas de la entidad.*	
	R136 Las altas de empleados no se han producido de acuerdo con la normativa aplicable. *Se han incorporado empleados sin cumplir la legalidad o las normas internas de la entidad.*	Las admisiones de personal son conformes con la normativa.
4. Elaboración de las nóminas	R140 Los datos sobre tiempo trabajado, permisos, bajas por enfermedad, etc, se computan incorrectamente *Los datos de tiempo trabajado y/o permisos no son exactos y se realizan pagos excesivos*.	Los datos sobre las horas trabajadas/asistencia y ausencias son debidamente procesados, aprobados y correctamente codificados para la elaboración de la nómina.
	R141 El cálculo de la nómina es inexacto o incompleto *Los cálculos de la nómina no se revisan para asegurar su razonabilidad y por tanto no se pueden detectar anomalías o errores significativos.* R142 El cálculo de las retenciones y deducciones es incorrecto R143 Las nóminas no recogen los conceptos fijos y variables correspondientes a la categoría profesional del trabajador. R144 Pago de incentivos no justificados *Pueden realizarse pagos no autorizados, inexactos o ilegales.*	Las nóminas (salarios, retenciones y deducciones) se calculan correctamente: • Todas las nóminas corresponden a empleados de la entidad y son exactas en lo que se refiere a condiciones, cantidades, importes y cálculos. • Los cálculos del salario bruto, salario neto y deducciones son correctos, y se basan en tiempos e importes autorizados.
5. Pago de la nómina	R151 Se realizan pagos incorrectos o duplicados. R152 se puede alterar el importe o destinatario de las transferencias.	Los pagos corresponden a servicios prestados y se realizan sólo a empleados reales. Todos los pagos se preparan basándose en documentos debidamente aprobados, se cotejan con los datos justificativos, se aprueban debidamente, se firman y se transfieren los fondos.
6. Reintegros	R161 Los pagos indebidos no se reclaman.	Existen controles automatizados para reclamar prontamente los pagos indebidos detectados.
7. Contabilidad	R171 Los datos del sistema de nóminas no coinciden con lo contabilizado. *Si no se reconcilian debidamente los datos de la aplicación de nómina con los datos contabilizados aumenta el riesgo de incorrecciones materiales en los estados financieros.* R172 Los gastos de personal y los distintos conceptos que componen la nómina son contabilizados en cuentas equivocadas	Los datos de la nómina contabilizada son completos y exactos. Los sueldos y salarios y demás gastos complementarios de personal se acumulan, clasifican y resumen adecuadamente en las cuentas. Todos los gastos y pagos se registran pronto y exactamente en cuanto a su beneficiario e importe

Tras la narrativa, el dibujo de los flujogramas y la identificación de los riesgos y controles existentes, estos se recogerán en unas tablas que relacionen los riesgos identificados con los objetivos de control y con los controles relevantes con objeto de identificar y obtener una mejor comprensión de las actividades de control que hacen frente de forma eficaz a las áreas en las que los RIM tienen mayores probabilidades de suceder.

Si hay varios controles que tienen el mismo objetivo, el auditor deberá entender cada uno de ellos y seleccionar como controles clave aquellos que considere que alcanzan más eficazmente su objetivo y teniendo en cuenta el coste/eficacia que puede suponer su comprobación.

Se debe determinar si el equilibrio entre controles manuales/automatizados y entre preventivos/correctivos es adecuado. Una excesiva confianza en controles manuales en un entorno informatizado puede ser un indicador de debilidad del control interno.

7. Segregación de funciones

Al revisar un proceso de gestión, un aspecto fundamental es el estudio de la segregación de funciones, que constituye uno de los principios más importantes del control interno.

Significa que las funciones se distribuyen entre las personas de forma que nadie pueda controlar todas las fases del proceso de una transacción de modo tal que puedan pasar inadvertidas incorrecciones debidas a errores o fraudes. Teóricamente, el flujo de las actividades debería proyectarse de tal forma que el trabajo de una persona sea independiente del de otra o sirva para comprobación de este último.

El objetivo de la segregación de funciones es alcanzado al distribuir las actividades clave de RRHH entre varias personas y/o restringir el número de personas con acceso a actividades que sean incompatibles, como por ejemplo, la gestión de datos maestros de RRHH y procesamiento de nóminas.

En la práctica, este principio de segregación de funciones ha de conciliarse con consideraciones tales como el volumen, la complejidad y la materialidad de los distintos tipos de operaciones y la secuencia de pasos necesarios para procesarlas. Los aspectos a considerar variarán ampliamente de una entidad a otra.

En los actuales sistemas altamente automatizados, en los que los usuarios tienen acceso potencialmente a todas las funciones del sistema, el análisis de la segregación de funciones adquiere una importancia especial y debe hacerse una detallada revisión de los riesgos existentes en los permisos de acceso a los sistemas informáticos. Dada su complejidad y "no visibilidad", en los sistemas informatizados, el análisis de la segregación de funciones muchas veces **solo será posible realizarlo** con la colaboración de personal especializado de la UASI utilizando técnicas de auditoría de sistemas.

Entre los mecanismos de control disponibles para ayudar a la hora de llevar a cabo una segregación de funciones eficaz se incluyen:

- Pistas de auditoría/trazabilidad
- Conciliaciones
- Informes sobre anomalías
- Supervisión.

En las empresas y entidades de mayor tamaño, las posibilidades de desagregación del trabajo en el proceso de gestión de nóminas son mayores. Una adecuada segregación de funciones contemplará:

- Un departamento de personal independiente (de la elaboración y pago de la nómina) autoriza y documenta las admisiones y bajas de personal, los sueldos y salarios y las deducciones y retenciones salariales.
- Ningún empleado tendrá responsabilidad total para modificaciones en el FME (Fichero Maestro de Empleados). Un empleado iniciará el cambio y otro revisará y autorizará el cambio.
- Los empleados que tengan capacidad de modificar el FME no deben intervenir en la elaboración de la nómina.
- La función de los jefes de los departamentos operativos, en lo que se refiere al proceso de gestión de nómina, se limita a la aprobación de los tiempos y datos de asistencia al trabajo (por ejemplo guardias médicas, horas extras, ausencias, etc.).
- La aprobación de la nómina debe ser realizada por una persona que no haya intervenido en su elaboración.
- Cuando se utiliza un proveedor externo, los cambios del FME serán comunicados al proveedor por empleados que no intervengan en la contabilización de la nómina, preparación de reconciliaciones o pagos.
- La ordenación del pago de nómina la realizan personas funcionalmente independientes dentro del proceso de elaboración de la nómina.
- La contabilización de nómina la realizan personas que no intervienen en las demás funciones relacionadas con la nómina.
- Un empleado que no intervenga en la elaboración y contabilización de la nómina reconciliará las transferencias ordenadas con el resumen de la nómina antes de aprobar el pago.

Un aspecto que ha de tenerse siempre en cuenta es el coste de mantenimiento de los controles en relación con el riesgo de las pérdidas por error o fraude que podrían producirse en ausencia de aquéllos. A veces no es posible establecer una adecuada segregación de tareas, sobre todo en entidades de pequeño tamaño, ya que

no se dispone de personal suficiente para su implantación, pero en estos casos deben establecerse otro tipo de **controles compensatorios**[6]que pueden ayudar a mitigar la gravedad de las debilidades de control:

- Un supervisor que no interviene en la elaboración de la nómina, revisa y aprueba los ficheros de la nómina antes y después de su cálculo definitivo.
- Se utilizan herramientas analíticas (como ACL) para verificar la exactitud de los salarios reconciliándolos con los tc'1, Mod110 y Mod190.
- Si un empleado que participa en la elaboración de la nómina también mantiene el FME, se debería generar un informe de todos los cambios en el FME para que fueran supervisados por una persona independiente.

Procedimientos de auditoría

Para facilitar la revisión, en el cuadro siguiente se recogen las principales situaciones de falta de segregación de funciones en el proceso de gestión de gastos de personal, que pueden entrañar riesgos de errores o irregularidades, y por tanto riesgos de auditoría. Dicho cuadro solo es un ejemplo de posibles situaciones conflictivas que debe adaptarse a la realidad en cada entidad. En la práctica debe analizarse como está estructurado el proceso de gestión en cada entidad fiscalizada, ya que las funciones principales y, en consecuencia, sus conflictos, dependen de cada caso específico.

El procedimiento de auditoría lógico consistiría en completar el formulario de MFSC-2861.1 y en cada subproceso hacerse las pertinentes preguntas relacionadas con la gestión del personal/nóminas, documentar las respuestas, la evidencia obtenida sobre los posibles conflictos de segregación de funciones y sus consecuencias en nuestra evaluación del control interno y valoración del riesgo.

Si no es adecuada la segregación de funciones se debe explicar por qué y hasta qué punto puede afectar al riesgo de auditoría. Se deben concretar los riesgos que puede provocar la falta de segregación. Se debe indagar si existen controles compensatorios que mitiguen los riesgos cuando no existe un control directo efectivo.

El auditor deberá hacerse las siguientes preguntas y consideraciones:

Función	Consideraciones de control / Preguntas de auditoría	Controles posibles/ Recomendaciones	Ejemplos de controles compensatorios
Gestión del FME	El empleado responsable de iniciar las modificaciones en el Fichero Maestro de Empleados (FME) ¿tiene también competencia para aprobar estos cambios?	Los cambios deben ser introducidos por un empleado y revisados y autorizados en el sistema por otro diferente. Todos los cambios realizados en el FME deben ser revisados y aprobados por un supervisor (que no sea el empleado que ha realizado el cambio) en el departamento de RH antes de que dichos cambios sean registrados en el sistema.	Debe elaborarse un informe automatizado de todos los cambios realizados en el FME para su revisión por un supervisor sin acceso para modificar el FME que comprobará que los cambios están aprobados.
Gestión del FME	Los empleados responsables de mantener el FME (p.ej. añadir/eliminar trabajadores, introducir cambios en las retribuciones), ¿realizan también las siguientes funciones?: • Tomar decisiones sobre contratación o despidos • Tener acceso al sistema de nóminas • Intervenir en el proceso de elaboración de nóminas • Generar las transferencias para pago de nóminas	Los empleados responsables de introducir cambios en el FME no deben intervenir en la elaboración ni en el pago de la nómina, ni deben adoptar decisiones sobre contratación o despidos. NOTA: En algunos casos, el módulo de RH y el módulo de nóminas pueden ser parte del mismo sistema. Sin embargo, los empleados responsables de la elaboración de nóminas no deben tener acceso al módulo de RH o al FME y viceversa.	
Gestión de personal	El personal que gestiona la elaboración de la nómina ¿interviene en el proceso de gestión de las altas, bajas y modificaciones de puestos?	Un departamento de personal independiente (de la elaboración y pago de la nómina) autoriza y documenta las admisiones y bajas de personal.	Tanto las altas, bajas y modificaciones de puestos de trabajo como la elaboración de la nómina se fiscalizan por el departamento de Intervención.
Control de asistencia	¿Las funciones de control de asistencia (horas extras, guardias, etc) están segregadas de las correspondientes a	La función de control sobre la documentación que autoriza los cambios en la nómina debe estar segregada del resto del proceso, ya que	El departamento de Intervención revisa los informes automatizados de control de asistencia obtenidos periódicamente.

[6] Un **control compensatorio** es aquel que reduce el riesgo de una debilidad, real o potencial, no eliminada por un control directo.

Función	Consideraciones de control / Preguntas de auditoría	Controles posibles/ Recomendaciones	Ejemplos de controles compensatorios
	elaboración de nómina, pago y contabilidad?	es un instrumento de control sobre las personas que inician o proponen los cambios en la nómina y sobre las que la elaboran.	
Control de asistencia	¿Pueden los empleados revisar y aprobar sus propias horas trabajadas, los tiempos registrados en el sistema de control de tiempo o las ausencias?	Las horas trabajadas / control de asistencia debe ser revisado y aprobado por el supervisor del empleado en cuestión antes de ser registradas o comunicadas al departamento de nóminas.	El registro de control de horas trabajadas está basado en parámetros físicos (huella, tarjeta, torno …) y el trabajador no puede modificar los registros anotados en la aplicación.
Elaboración de la nómina	Los mismos empleados responsables de elaborar la nómina llevan a cabo también algunas de las siguientes funciones: • ¿Modificar el FME? • ¿Aprobar la nómina?	La nómina debe ser revisada y aprobada por un empleado que no participe en su elaboración ni forme parte de la función de RH. El personal que elabora la nómina no puede modificar el FME.	Para intensificar los controles sobre el proceso de nóminas, debería considerar llevar a cabo una revisión analítica periódica de los gastos de nómina, incluyendo, entre otras cosas, el análisis de desviaciones respecto del presupuesto.
Elaboración de la nómina	Si la elaboración de la nómina la realiza una empresa externa ¿La persona que comunica las variaciones de nómina a la empresa es la misma que contabiliza y gestiona el pago de la nómina?	Si se utiliza un servicio externo, el empleado encargado de comunicar al proveedor los cambios en el fichero de retribuciones no debe participar en la contabilización de la nómina, ni preparar las transferencias de nómina. Este empleado tampoco debería recibir los informes finales de nóminas del proveedor externo de nóminas.	Antes de contabilizar y pagar la nómina elaborada por una empresa externa se revisa por Intervención o el departamento de control interno.
Pago de las nóminas	El mismo empleado responsable de revisar y autorizar el fichero de nóminas ¿prepara y ordena las transferencias de nómina?	Las personas autorizadas en la banca electrónica para realizar el pago de la nómina deben ser diferentes de las personas que intervienen en su elaboración y revisión/autorización. *A menos que exista connivencia entre varios participantes en el proceso de nóminas, ningún empleado tiene interés en falsificar los datos de la misma, salvo que pueda modificar el destinatario de los pagos finales. El pago de la nómina por parte de empleados que no intervienen en la elaboración restringe el riesgo fraudes.*	Se fiscaliza el pago, que incluye el detalle de las transferencias contenidas en el fichero de pago a bancos antes de realizar el pago. Para realizar el pago, además de remitir el fichero bancario se remite una orden de pago en soporte papel que contiene el detalle de todas las transferencias firmada mancomunadamente por al menos dos autorizados en las cuentas bancarias.
Pago de las nóminas	¿Son controlados y conciliados puntualmente las transferencias de nómina rechazadas por un supervisor que no sea de la función de nóminas?	Un empleado que no participa en la función de nóminas ni en recursos humanos debe revisar las transferencias rechazadas (devoluciones de nómina).	La Intervención fiscaliza gestión de los pagos devueltos.
Contabilidad	¿Realiza el empleado encargado de contabilizar la nómina alguna de las siguientes funciones: • Modificar el Fichero Maestro de Empleados • Preparar o autorizar la nómina • Preparar las transferencias de nómina?	La contabilización de la nómina se realiza por personal diferente del que la prepara, revisa y paga. *La separación del cálculo y elaboración de la nómina de la función de contabilidad facilita el control independiente de las operaciones de nómina.*	Una persona que no interviene en ninguna otra operación relativa al proceso de la nómina realiza regularmente la conciliación de la cuenta bancaria destinada al pago de la nómina e investiga las diferencias.
Contabilidad	El empleado responsable de conciliar el libro mayor con el sistema de nóminas ¿tiene también la capacidad de realizar apuntes en el sistema de nóminas o de realizar cambios en éste?	Existe un procedimiento aprobado para revisar a posteriori los importes contabilizados y los resúmenes de las nóminas. El personal que ejecuta esta revisión no participa en la elaboración y no tiene acceso a la aplicación de nómina.	

8. Análisis de las interfaces

Normalmente las entidades utilizan sistemas de personal/nóminas distintos de las aplicaciones contables y comparten la información mediante interfaces. Estas interfaces, que sirven para transferir datos de una aplicación a otra, son un área significativa de riesgo para mantener la integridad de los datos económicos y la confidencialidad de la información del personal.

Por ejemplo, una empresa utiliza una aplicación para gestionar las nóminas y mensualmente traspasa toda la información a la aplicación de contabilidad. El programa que se utiliza para hacer la transferencia de datos es la interfaz entre nómina y contabilidad. Siempre debe comprobarse que los datos se han trasladado a la aplicación contable de forma exacta y completa.

Las interfaces pueden estar automatizadas o ser manuales. En ambos casos existe el riesgo de **pérdida o manipulación** de la información, de forma que los datos de la aplicación de origen no coincidan con los que llegan a la aplicación de destino.

Debemos por tanto:

a) Identificar las interfaces existentes que puedan afectar significativamente a las cuentas anuales y suponer un riesgo de auditoría.
b) Identificar y evaluar los controles que tenga establecidos la entidad.
c) Diseñar y ejecutar las pruebas de auditoría que se estimen pertinentes para garantizar la exactitud e integridad de los datos.

En algunos casos la aplicación de gestión de recursos humanos es diferente de la de nómina y una interfaz gestiona la transferencia de información de una aplicación a otra. Otra interfaz habitual es la utilizada para realizar las transferencias bancarias para el pago de la nómina.

Pueden identificarse deficiencias de control como las de los siguientes ejemplos extraídos de nuestros informes:

Deficiencia de control observada	Riesgo	Recomendación
El intercambio de datos entre las aplicaciones de gestión de puestos y la aplicación de nómina se realiza mediante la remisión de un fichero informático, pero el control de integridad entre las dos aplicaciones es manual. No existe una interfaz de conexión automática que garantice que la información sobre los puestos de trabajo es la misma en las dos aplicaciones.	Esta circunstancia implica un riesgo **alto** sobre la integridad de la información y de que puedan producirse incoherencias entre los datos de las dos aplicaciones.	Recomendamos integrar las bases de datos o automatizar totalmente los controles de la interfaz entre las aplicaciones para mitigar el riesgo de discrepancias en la información de las bases de datos debida a errores o irregularidades.
La interfaz entre la aplicación de nómina y la de contabilidad es un fichero que se importa en esta segunda. Sobre la información del fichero se realizan manualmente numerosas correcciones para contabilizar la nómina que no quedan formalmente registradas.	El ajuste manual de la información entre aplicaciones implica un riesgo **alto** de que se introduzcan modificaciones no autorizadas en las aplicaciones contables.	Recomendamos el establecimiento de un procedimiento automatizado de traspaso de la información de las nóminas para su contabilización. En caso de realizar ajustes desde Intervención, deben quedar registrados los cambios realizados y su autorización.
La aplicación de nómina genera unos ficheros con el detalle de las transferencias individualizadas correspondientes a los importes líquidos de las nóminas. Estos ficheros (de tipo texto y por tanto modificables) se depositan en unas carpetas de acceso no restringido de la red del departamento de Personal y después se remiten a Tesorería. Dicho fichero no es revisado ni las cantidades verificadas.	Que el tipo de fichero de pagos exigido por las entidades bancarias sea editable y que esté depositado en una carpeta de acceso no restringido es un riesgo **alto** de que dicho fichero pueda ser modificado indebidamente y en consecuencia se realicen pagos de forma fraudulenta.	Recomendamos depositar los ficheros de pago en carpetas de acceso restringido al personal estrictamente necesario, así como establecer algún tipo de revisión de los ficheros enviados para comprobar que los importes pagados coinciden con los importes que resultan de la nómina aprobada.
La aplicación de nómina genera unos ficheros editables con el detalle de los asientos contables y otros con el detalle de las transferencias individualizadas correspondientes a los importes líquidos de las nóminas, que se envían por correo electrónico a personal de los departamentos de Contabilidad y de Tesorería. Este medio de transmisión no garantiza la confidencialidad y trazabilidad del acceso. Además, el fichero de transferencias no es revisado después de su utilización ni las cantidades pagadas son verificadas.	Estas circunstancias suponen un riesgo **alto** de que dichos ficheros puedan ser indebidamente visionados, modificados o alterados y pagadas cantidades no autorizadas.	Recomendamos que los ficheros se graben en una carpeta o ubicación determinada, exista autorización explícita del personal con acceso a dicha ubicación, así como establecer algún tipo de revisión de los ficheros de transferencias enviados para comprobar que los importes pagados coinciden con los importes que resultan de la nómina aprobada.

9. Evaluación de los CGTI: Factores de riesgo a considerar

Hay determinados controles de los procesos/aplicaciones cuya eficacia depende en una medida importante en el buen funcionamiento de los controles generales.

Por tanto, la revisión de los controles de aplicación y la decisión de depositar confianza en ellos debe hacerse tras una evaluación positiva de los controles generales de tecnologías de la información (CGTI), tanto de los existentes a nivel de entidad y sistemas TI como a nivel de los procesos/aplicaciones de gestión de personal/ nóminas, según los procedimientos descritos en MFSC-2850 y siguientes.

La **UASI** al realizar la revisión de los CGTI tendrá en cuenta, en particular, pero no exclusivamente, los siguientes riesgos existentes en el nivel de la aplicación informática de gestión auditada.

Entorno de control

Un entorno de control efectivo es fundamental para asegurar que la información sobre recursos humanos y el tratamiento de dicha información sean exactos y completos, y que se mantengan la integridad y confidencialidad de la información.

Gestión de cambios

Es importante que existan unos controles efectivos a fin de asegurar que los cambios en las aplicaciones sean autorizados y debidamente comprobados antes de introducirlos en el sistema de producción.

El procedimiento de gestión de cambios deberá evitar que se introduzcan sin la autorización apropiada modificaciones en la información sobre los trabajadores, o en la aplicación que gestiona las nóminas, etc. Contemplará entre otras cuestiones que:

- Todas las solicitudes de cambios a introducir en las aplicaciones de gestión de recursos humanos, así como cualquier cambio en la estructura de la base de datos deberán ser revisados y aprobados por el responsable de RH antes de ser implementados.
- Todos los cambios deben autorizarse antes de ser introducidos en el entorno de producción.
- Debe existir separación de funciones a fin de limitar la capacidad del personal para realizar cambios que afecten tanto a la base de datos de producción como a la configuración de la aplicación de nómina.

Si una aplicación se ha desarrollado en la entidad y un equipo de desarrolladores internos tiene acceso a modificar la aplicación, el riesgo asociado será alto. Sin embargo en una aplicación comercial cualquier cambio en el código fuente necesitará la intervención del fabricante y unos procedimientos adicionales.

Debido a la criticidad del sistema informático de gestión de recursos humanos y a los aspectos fundamentales de sus operaciones (gestión de nóminas, impuestos, etc.), el mantenimiento y las **actualizaciones** de las aplicaciones deberían ser incorporados al proceso de gestión de cambios. Es importante la oportuna aplicación de las actualizaciones del software para el sistema de gestión de personal, ya que tales actualizaciones a menudo incluyen cambios resultantes de la legislación en materia de fiscalidad y retribuciones.

Algunos ejemplos extraídos de nuestros informes:

Deficiencia de control observada	Riesgo	Recomendación
En el entorno de sistemas existe un elevado número de usuarios (50) con permisos de acceso a los entornos de producción y pruebas, lo que no garantiza el principio de segregación de funciones.	Esta situación supone un riesgo valorado como **medio** de que las personas que desarrollan aplicaciones puedan modificar los programas en producción de forma inadvertida o no autorizada, generando transacciones no autorizadas.	Recomendamos formalizar un procedimiento para la gestión de usuarios con acceso a los entornos de pruebas, preproducción y producción a través de la red de gestión, de forma que se garantice que el acceso al entorno de producción está limitado al mínimo número de personas justificado por el desempeño de las funciones del usuario, siempre atendiendo a los principios de mínimo privilegio y de segregación de funciones.

Controles de accesos y de usuarios

Una gestión eficaz de los controles de acceso de los usuarios proporciona garantía de que los sistemas de recursos humanos están adecuadamente protegidos para evitar el uso no autorizado, divulgación, modificación o pérdida de información. La gestión de usuarios es también un componente crítico para el establecimiento de una efectiva separación de funciones. Por ejemplo:

- El acceso o la modificación de los privilegios de acceso deben ser aprobados y documentados;
- Los usuarios del sistema de gestión de recursos humanos deberán ser identificados de forma única. Los usuarios tendrán un identificador individual de acceso y no deberán compartir contraseñas;
- El acceso de administrador o acceso "privilegiado" se limitará a personas del departamento de RRHH;
- El acceso al sistema se basará en una estructura de roles de usuario;
- Los privilegios de acceso al sistema y las normas de gestión deberán cumplir con los requisitos de segregación de funciones.
- El acceso directo a la Base de Datos (BD) subyacente es un aspecto crítico, ya que puede dejar puertas traseras para acceder a los datos sin necesidad utilizar la aplicación de gestión, por lo que tendrá la misma relevancia que los acceso a las aplicaciones de gestión.

Algunos ejemplos extraídos de nuestros informes:

Deficiencia de control observada	Riesgo	Recomendación
No consta que exista un procedimiento aprobado para tramitar y gestionar los permisos de acceso a la aplicación de RRHH y revisarlos periódicamente. La aplicación permite definir en detalle las capacidades de cada usuario pero no existe un esquema organizativo para aplicar estos permisos, de forma que se generan muchos tipos de usuarios de los que es difícil discernir las capacidades que tienen asignadas. Hemos observado que existen muchos usuarios con acceso a alguna de las funcionalidades más críticas de la gestión de puestos de trabajo (por ejemplo 13 usuarios tienen capacidad para ….).	La situación descrita supone un riesgo **alto** de que existan accesos indebidos o no autorizados a determinadas funcionalidades críticas de la aplicación.	Recomendamos que se apruebe un procedimiento de gestión de usuarios de la aplicación, basado en perfiles estandarizados, que contemple, tanto las altas, bajas y modificación de permisos, como la revisión periódica de los mismos con el objetivo de detectar y eliminar usuarios obsoletos, y ajustar los permisos a las necesidades funcionales de los usuarios de acuerdo con el principio de privilegio mínimo necesario para realizar las tareas asignadas.
La política de autenticación de los usuarios en la aplicación de RRHH (caducidad de contraseña, complejidad, historial, …) no se ajusta a lo que se consideran buenas prácticas para la seguridad de la información	Esta circunstancia representa un riesgo **alto** de que se produzcan accesos no autorizados.	Recomendamos elevar el grado de robustez de la política de autentificación para los accesos a la aplicación de RRHH para ajustarlos a los que se consideran buenas prácticas en la gestión de la seguridad de la información.
Las políticas de acceso y de configuración de las contraseñas del dominio y de la aplicación de nómina no son todo lo robustas que exigen las buenas prácticas en materia de gestión de TI. Asimismo, en la gestión de usuarios se han identificado algunos usuarios genéricos.	Esta configuración de las políticas de seguridad supone un riesgo **medio** de accesos no autorizados a las aplicaciones y al dominio, y la imposibilidad de atribuir responsabilidades.	Recomendamos modificar las políticas y parámetros de autenticación (contraseñas) configuradas en el dominio y en la aplicación y adaptarlas a los parámetros generalmente aceptados (complejidad mínima, cambio de contraseñas cada 3 a 6 meses, historial de contraseñas mínimo de 5, bloqueos ante intentos fallidos, etc.). También recomendamos cambiar los usuarios genéricos a usuarios nominativos, y en caso de necesitar utilizarlos, asignar la responsabilidad sobre dicho usuario genérico a alguna persona.
Hemos observado que en las aplicaciones de RRHH, determinadas personas tienen asignados permisos que exceden de las tareas asignadas a su puesto de trabajo (en Intervención, Concejalía, etc.).	La asignación de permisos a determinados usuarios, que no se corresponden con sus puestos de trabajo, supone un riesgo **alto** sobre la integridad, exactitud y confidencialidad de la información y, además, plantea conflictos de segregación de funciones.	Recomendamos que la gestión de usuarios en los sistemas se realice de acuerdo con el principio de concesión de los mínimos permisos necesarios para el ejercicio de las funciones asignadas.
Al revisar la gestión de usuarios, se han identificado múltiples usuarios genéricos o indeterminados.	Esta circunstancia supone un riesgo **alto** de accesos no autorizados a las aplicaciones y al dominio, y la imposibilidad de atribuir	Recomendamos eliminar los usuarios genéricos, transformándolos a usuarios nominativos y, en caso de necesitar utilizarlos excepcionalmente, asignar la responsabilidad sobre dicho usuario

Deficiencia de control observada	Riesgo	Recomendación
	responsabilidades y de garantizar una adecuada segregación de funciones en los procesos de gestión.	genérico a alguna persona determinada.
El personal del Área de SSII sigue un procedimiento para las altas de los usuarios en el dominio y en las aplicaciones que está afectado por una enorme casuística: personal del ente (ubicado dentro o fuera de las instalaciones), personal externo que está en las instalaciones del ente, personal externo que quiere acceder a información del ente, etc. No existe un procedimiento formalizado que contemple todas estas posibilidades, ni tampoco existe comunicación en caso de bajas de usuarios o cancelación de permisos. Tampoco se realizan revisiones periódicas de usuarios. Todo ello provoca que existan usuarios activos en el dominio y en las aplicaciones que ya no trabajan en la Entidad o usuarios que han cambiado de funciones pero continúan teniendo acceso a aplicaciones a las que no deberían.	Esta situación implica un riesgo **alto** de accesos no autorizados a las aplicaciones y a los datos. También compromete la eficacia de la segregación de funciones existente en los procesos de gestión.	Recomendamos formalizar un procedimiento de gestión de usuarios y de permisos, que contemple la implicación de los responsables de los diferentes departamentos en las altas, en los cambios de puesto de trabajo y en las bajas de los usuarios de dominio y de las aplicaciones. La gestión de usuarios debe realizarse de acuerdo con el principio de atribución de los mínimos permisos necesarios para el ejercicio de las funciones asignadas.

Continuidad del servicio

El mantenimiento de cualquier sistema requiere la adopción de unas medidas para el caso de que ocurra una interrupción en el funcionamiento del sistema. Se debe comprobar que las entidades cuentan con los procedimientos necesarios para recuperarse de tal interrupción:

- Se debe disponer de una estrategia documentada para la gestión de la copia de seguridad periódicas, tanto de los datos como de los programas de recursos humanos;
- Hay que definir los plazos de retención y los requisitos de almacenamiento para la información sobre recursos humanos, mensajes, informes y ficheros de salida; y
- Deben identificarse y aplicarse unos requisitos para proteger la información confidencial sobre recursos humanos y protegerse contra su modificación o divulgación no.

Algunos ejemplos extraídos de nuestros informes:

Deficiencia de control observada	Riesgo	Recomendación
Aunque se dispone de una arquitectura de alta disponibilidad para los servidores de aplicación, de nómina basada en la existencia de clústeres de servidores, todos los equipos se ubican en un mismo CPD.	En caso de ocurrir un desastre que afectase al CPD, existe el riesgo alto de que se pierdan, de forma irreversible, los sistemas de producción junto con las configuraciones de los sistemas y la lógica de las aplicaciones. La reconstrucción de esta pérdida (las principales aplicaciones de la Entidad) podría prolongarse durante meses.	Debe desarrollarse un plan de gestión de la continuidad del servicio, que contemple, en sentido amplio, todos los activos que dan soporte a sus procesos (personas, instalaciones, proveedores, sistemas de información, etc.), sus requisitos de disponibilidad, el desarrollo de los correspondientes planes de recuperación en caso de ocurrencia de una contingencia grave que afecte a su disponibilidad, así como los mecanismos orientados a garantizar la validez de dichos planes de manera continuada en el tiempo.
La copia de seguridad de datos y programas se guarda en una caja fuerte ignífuga en el Centro de Proceso de Datos (CPD). En caso de desastre, la copia de datos y programas puede correr la misma suerte que el CPD.	Esta situación implicaría un riesgo **alto** de pérdida de datos y programas. Además, esto es una obligación legal para los datos de carácter personal de nivel alto.	Recomendamos el traslado y ubicación fuera del CPD de las copias de seguridad que se realicen de datos y programas.
No se ha definido un plan de continuidad de la actividad que permita la recuperación de los procesos de gestión críticos, tras la ocurrencia de una contingencia que afecte a los sistemas de producción, en un tiempo limitado y fijado con anterioridad.	Existe un riesgo **alto**, en caso de un evento que afecte a los procesos de gestión críticos y los sistemas de información que los soportan, de que no se recuperen las actividades y los datos en los plazos y condiciones requeridas para el logro de los objetivos del Ayuntamiento.	Recomendamos elaborar y aprobar un plan de recuperación de la actividad, basado en un análisis de riesgos y en la identificación de los activos de TI que son críticos para la entidad, detallando las tareas a realizar para restablecer el servicio, los plazos máximos de respuesta y los periodos de retención de la información.

10. Procedimientos de Auditoría

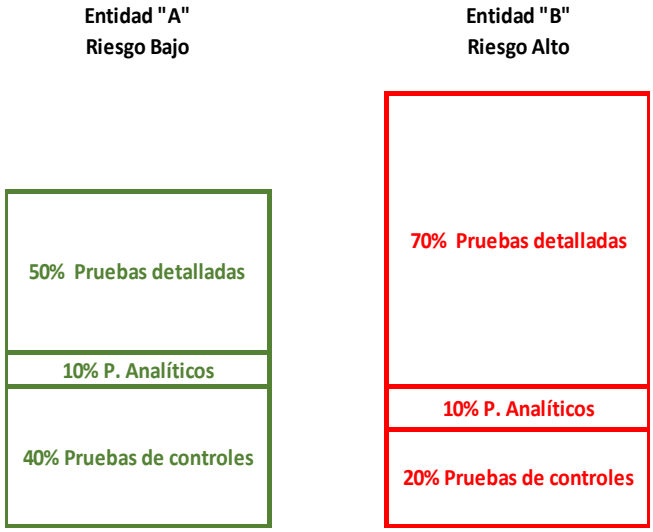
La naturaleza, momento y alcance de los procedimientos de auditoría se determinan de acuerdo con las circunstancias de cada trabajo y deben basarse en el conocimiento de la actividad que realiza el ente auditado, de su organización, de los riesgos valorados así como en la evaluación del control interno y de la importancia relativa de los saldos en las cuentas anuales.

Los procedimientos de auditoría son las respuestas a los riesgos valorados y por tanto deben ser deben ser proporcionales a esos riesgos. Así las áreas de riesgo más alto deben recibir mayor atención y esfuerzo de auditoría.

Los programas de auditoría deben ser adaptados a cada entidad en base a la valoración del riesgo de incorreciones materiales, e incluirán:

- Pruebas de controles (si procede)
- Procedimientos sustantivos (incluyendo procedimientos analíticos)

Podemos ver con un ejemplo gráfico como puede variar la cantidad (suficiencia) de evidencia necesaria y los tipos de pruebas necesarias para obtenerla



En las **pruebas de controles** el auditor debe decidir qué controles son relevantes y diseñar y ejecutar pruebas sobre los mismos. Tras realizar estas pruebas, si se han detectado deficiencias de control:

- Se debe evaluar la gravedad de dichas deficiencias
- Modificar la valoración preliminar del riesgo
- Documentar las implicaciones de las deficiencias de control.

Si no se han detectado deficiencias de control, se debe:

- Determinar que la valoración preliminar del riesgo como bajo es adecuada
- Determinar el grado de evidencia que proporcionan los controles sobre la corrección de los saldos.
- Determinar los procedimientos sustantivos a ejecutar.

Los procedimientos de auditoría relacionados con las áreas de gastos de personal se detallan en los anexos *MFSC-2861.4, MFSC-2861.5 y MFSC-2861.6* se incluyen los programas de trabajo estándar, que deben adaptarse a las circunstancias de cada fiscalización.

Dichos programas están disponibles en el sistema de papeles de trabajo electrónico de la Sindicatura (TeamStores) y son actualizados periódicamente.

11. Colaboración UASI

La realización de algunos de los procedimientos de auditoría descritos en esta guía, requerirán la colaboración de la UASI con el equipo de fiscalización encargado en trabajo. Con esa finalidad el Auditor responsable se pondrá en contacto con el Jefe de la UASI al iniciar la planificación del trabajo para coordinar la colaboración.

12. Aplicación de esta guía

Esta guía se aplicará en las fiscalizaciones de nivel de control general o cuando esté previsto fiscalizar el área de personal.

En las entidades de menor tamaño podrá limitarse la aplicación de determinados procedimientos si a juicio del auditor resulta más eficiente y se alcanzan igualmente los objetivos de auditoría.

Anexos:

Sección 2861.1: Documentar la comprensión del proceso de gestión de personal

De uso interno de la Sindicatura:

Sección 2861.4: Programa de auditoría de gastos de personal-EEPP

Sección 2861.5: Programa de auditoría de gastos de personal-EELL

Sección 2861.6: Programa de auditoría de gastos de personal-Administración

Sección 2861.8: Principal normativa relativa a personal de EELL

Sección 2861.9: Guía para la realización de pruebas de datos sobre personal/nóminas

Sección 2861.10: Principales deficiencias de control interno señaladas en los informes de la Sindicatura