

**AUDITORÍA DE EFICACIA DE LOS SISTEMAS DE
INFORMACIÓN Y DE CONTROL INTERNO DE LOS
PROCEDIMIENTOS DE GESTIÓN DE LA TESORERÍA DEL
AYUNTAMIENTO DE ALICANTE**

EJERCICIOS 2011-2013

ÍNDICE	Página
1. INTRODUCCIÓN	3
2. OBJETIVOS DE LA AUDITORÍA	4
3. ALCANCE DE LA AUDITORÍA	5
4. CONCLUSIONES GENERALES	6
5. REVISIÓN DE LOS CONTROLES GENERALES DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (CGTI)	8
6. CONTROLES EN EL PROCESO DE GESTIÓN DE LA TESORERÍA	16
7. PRUEBAS DE TRATAMIENTO MASIVO DE DATOS	22
8. SEGUIMIENTO DE LAS RECOMENDACIONES DEL INFORME SOBRE CONTROL INTERNO	23
9. TRÁMITE DE ALEGACIONES	23

ANEXO I: Enfoque metodológico de la auditoría de sistemas de información

ANEXO II: Descripción del proceso de gestión contable y de la tesorería

ANEXO III: Alegaciones del cuentadante

ANEXO IV: Informe sobre las alegaciones presentadas

1. INTRODUCCIÓN

La Sindicatura de Comptes estableció en 2011 un plan de trabajo de forma que, en un horizonte plurianual, se fiscalizarían todos los ayuntamientos de población superior a 50.000 habitantes de la Comunidad Valenciana.

La primera fase de ese plan consistía en efectuar una fiscalización del control interno de dichos ayuntamientos. Resultado de la misma fue la emisión en 2012, entre otros, de un informe de fiscalización del control interno del Ayuntamiento de Alicante, en el que el área de tesorería obtuvo una valoración de 878, siendo 456 la media de los diferentes ayuntamientos, mientras que en el entorno tecnológico la valoración fue de 1.237 sobre 748 de media. Estas valoraciones indicaban una situación claramente mejorable en estas áreas (a menor puntuación mejor evaluación del control interno).

La segunda parte de dicho plan incluye la realización de una fiscalización más general, profundizando además en la revisión de aquellas áreas de riesgo identificadas en el informe antes citado.

De acuerdo con la Ley de la Generalitat 6/1985, el Consell de la Sindicatura incluyó en el Programa Anual de Actuación de 2013 (PAA2013) la realización de una *fiscalización de diversos aspectos de la actividad económica-financiera del Ayuntamiento de Alicante* aplicando los procedimientos establecidos en la sección 902 de nuestro “Manual de fiscalización” y, además, una auditoría específica de la *eficacia de los sistemas de información y de control interno de los procedimientos de gestión de la tesorería*. El presente Informe recoge los resultados de esta fiscalización específica.

Alicante es un municipio capital de provincia con un volumen de gestión elevado. El presupuesto inicial de 2012 fue de 240.409.533 euros. El saldo de tesorería al cierre de ese ejercicio fue de 10.445.137 euros.

El proceso de gestión contable y de la tesorería del Ayuntamiento de Alicante se puede representar abreviadamente en el siguiente gráfico.

La gestión de la tesorería se encuentra condicionada por todo el proceso de gestión presupuestaria-contable, pues muchos de los controles que afectan a la tesorería se ubican en las fases previas de este proceso (por ejemplo, para que se pueda pagar un gasto debe haber sido previamente presupuestado, autorizado, dispuesto, justificado, fiscalizado y contabilizado).

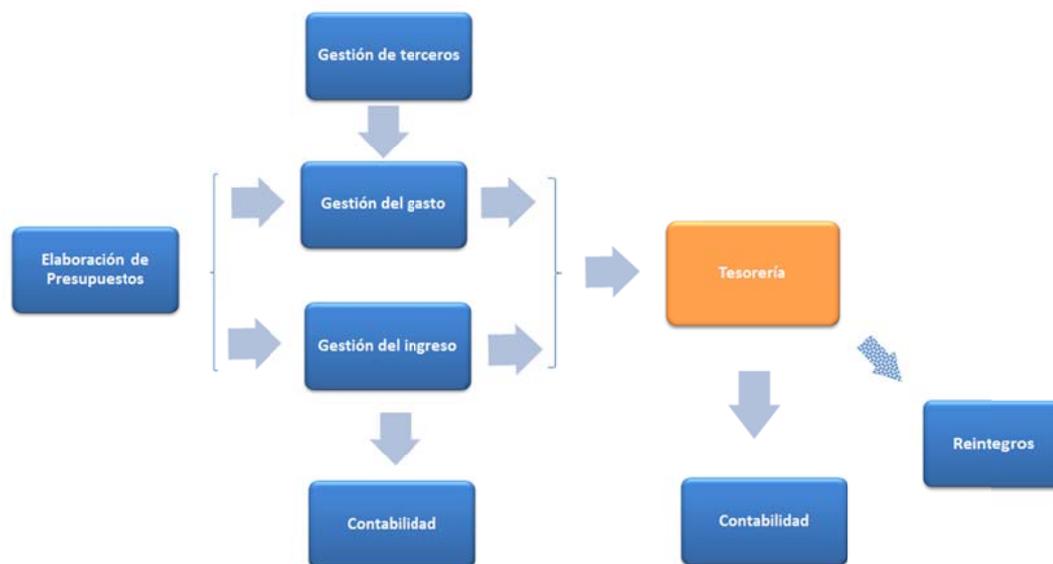


Gráfico 1

En el anexo II se describen resumidamente los principales subprocesos de gestión.

La auditoría de los procedimientos de gestión de la tesorería y de los sistemas de información y de control interno relacionados se ha realizado conjuntamente con la fiscalización de diversos aspectos de la actividad económica-financiera del Ayuntamiento de Alicante, cuyo informe se recomienda leer previamente al resultante de esta fiscalización específica.

Dadas las especiales características del trabajo a realizar respecto de los sistemas de información del Ayuntamiento, la fiscalización se ha realizado por personal especializado de la Sindicatura de Comptes con la colaboración de una firma de auditoría informática.

Debe destacarse que la colaboración de los responsables y del personal de los departamentos de sistemas de información y de administración del Ayuntamiento ha sido en todo momento completa (en especial de Tesorería, Intervención, Modernización y Atención Urbana), lo que ha facilitado la buena marcha de los trabajos de auditoría cuyo resultado se recoge en el presente Informe.

2. OBJETIVOS DE LA AUDITORÍA

El objetivo del presente trabajo ha consistido en analizar los procedimientos de gestión de la tesorería del Ayuntamiento de Alicante, incluyendo los sistemas de información en los que se apoyan, y determinar si el grado de eficacia de los controles existentes en dichos sistemas, tanto en las aplicaciones informáticas como a través de

procedimientos manuales, aportan un nivel de confianza razonable para garantizar la correcta ejecución de los cobros y pagos del Ayuntamiento, la adecuada custodia de los fondos y para reducir el riesgo de errores o irregularidades.

Asimismo se pretende ofrecer medidas correctoras a las posibles deficiencias de control interno encontradas en el curso de la auditoría, para lo que se formulan las pertinentes recomendaciones que contribuyan a incrementar la eficacia del sistema de control interno y la eficiencia de los procesos de gestión. Cuando la incidencia de control afecta a una norma legal se señala expresamente la correspondiente obligación de adaptación.

3. ALCANCE DE LA AUDITORÍA

Conforme al objetivo señalado en el apartado 2, el alcance de la presente fiscalización ha comprendido:

- a) El análisis de los procedimientos de gestión de la tesorería tanto los manuales como las aplicaciones y sistemas informáticos que soportan esa gestión, y de la eficacia de los controles internos existentes.
- b) La revisión de los controles generales de las tecnologías de la información (CGTI) soporte de las aplicaciones de gestión, cuya efectividad condiciona la de los controles en las aplicaciones.
- c) La revisión de la interfaz de intercambio automatizado de información entre las aplicaciones contable y de tesorería.
- d) También se han realizado una serie de pruebas masivas de datos dirigidas a comprobar si la información contable y de gestión de la tesorería tiene un grado suficiente de garantía respecto a su validez, integridad y exactitud.

No se han revisado las aplicaciones de gestión de los ingresos y gastos.

El diseño, implantación y buen funcionamiento de los controles en los procesos de gestión y en los sistemas de información es una responsabilidad que corresponde a los órganos de gobierno del Ayuntamiento encargados de los procesos revisados.

Dadas las limitaciones inherentes a cualquier sistema de control interno y, en concreto, de los controles implantados en la gestión de la Tesorería pueden existir hechos motivados por errores o irregularidades que no hayan sido detectados en la revisión efectuada.

El periodo revisado ha abarcado los ejercicios 2011, 2012 y 2013, mostrándose la situación de los controles implantados en los

procedimientos de gestión revisados existentes al finalizar el trabajo de campo en julio de 2013.

Las aplicaciones que soportan la mayor parte del proceso de gestión analizado son Sicalwin, Firmadoc y Delta.

Sicalwin es la aplicación con la que se registran los movimientos contables y que genera los estados financieros que componen la Cuenta General del Ayuntamiento. También permite gestionar la tramitación y contabilización de los documentos contables de ingresos y de gastos.

Firmadoc se utiliza para la gestión de los documentos y firmas electrónicas y sirve de complemento a Sicalwin, con la que está integrada, para la gestión de los documentos contables.

Delta es la aplicación utilizada en el Departamento de Tesorería para la gestión y control de ingresos y pagos.

La descripción gráfica simplificada del entorno tecnológico de los procesos analizados se muestra en el siguiente gráfico:

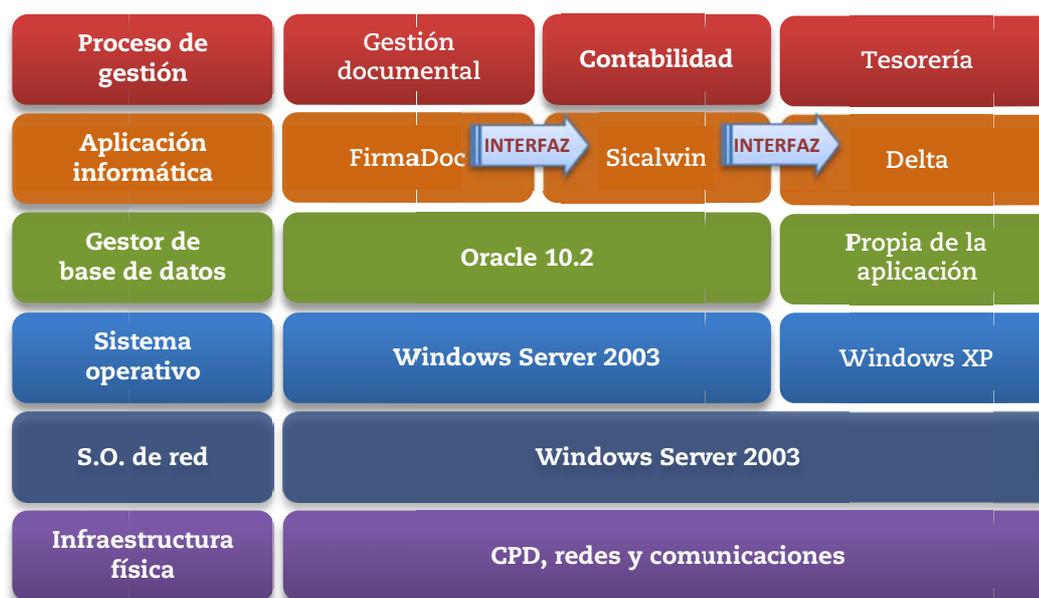


Gráfico 2

4. CONCLUSIONES GENERALES

Como resultado del trabajo efectuado, con el alcance descrito en el apartado 3, cabe concluir que el nivel de control existente en los sistemas de información y en los procedimientos de gestión de la tesorería aportan un nivel de confianza razonable para garantizar su correcta ejecución, la adecuada contabilización de las operaciones

realizadas y la validez, integridad, exactitud, confidencialidad y disponibilidad de la información.

Sin perjuicio de lo anterior, durante la realización del trabajo se ha identificado un conjunto de debilidades materiales y deficiencias significativas¹ de control que se detallan en los apartados siguientes junto con las recomendaciones que de ellas se derivan, cuya implantación puede contribuir a incrementar el ambiente de control y reducir la probabilidad y el riesgo de que existan errores o irregularidades.

El cuadro y gráfico siguientes muestran el grado de cumplimiento de la serie de controles que se han analizado en la presente auditoría.

Área	Eficacia de los controles			Total controles revisados
	Efectivos	Parcialmente efectivos	No efectivos	
Controles generales	24	18	25	67
Controles de aplicación	26	21	7	54
Total controles evaluados	50	39	32	121
	41,3%	32,2%	26,4%	100,0%

Cuadro 1

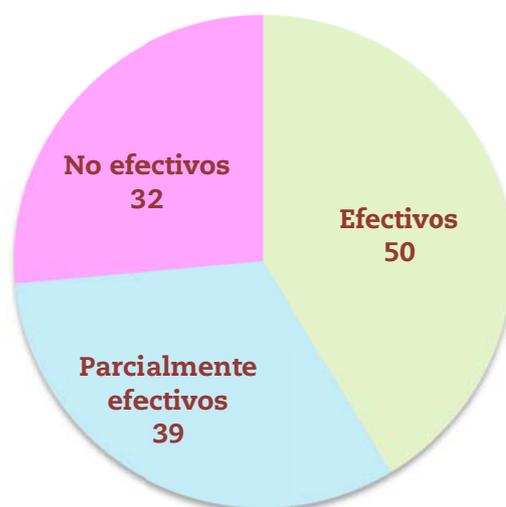


Gráfico 3

¹ Ver definiciones en el anexo I.

La interpretación de los datos anteriores sobre el nivel de control interno existente y la eficacia global del sistema de control interno, debe realizarse de forma conjunta con el resto de observaciones detalladas y recomendaciones contenidas en los apartados siguientes del presente Informe. Sólo se han incluido aquellas recomendaciones en las que se considera que existe una relación coste-beneficio positiva.

5. REVISIÓN DE LOS CONTROLES GENERALES DE TECNOLOGÍAS DE LA INFORMACIÓN (CGTI)

Los controles generales son las políticas y procedimientos que se aplican a la totalidad o a gran parte de los sistemas de información de una entidad, incluyendo la infraestructura tecnológica, y que ayudan a asegurar su correcto funcionamiento.

El objetivo principal de la revisión ha sido obtener una visión del grado de eficacia de los CGTI existentes en la gestión de los sistemas de información que soportan el funcionamiento de las aplicaciones Sicalwin, Firmadoc y Delta. De esta forma, la revisión se ha centrado en las áreas de *Marco organizativo*, *Acceso a datos y programas* (controles sobre la gestión de accesos de las aplicaciones antes citadas) y *Continuidad del servicio* tal como vienen definidas en el “Manual de fiscalización” de la Sindicatura de Comptes. La revisión de las áreas de *Operaciones de los sistemas de información* y *Gestión de cambios* se ha limitado al subconjunto de controles que se han considerado más relevantes de acuerdo con el objetivo y alcance de la presente auditoría.

La siguiente tabla y gráfico muestran el grado de cumplimiento de los 67 controles generales que se han revisado en la auditoría, que indican la existencia de un entorno general razonable de control en la Entidad, si bien existen numerosas oportunidades de mejora. De un total de 67 controles revisados un 35,8% resultaron efectivos, un 26,9% parcialmente efectivos y un 37,3% no efectivos, presentando el siguiente detalle.

Área	Eficacia de los controles			Total controles revisados
	Efectivos	Parcialmente efectivos	No efectivos	
Marco organizativo	5	4	7	16
Gestión de cambios	3	4	4	11
Operaciones de los SI	8	6	4	18
Acceso a datos y programas	6	3	6	15
Continuidad del servicio	2	1	4	7
Total controles evaluados	24	18	25	67
	35,8%	26,9%	37,3%	100,0%

Cuadro 2



Gráfico 4

Las principales deficiencias de control interno que se han identificado en la revisión efectuada y las recomendaciones que de ellas se derivan, cuya implantación puede contribuir a incrementar el ambiente de control y reducir la probabilidad y el riesgo de existencia de incidencias de control, son:

Marco organizativo

1. El Pleno del Ayuntamiento no ha aprobado la política general de seguridad de la información que garantice el compromiso de la Entidad con la seguridad de la información y establezca la asignación de funciones y responsabilidades en esta materia. Tampoco se han elaborado planes de formación y concienciación para la seguridad de la información dirigidos a los usuarios de los sistemas de información del Ayuntamiento.

La inexistencia de un compromiso formal y explícito del máximo órgano de gobierno de la Entidad con la seguridad de la información supone un elemento de incertidumbre y un riesgo alto para la efectiva aplicación de las medidas e iniciativas sobre seguridad de la información impulsadas desde dentro de la organización.

Recomendamos que el Pleno apruebe una política de seguridad de la información de la Entidad que contemple la estructura organizativa en esta materia y la asignación de responsabilidades. Esta política deberá desarrollarse a través de normas específicas para cada área (uso de equipos, accesos, ...). También se deben aprobar y programar los planes de formación en materia de seguridad de la información que abarquen a todos los usuarios de los sistemas.

2. El Ayuntamiento no dispone de un plan estratégico en materia de TI que permita garantizar que se alcancen los objetivos asignados a esta área para el logro de los objetivos generales de la Entidad. Tampoco se dispone de planes anuales de inversiones en TI adecuadamente valorados y presupuestados.

La ausencia de estos planes supone un riesgo medio de que no exista alineación entre los objetivos de la organización y la infraestructura tecnológica necesaria para lograrlos.

Recomendamos que el Pleno apruebe un plan estratégico de TI así como la elaboración de planes anuales alineados con los objetivos estratégicos del Ayuntamiento. Estos planes deberán concretar los proyectos o fases de proyectos a ejecutar en cada ejercicio al que se refieran y las dotaciones presupuestarias necesarias.

3. El Ayuntamiento no ha elaborado y aprobado los planes de adecuación previstos en los Real Decreto 3/2010 y Real Decreto 4/2010, por los que se aprueban los esquemas nacionales de seguridad e interoperabilidad, que son de obligado cumplimiento por todas las administraciones públicas.

Además de suponer un incumplimiento de la normativa de aplicación, la falta de adaptación del Ayuntamiento a esta normativa supone un riesgo medio de que la protección de los sistemas de información no sea la adecuada a su clasificación y una falta de adaptación a los mecanismos de intercomunicación entre administraciones públicas, tan necesarios en la administración electrónica.

El Ayuntamiento debe realizar las actuaciones oportunas para adaptar sus sistemas de información a los requisitos establecidos en los reales decretos citados.

De acuerdo con la información facilitada se han iniciado los trabajos para elaborar y aprobar estos planes de adecuación aunque no habían concluido a la fecha de finalización de la auditoría.

4. Aunque el Ayuntamiento ha realizado acciones encaminadas a cumplir la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, no dispone del documento de seguridad LOPD ni ejecuta las auditorías previstas en la norma.

El incumplimiento de la normativa supone un riesgo medio de posibles sanciones y/o de perjuicio para la imagen del Ayuntamiento.

El Ayuntamiento debe finalizar lo antes posible con las acciones emprendidas para lograr un completo cumplimiento en materia de

LOPD.

5. Los procedimientos de gestión llevados a cabo en el departamento de tecnologías de la información no se encuentran, en general, descritos y aprobados al adecuado nivel directivo. Entre otros, se encuentran pendientes de desarrollar los siguientes: notificación y gestión de incidencias, configuración de la protección antimalware y protección y gestión de la información.

El hecho de que no se hayan redactado y aprobado los procedimientos implantados en materia de gestión de las TI implica un riesgo medio de falta de homogeneidad e inadecuación en la ejecución de aquéllos, así como una mayor dependencia de la organización respecto a las personas.

Recomendamos que se formalicen y aprueben los procedimientos de gestión del departamento de TI, empezando por aquellos más críticos o relevantes.

Gestión de cambios en aplicaciones y sistemas

6. El Ayuntamiento no dispone en la actualidad de un procedimiento aprobado de identificación y comunicación de las necesidades de software ni de gestión de cambios en las aplicaciones.

Respecto a la gestión de cambios, si bien se cuenta con procedimientos técnicos asociados queda pendiente el desarrollo de los siguientes aspectos:

- Creación de un entorno de pruebas.
- Inclusión en el procedimiento de las pruebas a realizar y su aprobación previa al pase a producción.
- Definición de un proceso de emergencia para revertir posibles cambios defectuosos.
- Registro de cambios realizados.

La inexistencia de procedimientos de identificación de necesidades de software y de gestión de cambios aprobados supone un riesgo medio de pérdida de eficiencia y de que los cambios en las aplicaciones se ejecuten sobre los sistemas reales que soportan los servicios del Ayuntamiento sin realizar los controles previstos en las normas generalmente aceptadas de buena gestión de los sistemas de información.

Recomendamos que se apruebe un procedimiento de ejecución periódica que permita recabar información sobre nuevas aplicaciones y las necesidades de software y su comunicación al departamento de Modernización y de un procedimiento de gestión

de cambios en las aplicaciones que contemple los controles antes citados y aquellos otros que se consideren relevantes en función de las características de los sistemas del Ayuntamiento.

Operaciones de los sistemas de información

7. La gestión de los proveedores de servicios de TI no contempla, en todos los casos, acuerdos de nivel de servicio que garanticen una adecuada calidad del servicio y cláusulas para garantizar la confidencialidad de la información. No consta que se hayan definido indicadores que permitan evaluar los servicios prestados, ni que se haga un seguimiento de los mismos.

La ausencia de un control y una medición de los servicios prestados por los proveedores de servicios TI y la ausencia de compromisos contractuales sobre la confidencialidad de la información supone un riesgo medio de que se produzcan menores rendimientos y una pérdida de eficiencia en el funcionamiento de los sistemas, y de generar costes adicionales en la prestación de los servicios.

Recomendamos que en las siguientes licitaciones de contratos de servicios TI se prevean cláusulas que fijen los niveles de servicio a prestar por los proveedores e indicadores de referencia para cuantificarlos así como las necesarias cláusulas de confidencialidad en el tratamiento de la información. También es deseable que incluyan cláusulas que garanticen la disponibilidad del código fuente de las aplicaciones, la transmisión de los conocimientos necesarios para la gestión de las TI al Ayuntamiento y que garanticen la continuidad de los servicios en caso de cambio de proveedor. Para realizar el seguimiento de los contratos recomendamos nombrar formalmente un responsable de cada contrato que realice el seguimiento de los niveles de servicios prestados por los contratistas de TI y se documente el seguimiento realizado.

8. El Ayuntamiento tiene implementadas diferentes medidas para garantizar la seguridad en los accesos a los dos centros de proceso de datos (CPD) que incluyen el control de las personas autorizadas mediante tarjetas y de control de la seguridad ambiental de los equipos (elementos de extinción de incendios, aire acondicionado, control de temperaturas, etc.).

Sin embargo, hemos observado algunos aspectos que implican riesgos para la seguridad y el adecuado funcionamiento de los equipos:

- En uno de los CPD la capacidad de los SAI se considera insuficiente y no existen equipos electrógenos.

- La proximidad de determinadas tuberías de agua condiciona la seguridad.
- En el otro CPD el aire acondicionado debería ser reforzado. Se deberían eliminar los papeles y otros elementos almacenados.
- No existe un procedimiento que garantice la revisión periódica de las personas autorizadas para el acceso y su correspondencia con las autorizaciones vigentes.

Estas circunstancias suponen un riesgo medio sobre el adecuado funcionamiento de los equipos ubicados en el CPD, que soportan todas las actividades críticas del Ayuntamiento y de que se produzcan accesos no autorizados.

Recomendamos establecer medidas correctivas de los hechos señalados que condicionan la seguridad de los equipos ubicados en el CPD y, por ello, las actividades del Ayuntamiento.

Controles de acceso a datos y programas

9. La red local del Ayuntamiento dispone de mecanismos de seguridad para prevenir accesos no autorizados, cortafuegos y DMZ, que se encuentran adecuadamente configurados. No obstante, no se han elaborado políticas ni procedimientos escritos para configurarlos por lo que existe una dependencia de los conocimientos del personal del área de sistemas.

La situación de dependencia supone un riesgo medio sobre el adecuado funcionamiento de los sistemas en caso de bajas o cambios de puesto de trabajo del personal.

Recomendamos elaborar políticas y procedimientos escritos para llevar a cabo las tareas necesarias de configuración de la seguridad en la red local, de forma que la información esté disponible en todo momento para el Ayuntamiento. Dichos procedimientos deberían contemplar además la revisión de los registros de incidencias de seguridad y la forma de autorizar a los usuarios con permiso de acceso a los elementos de seguridad de la red.

10. No existe un procedimiento aprobado para la gestión de las altas, bajas o modificaciones de permisos de los usuarios de los sistemas de información del Ayuntamiento. El procedimiento seguido en la práctica contempla de manera informal las autorizaciones necesarias, al menos en las aplicaciones revisadas.

Tampoco se revisan con una periodicidad preestablecida los usuarios y perfiles que existen en las aplicaciones. Además, se ha observado la existencia de usuarios genéricos en el dominio Windows. Algunos usuarios tienen la capacidad en la aplicación

Sicalwin para dar altas de terceros cuando no tienen asignadas estas funciones.

Esta situación implica un riesgo alto de pérdida de trazabilidad de las acciones en la red y de accesos indebidos por la posibilidad de que existan usuarios obsoletos o con permisos que exceden a los que se necesitan para ejercer las tareas asignadas.

Recomendamos que se apruebe al adecuado nivel directivo un procedimiento escrito de gestión de usuarios. Dicho procedimiento debe contemplar además la realización periódica de revisiones de los usuarios autorizados y los permisos asignados en los sistemas y aplicaciones, de forma que se garantice que cada usuario dispone de las capacidades mínimas necesarias para desempeñar sus tareas y ninguna más y que no existen usuarios genéricos. Debe conservarse la documentación acreditativa de la realización de las revisiones, los resultados y las acciones llevadas a cabo.

Los permisos de acceso directo a la base de datos de la aplicación Sicalwin para personal diferente del que la gestiona deben eliminarse o establecer controles alternativos de revisión de accesos.

11. Las políticas de configuración de las contraseñas de las aplicaciones revisadas (Sicalwin, Firmadoc y Delta), del dominio Windows, de la base de datos y del sistema operativo que soporta la base de datos no son todo lo robustas que exigen las buenas prácticas en materia de gestión de TI.

Esta configuración de las políticas de seguridad supone un riesgo medio de accesos no autorizados o indebidos a las aplicaciones.

Recomendamos modificar las políticas de autenticación (contraseñas) y adaptarlas a los parámetros generalmente aceptados (complejidad mínima de contraseñas, historial de contraseñas, caducidad, bloqueos ante intentos fallidos, etc.).

De acuerdo con la información facilitada las políticas de acceso de la aplicación Sicalwin se han adaptado a las buenas prácticas en 2013 con posterioridad a la revisión realizada.

12. La configuración actual de los sistemas operativos no permite registrar todas las incidencias acontecidas en la red que pueden ser relevantes. Los registros de actividad en las aplicaciones Sicalwin y Delta no se revisan y los de la primera se borran periódicamente.

La ausencia de registros de auditoría de las actuaciones de los usuarios en la red en las aplicaciones para acciones importantes o la falta de revisión de los mismos supone un riesgo medio de que

no se detecten actividades inadecuadas o de que ante una incidencia que se deba investigar resulte imposible su trazabilidad.

Recomendamos modificar las directivas de auditoría del servidor controlador del dominio y activar el registro de auditoría para otras incidencias importantes, como el uso de privilegios, cambios de directivas, el acceso a objetos (carpetas y archivos). Debe aprobarse un procedimiento de revisión periódica de las actividades en la red y también en las aplicaciones críticas (incluidas Sicalwin y Delta). El procedimiento debería regular la ubicación y periodos de conservación de los registros de auditoría.

Continuidad del servicio

13. No se ha definido un plan de continuidad de la actividad que permita recuperar los procesos de gestión críticos, tras la ocurrencia de una contingencia que afecte a los sistemas de producción, en un tiempo razonable y fijado con anterioridad. Las iniciativas parciales implantadas para asegurar cierta capacidad de recuperación de los sistemas se basan exclusivamente en la realización de copias de seguridad.

Existe un riesgo alto de que, en caso de una incidencia que afecte a los procesos de gestión críticos y los sistemas de información que los soportan, 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 determinación de los activos de TI que son críticos para la Entidad y formalizar los correspondientes acuerdos de reposición de equipos, detallando los plazos máximos de respuesta y periodos de retención de la información. Debe preverse la realización de pruebas periódicas del plan de recuperación y su documentación.

14. El Ayuntamiento realiza copias de seguridad de los datos críticos con una periodicidad planificada que consideramos adecuada. No obstante, no se han definido formalmente los tiempos de retención necesarios para cada tipo de información. El departamento de sistemas ha establecido los tiempos de retención de las copias de seguridad en base a su criterio y conocimientos.

El hecho de que no se realicen pruebas de restauración de las copias de seguridad y la falta de participación de los responsables de cada proceso en la fijación de los periodos de retención de las mismas supone un riesgo medio de que la información de las copias no se encuentre disponible o de que no se adecue a las necesidades de los usuarios.

Recomendamos definir formalmente los periodos de retención de la información de la Entidad con la participación de los responsables funcionales de los procesos con el fin de asegurar que se tendrá disponible la información durante el tiempo que pueda ser necesaria o requerida. Deben realizarse pruebas periódicas de restauración que deben quedar documentadas.

En el siguiente gráfico se muestra la clasificación de las recomendaciones según los criterios combinados de riesgo potencial a mitigar y coste de su implantación (ver anexo 1).

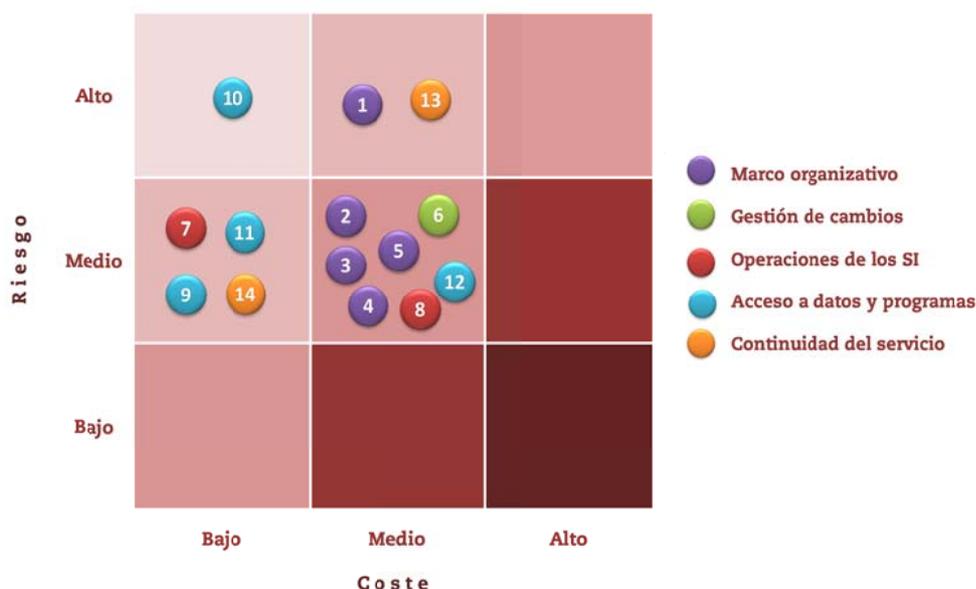


Gráfico 5

6. CONTROLES EN EL PROCESO DE GESTIÓN DE LA TESORERÍA

Los controles incorporados en las aplicaciones informáticas de gestión tienen por finalidad asegurar la integridad, exactitud y validez de las transacciones y datos durante todo el procesamiento (manual o automatizado) de las operaciones de gestión de la tesorería. Su propósito es establecer procedimientos de control específicos con el fin de asegurar razonablemente que todas las transacciones son autorizadas, registradas y procesadas de forma completa, adecuada y oportuna.

La revisión del proceso de gestión contable y de la tesorería ha incluido un análisis de riesgos y de las interfaces entre las aplicaciones implicadas en la gestión.

La siguiente tabla y gráfico muestran el grado de cumplimiento de los 54 controles del proceso de gestión que se han revisado, que refleja la existencia de un entorno general razonable de control en la Entidad.

Proceso de gestión contable y de la tesorería	Eficacia de los controles			Total controles revisados
	Efectivos	Parcialmente efectivos	No efectivos	
Controles	26	21	7	54
	48,1%	38,9%	13,0%	100,0%

Cuadro 3

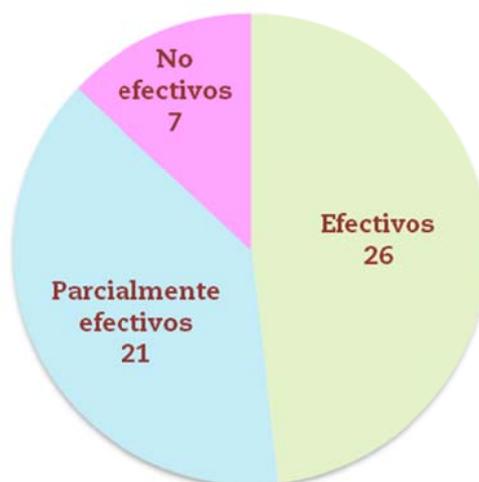


Gráfico 6

Hemos identificado y revisado 54 controles implantados en el proceso, de los cuales un 48,1% han resultado efectivos y un 38,9% parcialmente efectivos mientras que un 13,0% han resultado no efectivos.

Las principales deficiencias de control interno detectadas durante la revisión del proceso y que son susceptibles de mejora, son las siguientes:

1. La elaboración del proyecto de presupuesto se realiza a partir de los presupuestos del año anterior mediante una hoja de cálculo. Los responsables de las diferentes áreas incorporan sus previsiones de gasto y se vuelcan a la aplicación Sicalwin. Los presupuestos prorrogados se generan con un procedimiento similar.

La importación en Sicalwin de los presupuestos elaborados desde la hoja de cálculo se realiza con la ayuda de una aplicación denominada "Gestión de Presupuestos 2013", que realiza varias validaciones sobre los campos clave de los presupuestos para evitar introducir en Sicalwin información incorrecta. No obstante, la importación de los datos a Sicalwin se realiza directamente sobre la base de datos.

Los procedimientos y herramientas utilizados para elaborar los presupuestos y las prórrogas de presupuestos no incluyen controles que garanticen la integridad y adecuación de los importes

consignados por lo que existe riesgo medio de que se produzcan errores no detectados en su elaboración.

Recomendamos cambiar los procedimientos y herramientas para elaborar los presupuestos y/o establecer controles compensatorios para garantizar los cálculos realizados (por ejemplo, revisiones de los cálculos por personal diferente al que los realiza).

Se deberían utilizar las herramientas de la propia aplicación Sicalwin para elaborar el presupuesto o, alternativamente, establecer controles compensatorios, como habilitar en Oracle el registro de los cambios realizados en las tablas de la base de datos de Sicalwin (en este caso concreto para las tablas de presupuestos) y además que una persona distinta se encargue de revisar/validar la información introducida de los presupuestos.

2. Los concejales de cada área realizan sus propuestas de créditos a incluir en el presupuesto antes de su aprobación. No obstante, se ha evidenciado que no se incluyen en los presupuestos todos los gastos previstos (existen operaciones pendientes de aplicar no incluidas).

El hecho de no se incluyan en el presupuesto gastos ya realizados o que seguro que se van a realizar supone un riesgo alto de que se realicen nuevos gastos sin que se apliquen a presupuesto los ya realizados o aquellos en los que con toda seguridad se va a incurrir.

Recomendamos que al elaborar los presupuestos se tenga en cuenta todos los gastos realizados y pendientes de contabilizar y todos los gastos previstos necesarios. Los ingresos deben presupuestarse en base a previsiones fiables y justificadas.

3. El acceso de los usuarios a Sicalwin se realiza en base a los perfiles asignados a cada usuario. Sin embargo, se ha detectado un usuario, que tiene acceso a la gestión de presupuestos cuando no lo necesita para sus funciones. También se han detectado usuarios compartidos y obsoletos.

La existencia de usuarios con capacidades en la aplicación superiores a las necesarias y de usuarios compartidos u obsoletos supone un riesgo medio de accesos indebidos o no autorizados y de falta de trazabilidad de las acciones realizadas en la aplicación.

Recomendamos elaborar un procedimiento que contemple la revisión periódica los perfiles de acceso de los usuarios a la aplicación Sicalwin para garantizar que cada usuario tiene acceso a las funcionalidades que necesita para su puesto de trabajo y ninguna adicional y que no existen usuarios obsoletos o compartidos.

De acuerdo con la información facilitada con posterioridad a la realización del trabajo de auditoría, el Ayuntamiento ha revisado los usuarios de la aplicación Sicalwin y ha adecuado los permisos a las necesidades de los puestos de trabajo, lo que no ha sido objeto de verificación por la Sindicatura de Comptes.

4. Las altas de terceros las realiza el personal de Tesorería en Sicalwin y posteriormente se incorporan a la aplicación Delta cuando se verifican los pagos. Excepcionalmente los usuarios de Intervención pueden modificar los terceros y/o los documentos contables tramitados para fiscalizar o contabilizar nuevas propuestas en Sicalwin (sobre todo en el cierre contable cuando en gestión no se tiene ya acceso a la contabilidad).

La ausencia de segregación de funciones en procesos críticos como las altas de terceros y la falta de homogeneidad de los datos de terceros en ambas aplicaciones supone un riesgo medio de que se realicen pagos indebidos o no autorizados.

Recomendamos elaborar y aprobar un procedimiento para las altas de terceros en las aplicaciones que contemple la segregación de funciones entre procesos críticos (altas de terceros / contabilización / realización de pagos). Alternativamente, se podría establecer un control compensatorio de forma que las altas de terceros que se realizan en Tesorería sean fiscalizadas por la Intervención antes de ser efectivas en la aplicación.

Recomendamos unificar los datos de terceros entre Delta y Sicalwin. La disponibilidad de la documentación acreditativa de las altas de terceros en la aplicación Sicalwin sería una mejora significativa para su gestión.

5. El registro de facturas en la aplicación Sicalwin carece de algunos controles de integridad sobre la información introducida. Sicalwin permite introducir fechas de registro de las facturas anteriores a la fecha de registro real, modificar la fecha de factura, no controla o impide introducir importes desmesurados y no integra verificaciones sobre el IVA de las facturas.

La falta de controles de integridad de la información sobre las facturas recibidas implica un riesgo medio de que la información existente en la aplicación utilizada para gestionar no sea precisa.

Recomendamos establecer controles automatizados en la aplicación Sicalwin para el registro de facturas sobre la fecha de registro, fecha factura, importes y cálculos de IVA.

6. No existen procedimientos escritos formalmente aprobados sobre los diferentes tipos de controles de fiscalización previa llevados a

cabo por la Intervención y sobre la fiscalización formal y material de los pagos. Intervención realiza estas tareas en base a programas desarrollados internamente y/o listados de verificaciones que facilitan el control de la legalidad.

La ausencia de estos procedimientos aprobados para la fiscalización de expedientes supone un riesgo medio de que no se realicen, en todos los casos, las verificaciones establecidas para la fiscalización de expedientes.

Recomendamos elaborar y aprobar procedimientos para la fiscalización de los diferentes tipos de gastos, pagos e ingresos. Debería modificarse la aplicación Sicalwin para que permita realizar automatizadamente controles en los pagos sobre la contabilización de las obligaciones, los terceros, cuentas bancarias e importes propuestos para el pago.

7. Se han observado deficiencias en la restricción de acceso a determinadas carpetas que contienen datos relevantes de la gestión de pagos del Ayuntamiento.

Existe un riesgo medio de que se produzcan accesos no autorizados a dicha información.

Se recomienda establecer y formalizar un procedimiento que limite el acceso a la información relevante sobre los pagos, de forma que sólo puedan acceder a estos datos las personas que lo necesiten para sus funciones y que impida modificaciones no autorizadas.

8. Las revisiones sobre los pagos realizados por la Tesorería no se pueden realizar de forma automatizada, ya que las entidades financieras no remiten esta información detallada.

La falta de información sobre el detalle de los pagos efectivamente realizados, implica un riesgo medio de que se realicen pagos erróneos y no sean detectados.

Recomendamos que se solicite a las entidades financieras el detalle de los pagos realizados en cada remesa y elaborar y aprobar un procedimiento que prevea una revisión periódica de los pagos realizados.

9. No existe un procedimiento aprobado que regule la realización de los arqueos. Tesorería elabora los arqueos diarios de las diferentes cajas de metálico de que dispone el Ayuntamiento pero no se firman por los que los realizan y supervisan. Estas operaciones se firman por los responsables al cierre del ejercicio, en cumplimiento de la normativa y en 2013 con motivo del relevo de la tesorera.

Esta situación implica riesgo alto de que no se realicen todas las verificaciones procedentes en los arqueos y, por tanto, de que algunas incidencias sobre el efectivo puedan pasar desapercibidas.

Recomendamos elaborar y aprobar un procedimiento para la realización de los arqueos diarios, que contemple la firma por las personas que los realizan y supervisan y las verificaciones a realizar. El procedimiento debería contemplar la documentación que se debe aportar y conservar para justificar los saldos y movimientos de las cajas y la asignación de tareas.

10. Los arqueos diarios se realizan por el personal de la Tesorería que utiliza una aplicación de desarrollo propio. Se ha observado que esta aplicación presentaba, en ocasiones, un funcionamiento inadecuado, generando los arqueos con errores.

La puesta en funcionamiento de modificaciones en las aplicaciones de gestión de arqueos, sin las verificaciones procedentes, supone un riesgo medio de que los fondos en metálico del Ayuntamiento no estén adecuadamente controlados.

Recomendamos no implementar cambios en las aplicaciones de gestión financiera, sin realizar las validaciones necesarias.

11. En general, los cobros en metálico de tributos y multas se realizan en alguna de las cajas de metálico de la Corporación. Se contabilizan cuando se confecciona el arqueo diario. Sin embargo, en los ingresos por arrastre de vehículos y multas se utiliza una aplicación propia que vuelca los datos en el módulo “Cobro en tesorería” de la aplicación de Hacienda. Estos cobros no se reflejan en contabilidad hasta que se realiza el ingreso en banco o traspaso de efectivo a la caja principal y se aplican los ingresos. Las gestiones de cobro de los derechos por multas de aparcamiento y arrastres se realizan por policías municipales.

La existencia de cobros realizados no registrados en la contabilidad municipal supone un riesgo alto sobre la integridad de esos fondos.

Recomendamos modificar los procedimientos para que todos los ingresos realizados en metálico se reflejen diariamente en la contabilidad municipal. Las tareas de gestión de cobro deben asignarse al personal de Tesorería.

12. El Ayuntamiento dispone de siete cajas para cobro en metálico. Cinco de ellas se gestionan mediante un cajero automático exclusivamente. En la caja principal y en otra de las cajas de efectivo (Babel) existe personal para atender a los ciudadanos en la gestión de los ingresos.

La gestión de cobros en efectivo en cajas del Ayuntamiento supone un riesgo medio sobre la integridad de los fondos del Ayuntamiento.

Recomendamos eliminar o reducir al mínimo imprescindible los cobros en efectivo y sustituirlos por procedimientos de cobro a través de entidades colaboradoras y pago telemático.

En el siguiente gráfico se muestra la clasificación de las recomendaciones según los criterios combinados de riesgo potencial a mitigar y coste de su implantación (ver anexo I). Sólo se han considerado las recomendaciones cuya relación riesgo-coste se considera favorable para su implementación.



Gráfico 7

7. PRUEBAS DE TRATAMIENTO MASIVO DE DATOS

El alcance de las pruebas de tratamiento masivo de datos ha incluido la realización de las siguientes validaciones:

- Realizar un subconjunto de pruebas orientadas a evaluar la integridad y coherencia de la información recibida del sistema contable Sicalwin con programas de tratamiento masivo de datos.
- Verificar que los estados financieros aprobados por la Entidad correspondientes a los ejercicios 2011 y 2012 se corresponden con la información registrada y contabilizada en el programa de gestión Sicalwin.

Los resultados de las pruebas han sido, en general, satisfactorios, ya que ha sido posible comprobar que:

- La información inicial recibida de los datos extraídos de la aplicación contable Sicalwin satisface las verificaciones realizadas sobre su integridad.
- Los estados financieros (balance, cuenta de resultados económico patrimonial, presupuesto de ingresos y gastos) aprobados por la Entidad referidos a los ejercicios 2011 y 2012 se corresponden con la información de las bases de datos con la información contable detallada facilitada a la Sindicatura de Comptes.

8. SEGUIMIENTO DE LAS RECOMENDACIONES DEL INFORME SOBRE CONTROL INTERNO

En las páginas 41 y 42 del Informe sobre Fiscalización del Control Interno del Ayuntamiento de Alicante del ejercicio 2011 se indicaban nueve debilidades de control sobre la organización, las operaciones, el control de accesos y la continuidad del departamento de Sistemas de Información. Todas ellas se reiteran en las recomendaciones efectuadas en los apartados 5 y 6 de este Informe.

9. TRÁMITE DE ALEGACIONES

En cumplimiento de lo acordado por el Pleno de les Corts Valencianes en la reunión del día 22 de diciembre de 1986, así como del Acuerdo del Consell de esta Sindicatura de Comptes en el que se tuvo conocimiento del borrador del Informe de fiscalización, se remitió a los gestores del ayuntamiento fiscalizado el citado borrador para que, en el plazo concedido, formularan, en su caso, alegaciones.

En relación con el contenido de las alegaciones y su tratamiento, es preciso señalar lo siguiente:

- 1) El órgano fiscalizado ha formulado, en su caso, alegaciones y consideraciones que afectan a determinadas partes o cuestiones del Informe.
- 2) Todas las alegaciones han sido analizadas detenidamente.
- 3) Las alegaciones admitidas se han incorporado al contenido del Informe.

El texto de las alegaciones formuladas, así como el informe motivado que se ha emitido sobre las mismas que ha servido para su estimación o desestimación por esta Sindicatura, se adjuntan en los Anexos III y IV de este Informe.

APROBACIÓN DEL INFORME

De acuerdo con los artículos 17. f) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes y 60. e) de su Reglamento y, en cumplimiento del Programa Anual de Actuación de 2013 de esta Institución, el Consell de la Sindicatura de Comptes, en reunión del día 26 de febrero de 2014, aprobó este Informe de fiscalización.

Valencia, 26 de febrero de 2014

EL SÍNDIC MAJOR

A blue ink signature is written over a circular stamp. The stamp contains the text 'SINDICATURA DE COMPTES' at the top, 'RATIFICADO' in the middle, and 'SINDIC MAJOR' at the bottom. The signature is a cursive script that starts with a large 'R' and ends with a long horizontal stroke.

Rafael Vicente Queralt

ANEXO I

ENFOQUE METODOLÓGICO DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

El trabajo realizado se ha estructurado en dos grandes bloques:

- a) *Revisión de los controles generales establecidos en los sistemas de información que dan soporte al proceso de gestión revisado y a la gestión económico-financiera.*

Puesto que el proceso de gestión y las aplicaciones informáticas revisadas están soportadas por los sistemas de información, la auditoría ha incluido el análisis de los controles generales del entorno de tecnologías de la información, que establecen un marco general de confianza respecto del funcionamiento de los controles en los procesos y aplicaciones de gestión.

Para poder confiar en los controles implantados en las aplicaciones informáticas es requisito fundamental que los controles generales del entorno de TI sean efectivos y, por tanto, permitan garantizar el buen funcionamiento de aquellos, ya que, en caso contrario, no se podrá confiar en los controles automáticos embebidos en las mismas.

- b) *Revisión de los controles internos del proceso de gestión de la tesorería.*

La finalidad es determinar si el nivel de control existente en las aplicaciones y la eficacia de los controles relevantes garantizan la correcta ejecución del proceso de gestión revisado, y mitigan el riesgo de errores e irregularidades, garantizando la validez, integridad y exactitud de la información. En síntesis el procedimiento seguido ha consistido en:

1. Adquirir una comprensión adecuada del proceso de gestión auditado e identificar los riesgos existentes en cada fase del proceso y los controles implementados por el ayuntamiento; conocer y entender los sistemas informáticos involucrados, los flujos de datos que generan las operaciones y cómo impactan en los estados financieros.
2. Analizar tanto los controles automáticos embebidos en las aplicaciones informáticas como los controles manuales establecidos para mitigar los riesgos existentes.

El propósito de esa evaluación es determinar si los controles implementados en los procesos son suficientes y son eficaces en diseño (están diseñados adecuadamente para cubrir los riesgos de errores en los estados financieros en cada uno de los procesos analizados), identificando los controles relevantes o controles clave.

3. Comprobar, mediante las oportunas pruebas de auditoría, si los controles relevantes seleccionados son eficaces en su funcionamiento operativo.

Criterios de evaluación de los controles internos

Con el objetivo de facilitar la comprensión de la eficacia de los controles, éstos se han categorizado en los siguientes niveles:

Efectivos	Parcialmente efectivos	No efectivos
El control se ha implantado en su totalidad y no presenta debilidades de ningún tipo.	El control no se ha implantado en su totalidad o presenta alguna debilidad.	El control no se ha llegado a implantar o se realiza un control irregular de la actividad o no se guarda evidencia del control.

Cuadro 1

Criterios para la categorización de las recomendaciones

Las recomendaciones efectuadas están basadas en las deficiencias de control interno detectadas. Su categorización se ha establecido en función de los criterios de riesgo y coste de implantación.

El principal criterio de priorización sugerido para abordar la resolución de estas deficiencias se basa en el riesgo potencial que representa la incidencia detectada. Las primeras actuaciones a llevar a cabo serán aquellas que mitigan los riesgos de nivel alto. Seguidamente, se debería actuar sobre las acciones que mitigan riesgos de nivel medio y, en última instancia, se abordarán aquellas acciones que mitiguen riesgos de nivel bajo.

También se señala una indicación del coste o complejidad de implantación del control sugerido, de forma que se pueda efectuar una evaluación coste/beneficio de las recomendaciones propuestas.

A continuación se detallan los criterios de categorización empleados:

Criterio	Descripción	Nivel
Riesgo	Probabilidad de contingencia o vulnerabilidad acorde al impacto potencial de la incidencia detectada.	Alto Aspectos de control o debilidades materiales que pueden llegar a afectar de forma muy significativa al control interno o pueden representar un riesgo de incorrección material en las cuentas anuales.
		Medio Aspectos de control o deficiencias significativas que no representan una buena práctica y que podrían repercutir en el sistema de control interno o en la integridad de los datos.
		Bajo Deficiencias de control interno que no le afectan significativamente, ni es probable que lleguen a representar un riesgo de incorrección material en las cuentas anuales, pero que a nuestro juicio deben ser consideradas por la dirección de la Entidad.
Coste	Valoración aproximada o estimativa de los recursos que debe destinarse a la ejecución de la acción recomendada	Alto Aspecto de control o deficiencia que tiene una solución compleja y/o requiere un tiempo de implantación más largo y/o un coste elevado.
		Medio Aspecto de control o deficiencia que tiene una solución intermedia en duración y en dificultad.
		Bajo Aspecto de control o deficiencia que tiene una solución fácil y rápida.

Cuadro 2

Según la sección 850 del “Manual de fiscalización” de la Sindicatura de Comptes, las incidencias detectadas en la revisión de los controles internos se clasifican de la siguiente forma:

- Una **deficiencia de control interno** existe cuando el diseño o el funcionamiento de un control no permite al personal de la Entidad o a su dirección, en el curso ordinario de las operaciones, prevenir o detectar errores o irregularidades en un plazo razonable. Pueden ser deficiencia de diseño del control (cuando un control necesario para alcanzar el objetivo de control no existe o no está adecuadamente diseñado) o deficiencias de funcionamiento (cuando un control adecuadamente diseñado no opera tal como fue diseñado o la persona que lo ejecuta no lo realiza eficazmente).
- Una **deficiencia significativa** es una deficiencia en el control interno, o una combinación de deficiencias, que afectan adversamente la capacidad de la Entidad para iniciar, autorizar, registrar, procesar o reportar información financiera o presupuestaria de forma fiable, de acuerdo con los principios o normas contables y/o presupuestarias aplicables, y existe una probabilidad que es más que remota, de que una manifestación errónea en las cuentas anuales, que no es claramente trivial, no sea prevenida o detectada.
- Una **debilidad material** es una deficiencia significativa en el control interno o una combinación de ellas, respecto de las que existe una razonable posibilidad de que una manifestación errónea significativa en las cuentas anuales no sea prevenida o detectada y corregida en plazo oportuno.

ANEXO II

DESCRIPCIÓN DEL PROCESO DE GESTIÓN CONTABLE Y DE LA TESORERÍA

A continuación, se detallan de forma resumida las diferentes fases del proceso de gestión contable y de la tesorería.

Elaboración de los presupuestos

El presupuesto es un documento esencial para la gestión municipal que debe ser aprobado por el Pleno del Ayuntamiento.

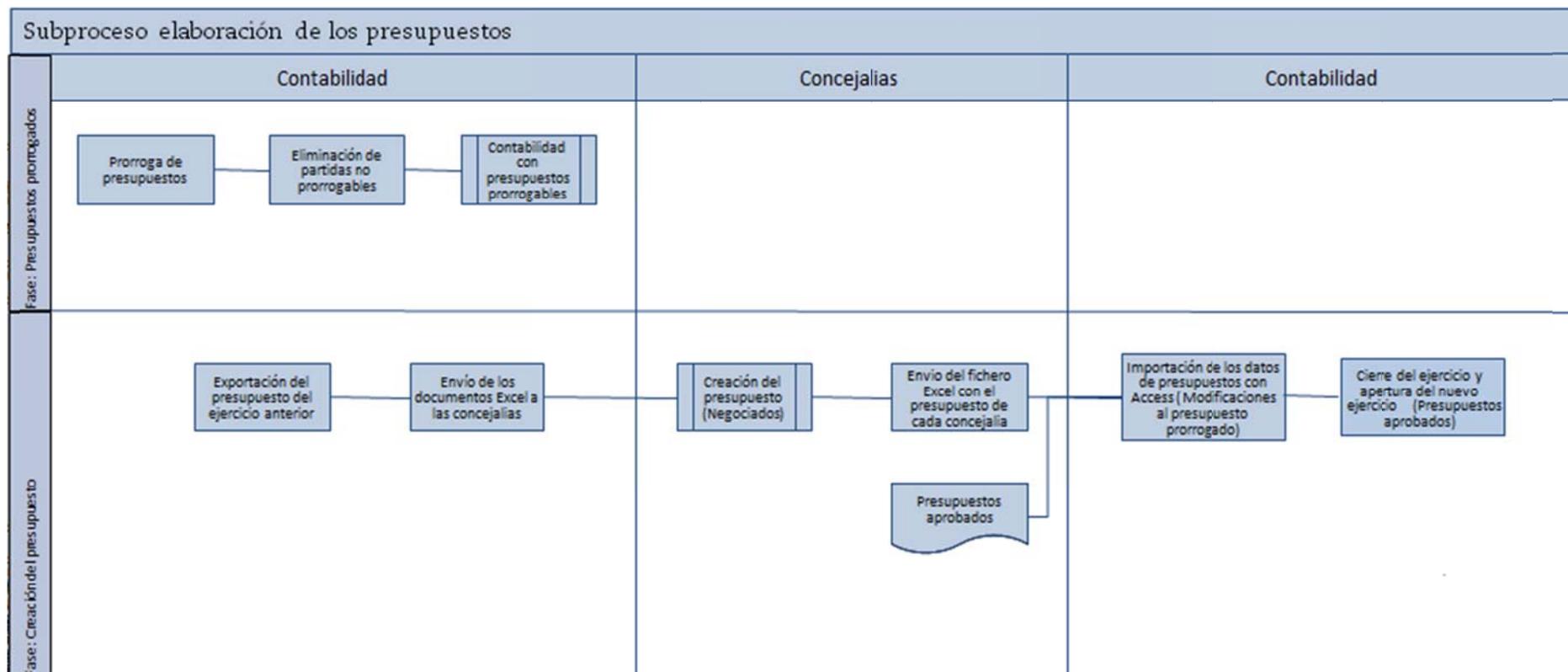
El presupuesto del Ayuntamiento de Alicante, en los últimos ejercicios (2011, 2012 y 2013) no ha sido aprobado previamente al inicio del ejercicio presupuestario, como prevé la normativa, y se han debido iniciar los ejercicios presupuestarios con una prórroga de los del ejercicio anterior.

Los créditos presupuestarios del presupuesto prorrogado se incorporan al nuevo ejercicio de forma automatizada a través de la aplicación Sicalwin, pero deben corregirse para eliminar las partidas que legalmente no pueden ser objeto de prórroga. Estas correcciones se realizan por la persona que actúa como administrador de la aplicación a través de la aplicación ACCESS y una conexión directa a la base de datos de Sicalwin.

La elaboración de los proyectos de presupuesto es un proceso en el que participan los responsables de las diferentes áreas de gestión del Ayuntamiento, que aportan sus datos sobre las necesidades presupuestarias previstas, con la participación de la Oficina Presupuestaria. El proyecto de presupuesto definitivo aprobado por la Junta de Gobierno Local, previos los informes preceptivos se remite al Pleno para su aprobación.

Cuando son necesarias modificaciones de los presupuestos disponibles, se tramitan los correspondientes expedientes de modificación de créditos que, una vez aprobados, se introducen en la aplicación Sicalwin.

La descripción gráfica del subproceso de gestión de los presupuestos se detalla en el gráfico siguiente.



Gestión de terceros

Los proveedores o acreedores del Ayuntamiento deben figurar en el registro de terceros del Ayuntamiento para que se pueda tramitar contablemente cualquier expediente de gasto.

La Tesorería del Ayuntamiento es la responsable del alta de terceros. Existe un procedimiento para dar de alta los terceros en el que los proveedores deben aportar documentalmente, a través de un modelo de instancia, sus datos personales y bancarios. Los datos correspondientes a las altas de terceros se gestionan a través de la aplicación Delta y también se introducen manualmente en la aplicación Sicalwin.

Gestión de los gastos: Retención, autorización, disposición del gasto y contabilización de la obligación reconocida

Una vez aprobados e introducidos en la aplicación Sicalwin los presupuestos disponibles (bien del presupuesto prorrogado, del presupuesto aprobado o de las modificaciones aprobadas) las diferentes áreas del Ayuntamiento pueden iniciar su gestión y realizar los pasos para utilizar los créditos disponibles.

La gestión y contabilización de gasto se efectúan por los responsables de las áreas a través de las aplicaciones Sicalwin y Firmadoc, realizando operaciones de retención de créditos, autorización, disposición de los créditos y contabilización de la obligación.

En todos los casos, las operaciones sólo las pueden realizar las personas que tienen los permisos para realizar una determinada gestión.

En general se exige la participación y firma digital de varias personas para contabilizar y aprobar un gasto y, en todos los casos, existe un procedimiento de fiscalización, también validado a través de firma digital.

Los procedimientos de gestión del gasto exigen la participación, a través de la aplicación, de las personas que tienen asignadas cada una de las tareas, de acuerdo con el procedimiento definido en la aplicación Sicalwin, de forma que un gasto no se puede aprobar por el órgano competente si previamente no ha sido propuesto por la persona que tiene la competencia.

Una vez realizado el gasto, en Intervención se registran y escanean las facturas remitidas por los proveedores que se incorporan a la aplicación Sicalwin para su contabilización y están visibles en todo momento por los participantes en el proceso.

Auditoría de eficacia de los sistemas de información y de control interno de los procedimientos de gestión de la tesorería del Ayuntamiento de Alicante. Ejercicios 2011-2013

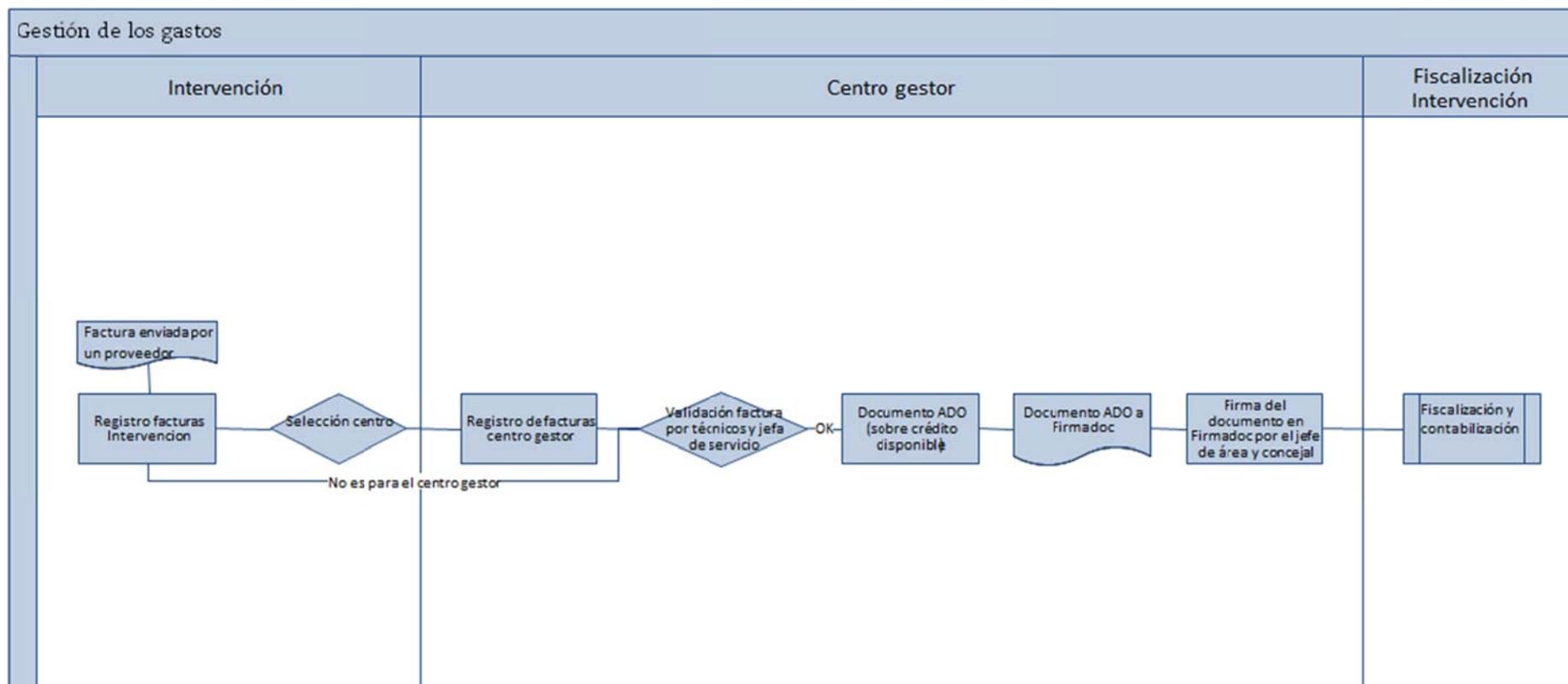
Las facturas se ponen a disposición al área competente para su tramitación, que las verifica a través de la aplicación y, mediante firmas digitales, las valida y aprueba.

Una vez aprobada, de acuerdo con los procedimientos establecidos para cada tipo de gasto, se fiscaliza y contabiliza en Sicalwin la obligación reconocida por el departamento de Intervención.

Para la fiscalización de los diferentes tipos de expedientes, la Intervención utiliza una aplicación auxiliar de desarrollo propio que contempla los tipos de verificaciones a realizar y genera los informes de fiscalización correspondientes.

Una vez fiscalizados y contabilizados los gastos, las obligaciones reconocidas están disponibles en la aplicación Sicalwin para tramitar los pagos desde la Tesorería.

La descripción gráfica del subproceso de recepción, aprobación, fiscalización y contabilización de las facturas se detalla en el gráfico siguiente.



Pagos

La gestión de las obligaciones pendientes de pago corresponde a la Tesorería municipal.

Los pagos se realizan, como norma general, mediante transferencia bancaria.

El procedimiento de gestión de pagos, parte de las obligaciones reconocidas contabilizadas en Sicalwin. Los listados de pagos pendientes se imprimen en la Tesorería para su tramitación. Las relaciones de pagos se imprimen en papel, se firman por el tesorero y el concejal de Hacienda y se remiten a Intervención para su fiscalización.

En el proceso de fiscalización, la Intervención comprueba que los pagos a realizar se corresponden con obligaciones reconocidas no pagadas, los importes totales y líquidos a pagar, las partidas presupuestarias y los terceros. Realizada la fiscalización, el Interventor firma en la aplicación Sicalwin y sobre el papel la relación de pagos.

En Tesorería, a partir de la aplicación se genera un fichero de pagos en el formato correspondiente de la Asociación Española de Banca (C34), para remitir a la Entidad financiera mediante los sistemas de pago electrónicos.

Las órdenes de pago firmadas manualmente se remiten mediante correo electrónico, fax o físicamente, según los casos, a las entidades financieras. Las entidades financieras no realizan los pagos hasta que no se remiten estas órdenes.

Además del procedimiento de pagos habitual que se ha descrito, el Ayuntamiento también cuenta con otros procedimientos de pago como son la caja fija y los pagos a justificar.

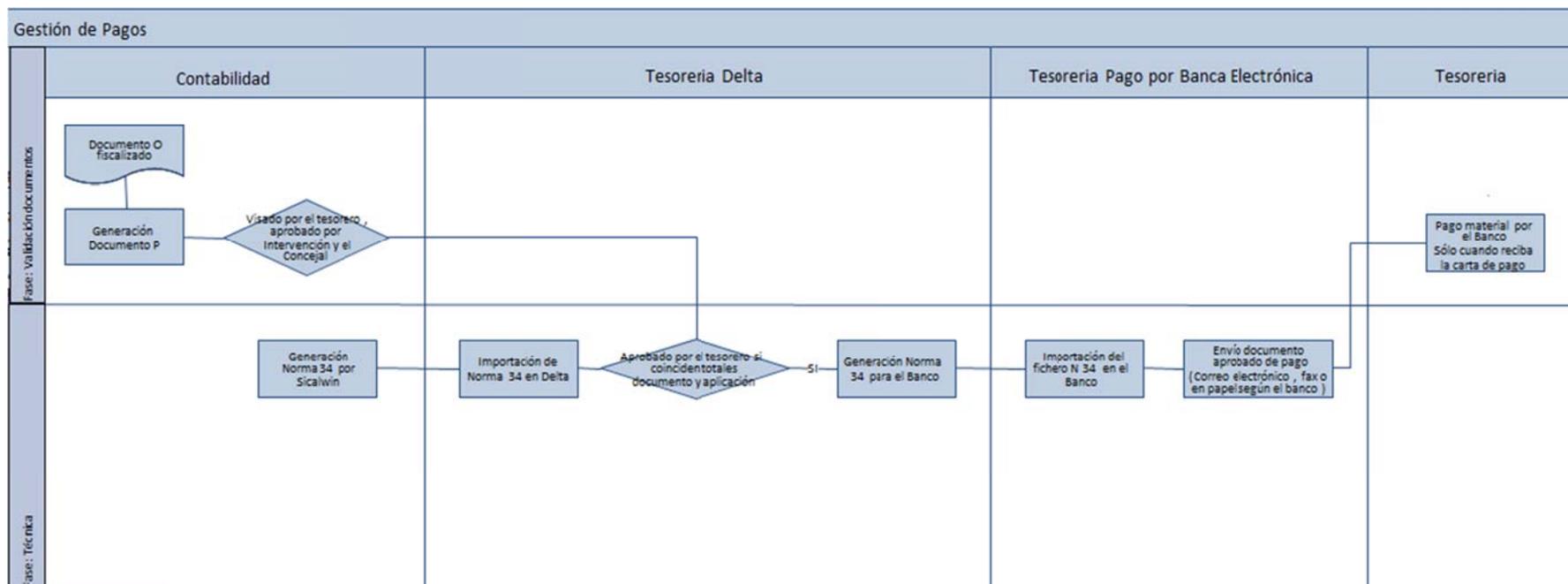
La regla 21 de las bases de ejecución del presupuesto del Ayuntamiento regula los pagos a justificar, para atender los pagos de gastos para los cuales no es posible obtener los justificantes antes del pago, si bien ésta no ha sido desarrollada por el Ayuntamiento, por lo que los procedimientos no contemplan todos los aspectos de control deseables y/o exigidos por la normativa.

En la regla 22 de las bases de ejecución del presupuesto se contemplan las normas de funcionamiento de los anticipos de caja fija a los habilitados para gastos corrientes de carácter repetitivo de importe reducido (inferiores a 2.000 euros).

En 2011 se contaba con una tarjeta de crédito que fue cancelada en 2012.

La descripción gráfica del subproceso de pagos se detalla en el gráfico siguiente.

Auditoría de eficacia de los sistemas de información y de control interno de los procedimientos de gestión de la tesorería del Ayuntamiento de Alicante. Ejercicios 2011-2013



Gestión de reintegros de pagos

El Ayuntamiento tiene establecidos procedimientos para la verificación de los pagos. Cuando se producen pagos indebidos, los departamentos de gestión afectados realizan los trámites para obtener la devolución de lo indebidamente pagado. Los importes recuperados se contabilizan en Sicalwin una vez recaudados.

Gestión de ingresos y cobros en la Tesorería

El Ayuntamiento recauda los ingresos liquidados en voluntaria, a través de sus centros de cobro (cajas de efectivo), cajeros automáticos y también mediante cuentas restringidas de recaudación en entidades bancarias colaboradoras.

La recaudación de los cobros en ejecutiva la tiene delegada en el organismo de recaudación dependiente de la Diputación de Alicante desde el ejercicio 1993.

En septiembre de 2013, el Ayuntamiento aprobó el convenio de delegación en materia de gestión, recaudación tributaria e ingresos de derecho público entre el Ayuntamiento de Alicante y la Diputación de Alicante, que extiende la colaboración en estas materias a los tributos en periodo voluntario.

El Ayuntamiento dispone de siete cajas de efectivo en diferentes dependencias municipales: 01 Caja Principal, 02 Caja tesorería (cajero), 03 Caja y cajero automático Babel (policía), 04 Cajero Tossal (piscina), 05 Caja piscina Babel, 06 Cajero estadio atletismo, 07 Cajero Castillo (a partir de 2013).

El control de los saldos de efectivo en estas cajas del Ayuntamiento se realiza a través de la aplicación “Cobro en tesorería” que genera los documentos de los arqueos diarios en las cajas de la Corporación que se utilizan como referencia para la contabilización de los ingresos y trasposos en la aplicación Sicalwin.

ANEXO III

ALEGACIONES DEL CUENTADANTE



**CONSELLERIA D'ECONOMIA,
INDÚSTRIA, TURISME I OCUPACIÓ
SERVICI TERRITORIAL DE COMERÇ
I CONSUM D'ALACANT**

Rambra de Méndez Núñez, 41
4a planta
03002 ALACANT
Telèfon 012
Fax 966.478.141

GENERALITAT VALENCIANA
CONSELLERIA D'ECONOMIA, INDÚSTRIA, TURISME I OCUPACIÓ
ST de Comerç i Consum - Alacant

Data - 8 FEB. 2014

Eixida núm.

1339



**SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA**

REGISTRE GENERAL

DATA: 07/02/2014 12.54

Núm: 201400798 ENTRADA

**SINDICATURA DE COMPTES DE LA
COMUNITAT VALENCIANA
SANT VICENT, 4
46002 VALENCIA**

De acuerdo con lo dispuesto en el artículo 38 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se acompaña a la presente el escrito recibido en este Servicio Territorial de Comercio y Consumo que a continuación se detalla:

Fecha registro	Número Registro	Interesado
5-2-2014	995	AYUNTAMIENTO DE ALICANTE (ALCALDIA)

Alicante a 06 de febrero de 2014

LA JEFA DEL SERVICIO TERRITORIAL DE COMERCIO Y CONSUMO


ANA BALLENILLA GARCIA DE GAMARRA



AYUNTAMIENTO DE ALICANTE

ALCALDÍA

AYUNTAMIENTO DE ALICANTE
REGISTRO GENERAL
S2014010600
SALIDA
05/02/2014 12:35:14

GENERALITAT VALENCIANA
CONSSELLERIA D'ECONOMIA, INDÚSTRIA, TURISME I OCUPACIÓ
SI de Comerç i Consum - Alacant

Data - 5 FEB. 2014

Entrada núm. 995

Fecha: 04 de febrero de 2014.

Asunto: Alegaciones informe

Remitente: Oficina presupuestaria

Destinatario:

Excmo. Sr. Síndic de Comptes
SINDICATURA DE COMPTES

c/San Vicente 4
46002 - VALENCIA

Una vez examinado por diferentes servicios municipales el borrador de sus informes sobre "Diversos aspectos de la actividad económico-financiera del Ayuntamiento de Alicante. Ejercicio presupuestario 2011" y sobre "Auditoria de eficacia de los sistemas de información y de control de los procedimientos de gestión de la Tesorería del Ayuntamiento de Alicante. Ejercicio 2011-2013", y dentro del plazo que al efecto se nos concedió, adjunto le remito las alegaciones que al respecto creemos necesario formular.

Quedamos a su disposición para cualquier aclaración que precise al respecto.



LA ALCALDESA

Fdo. Sonia Castedo Ramos



AYUNTAMIENTO DE ALICANTE

Alegaciones que se formulan al borrador de informe sobre “Auditoria de eficacia de los sistemas de información y de control interno de los procedimientos de gestión de la Tesorería del Ayuntamiento de Alicante. Ejercicios 2011-2013”

Primera Alegación.-

Al Apartado. 1 del borrador de Informe. Marco Organizativo. Pág. 10.

Contenido de la Alegación.-

Todos los textos normativos que integrarán la política general de seguridad de la información del Ayuntamiento se encuentran ya elaborados y pendientes tan solo de una última revisión para iniciar su tramitación al Pleno Municipal.

Por lo que se solicita se proceda a la modificación de su informe, dejando sin efecto las calificaciones expresadas así como las recomendaciones derivadas de las pretendidas debilidades y reflejando todo ello en sus conclusiones generales.

Segunda Alegación.-

Al Apartado. 3. Planes de adecuación a los esquemas nacionales de Seguridad. Pág. 11.

Contenido de la Alegación.-

El R.D. 3/2010, de 8 de enero que regula el Esquema Nacional de Seguridad establece hasta el 30 de enero de 2014 como plazo para aprobar el documento de adecuación al Esquema Nacional de Seguridad. El Ayuntamiento tiene previsto acometer la confección y aprobación de dicho documento en el presente ejercicio, una vez se apruebe la normativa que constituya la política general de Seguridad de la Información.

Por lo que se solicita se proceda a la modificación de su informe, dejando sin efecto las calificaciones expresadas así como las recomendaciones derivadas de las pretendidas debilidades y reflejando todo ello en sus conclusiones generales.

Tercera Alegación.-

Apdo. 4. Documento de Seguridad L.O.P.D. Pág.11.

Contenido de la Alegación.-

A fecha de emisión de las presentes alegaciones el Ayuntamiento de Alicante ya dispone del Documento de Seguridad que prescribe la L.O. 15/1999, de 13 de



AYUNTAMIENTO DE ALICANTE

diciembre, de Protección de Datos de Carácter Personal. Asimismo, cuenta con un responsable de Seguridad de la Información formalmente designado.

Por lo que se solicita se proceda a la modificación de su informe, dejando sin efecto las calificaciones expresadas así como las recomendaciones derivadas de las pretendidas debilidades y reflejando todo ello en sus conclusiones generales.

Documentación justificativa de la alegación:

Se adjunta como documentos anexo nº 1 fotocopia compulsada del decreto de nombramiento del responsable de Seguridad de la Información en el Ayuntamiento de Alicante y como anexo nº 2 documento acreditativo de la recepción del Documento de Seguridad del Ayuntamiento de Alicante.

Cuarta Alegación.-

Al Apartado 6. Procedimiento de identificación y comunicación de las necesidades de software y gestión de cambios en las aplicaciones. Pág. 12.

Contenido de la Alegación.-

El Ayuntamiento de Alicante dispone de un procedimiento aprobado por el adecuado nivel directivo de identificación y comunicación de las necesidades de software y de la gestión de cambios en las aplicaciones tal y como se acredita mediante el documento anexo.

Dicho procedimiento tiene definidas internamente distintas categorías de cambios, de tal modo que en cada categoría, se define el perfil de usuario que la puede solicitar, indicándose si es necesario que la petición vaya firmada digitalmente o no.

Existe asimismo, un entorno de pruebas en el cual se efectúan siempre todas las que se estiman necesarias, no pasándose a producción hasta que estas son satisfactoriamente aprobadas por el jefe del departamento correspondiente.

Por lo que se solicita se proceda a la modificación de su informe, dejando sin efecto las calificaciones expresadas así como las recomendaciones derivadas de las pretendidas debilidades y reflejando todo ello en sus conclusiones generales.

Documentación justificativa de la alegación:

Se adjunta como documento anexo nº 3 fotocopia compulsada del documento de referencia.



AYUNTAMIENTO DE ALICANTE

Quinta Alegación.-

Al Apartado. 7. Operaciones de los sistemas de Información. Gestión de los proveedores de servicios y cláusulas de confidencialidad. Pág. 13.

Contenido de la Alegación.-

El borrador de informe recomienda nombrar formalmente un responsable de cada contrato para realizar su seguimiento, cuando lo cierto y así queda acreditado en toda la documentación contractual disponible en este Servicio, es que, en desarrollo de lo dispuesto en el art. 52.1 del Texto Refundido de la Ley de Contratos del Sector Público aprobado por RDLeg 3/2011, de 14 de noviembre, la base 18 de Ejecución de Presupuesto Municipal aprobado por acuerdo plenario de este Ayuntamiento, en su apartado primero, punto 7, contempla y define la figura del responsable del contrato que cumple, entre otros, con dicho cometido.

Por otro lado, en todos los contratos tramitados desde este Servicio que puedan tener la más mínima trascendencia a efectos de tratamiento de información, se incluye una cláusula de confidencialidad.

Por lo que se solicita se proceda a la modificación de su informe, dejando sin efecto las calificaciones expresadas así como las recomendaciones derivadas de las pretendidas debilidades y reflejando todo ello en sus conclusiones generales.

Documentación justificativa de la alegación:

La Base 18 de Ejecución de Presupuesto Municipal alegada, se encuentra accesible en la página web del Ayuntamiento de Alicante; perfil del contratante; normativa, modelos y legislación de contratación.

Sexta Alegación.-

Al Apartado. 8. Seguridad en los accesos a los centros de proceso de datos (CPD). Pág. 14.

Contenido de la Alegación.-

En el párrafo quinto del apartado 8 del informe se exponen deficiencias y se recomienda reforzar el aire acondicionado del CPD y eliminar los papeles y otros elementos almacenados en el mismo.

A fecha de redacción de las presentes alegaciones ya se encuentra reforzado el aire acondicionado del CPD y se han retirado del mismo los papeles y demás elementos almacenados de forma idónea.

Por lo que se solicita se proceda a la modificación de su informe, dejando sin efecto las calificaciones expresadas así como las recomendaciones derivadas de las pretendidas debilidades y reflejando todo ello en sus conclusiones generales.



AYUNTAMIENTO DE ALICANTE

Séptima Alegación.-

Al Apartado 12. Pág. 16.

Contenido de la Alegación.-

Establece el borrador de informe que la configuración de los sistemas operativos no permite el registro de todos los eventos que pueden ser relevantes, sin embargo:

- En la actualidad las unidades de red usadas por el Ayuntamiento se encuentran alojadas en cabinas NetApp FAS, con sistema operativo Data Ontap.
- Las unidades de red CIFS, las soporta un software original de Microsoft Windows y la seguridad es la de un sistema de ficheros NTFS.
- Los eventos de los que se guarda registro, son los que se han considerado mas relevantes considerando las limitaciones de espacio de almacenamiento que se tienen.
- Se almacenan las conexiones al recurso de red y el borrado de archivos y carpetas.
- Los ficheros de auditoria resultantes son tratados por el sistema de copia de seguridad, llevándose a cinta con una retención de 1 año.
- En BBDD son las propias aplicaciones las que registran los accesos y cambios que consideran relevantes.
- **Conclusión**, se guardan los registros de los eventos que se han considerado oportunos y relevantes durante un año.

Por lo que se solicita se proceda a la modificación de su informe, dejando sin efecto las calificaciones expresadas así como las recomendaciones derivadas de las pretendidas debilidades y reflejando todo ello en sus conclusiones generales.

Octava Alegación.-

Al Apartado 13. Continuidad del servicio. Pág. 16.

Contenido de la Alegación.-

- Aunque no se dispone de un documento que estructure un plan único de recuperación, está montada una estructura que dota de protección contra desastres y alta disponibilidad a determinados servicios.
- Base de Datos.
 - Se encuentran sincronizadas la BBDD de producción y la secundaria. Existe el procedimiento diario de comprobación de la correcta sincronización de las BBDD, documentado y planificado en la herramienta de generación de tareas.
 - Está documentado con todo detalle la activación de la BBDD secundaria al rol de primaria en caso de desastre.
 - Entendemos que la BBDD, que es un activo crítico, tiene un plan de continuidad.



AYUNTAMIENTO DE ALICANTE

- Almacenamiento en red.
 - Ciertos recursos de red CIFS (los considerados imprescindibles para el funcionamiento de los servicios críticos: policía y recursos de red necesarios para la ejecución de aplicativos de usuario) y volúmenes asociados a la base de datos y a los datastores de producción del entorno de virtualización se encuentran en un sistema en cluster, sincronizados de forma instantánea. Ante cualquier incidencia o desastre en uno de los dos CPDs se dispone inmediata y automáticamente de esta información. Se encuentran documentados los procedimientos de manejo del cluster de almacenamiento.
 - Como en el caso de la BBDD, este es un recurso crítico y entendemos que constituye un plan de continuidad.
- Sistema virtualizado.
 - Los servidores que actúan como virtualizadores son 4, 3 en el CPD1 y 1 en el CPD2.
 - Las MVs consideradas críticas se encuentran en volúmenes sincronizados en ambos CPDs. Ante un desastre en uno de los dos CPDs las MVs consideradas críticas pasarán a ejecutarse en los virtualizadores del CPD superviviente ya que todos los recursos necesarios están inmediatamente disponibles.
 - La arquitectura actual ofrece continuidad a las MVs críticas ante incidencias.
- Sistema de Mensajería.
 - El sistema de mensajería está montado en una MV de las consideradas críticas, por tanto dispone de continuidad tal y como se describe para el sistema virtualizado.

Por lo que se solicita se proceda a la modificación de su informe, dejando sin efecto las calificaciones expresadas así como las recomendaciones derivadas de las pretendidas debilidades y reflejando todo ello en sus conclusiones generales.

Novena Alegación.-

Al Apartado 6 punto 1.- página 19.-

Contenido de la Alegación:

Los datos del presupuesto se vuelcan a la aplicación de formación presupuestaria de SicalWin antes de su aprobación por el Pleno, incluso antes de la aprobación del proyecto de presupuesto por la Junta de Gobierno Local, ya que el expediente del presupuesto se forma con los datos y listados obtenidos desde la base de datos de formación presupuestaria de SicalWin. Dado que el expediente se forma con la información obtenida desde esa base de datos de SicalWin, no es posible que se produzcan errores no detectados en su elaboración.



AYUNTAMIENTO DE ALICANTE

Además se realiza la fiscalización previa y completa de los presupuestos por parte de la Intervención General (personal diferente del que realiza la formación presupuestaria), con la información obtenida de la base de datos de formación presupuestaria de SicalWin. Los cálculos se realizan por el propio sistema y son verificados y fiscalizados por la Intervención General.

Se solicita sea eliminado el punto 1.- dado que, como se ha explicado, resulta imposible que se produzcan errores no detectados en la elaboración presupuestaria.

Décima Alegación.-

Al Apartado 6 punto 5.- página 21.-

Contenido de la Alegación:

Existe un parámetro en la aplicación que permite bloquear la fecha de registro de la factura. Si dicho parámetro establece que la fecha de registro está bloqueada, este campo se informa siempre con la fecha del día en el que se produce el registro de la factura. Sin embargo, en la mayor parte de las entidades existe la necesidad de desbloquear este campo para poder informar una fecha diferente a la del día del registro. Un claro ejemplo de esta situación es cuando un proveedor presenta una factura por el registro general de documentos, y la misma no se incorpora al sistema contable en el mismo día. En ese caso, la fecha de registro de la factura ha de ser la que corresponde al momento del registro del documento en el registro general, que obviamente es anterior a la del día del registro.

Documentación justificativa de la alegación:

Nº. 5.- Pantalla demostrativa de bloqueo de fecha de registro.-

Respecto de la posibilidad de introducir una factura con una fecha de emisión posterior a la fecha de registro, certificamos que es imposible hacer esta operación.

La posibilidad de modificar la fecha de emisión de una factura existe en los mismos términos que se ha explicado anteriormente y siempre y cuando dicha factura no se haya contabilizado, ya que en ese momento, la operación contable en la que se soporta hereda la fecha de la factura e impide que se modifique la misma, y no solo la fecha, sino ningún otro dato de dicha factura. Para poder realizar cualquier modificación sobre la factura, sería necesario anular la operación contable asociada.

Documentación justificativa de la alegación:

Nº.6.- Pantalla control de disponible en facturas.-



AYUNTAMIENTO DE ALICANTE

En cuanto a las verificaciones del IVA de la factura sí que existen en la aplicación pero el Ayuntamiento no las graba con esos datos ya que no se trata de IVA soportado deducible y se decidió por la Intervención General economizar en la introducción de datos ya que es una información que no afecta contablemente a la Entidad. En el caso de que se introdujese esa información en el registro el sistema realizaría las verificaciones pertinentes sobre el % de IVA y sus resultados numéricos.

Documentación justificativa de la alegación:

Nº.7- Pantallas demostrativas control de I.V.A.

Se solicita sea eliminado el punto 5.- dado que, como se ha explicado, ya existen en la aplicación SicalWin los controles automatizados que se recomiendan.

Décimo Primera Alegación.-

Al Apartado 6 punto 6.- página 22.-

Contenido de la Alegación:

La aplicación de fiscalización utiliza los procedimientos desarrollados en la Resolución de 4 de julio de 2011, de la intervención General de la Administración del Estado, por la que se publica el Acuerdo del Consejo de Ministros, de 1 de julio de 2011, por el que se modifica el de 30 de mayo de 2008, por el que se da aplicación a la previsión de los artículos 152 y 147 de la Ley General Presupuestaria, respecto al ejercicio de la función interventora en régimen de requisitos básicos.

Sin la fiscalización positiva a través de esta aplicación no se dará la fiscalización por realizada y los procedimientos vienen recogidos en el texto en que se basa la misma.

En cuanto a SicalWin disponemos de un módulo de áreas gestoras donde se han definido los estados y trámites que proporcionan un circuito de tramitación que permita una fiscalización exhaustiva de cada fase contable antes de ser aprobada definitivamente. No se permite la eliminación física de operaciones, siendo necesario la anulación de las operaciones que tras ser aprobadas definitivamente, tenga algún defecto en forma no detectado anteriormente en el circuito de tramitación o fiscalización. Todos estos registros quedan almacenados en nuestras bases de datos, donde se guarda el usuario y fecha de sistema, de cada una de las anotaciones realizadas.

Documentación justificativa de la alegación:

Nº.8- Pantallas demostrativas procesos fiscalización.-



AYUNTAMIENTO DE ALICANTE

Existen controles en la aplicación que impiden poder crear terceros con NIF o CIF incorrectos y cuentas bancarias erróneas.

Documentación justificativa de la alegación:

Nº.9- Pantallas demostrativas control CIF/ NIF y cuentas bancarias.-

Respecto del control de los saldos de obligaciones, los controles de la aplicación son exhaustivos: por un lado no se puede realizar una orden de pago si la correspondiente obligación no tiene saldo suficiente, si la partida afectada no tiene saldo suficiente, ni si la bolsa de vinculación tiene saldo suficiente. El tercero y las cuentas bancarias de las órdenes de pago y de los pagos los toma el sistema del tercero informado en la obligación.

Documentación justificativa de la alegación:

Nº.10- Pantalla demostrativa control Orden de pago sobre Obligación Reconocida.

Se solicita sea eliminado el punto 6.- dado que, como se ha explicado, ya existen los procedimientos, al estar basados en la Legislación referenciada anteriormente. Además en la aplicación SicalWin los controles automatizados que se recomiendan, existen, están en funcionamiento y son de ejecución obligada.

Es todo cuanto se tiene el deber de informar

Alicante, a 4 de febrero de 2014



La Alcaldesa

Fdo.: Sonia Castedo Ramos



AYUNTAMIENTO DE ALICANTE

RELACION DE DOCUMENTOS JUSTIFICATIVOS APORTADOS JUNTO A LAS ALEGACIONES FORMULADAS AL INFORME DE LA SINDICATURA DE CUENTAS RELATIVO A LA "AUDITORIA DE EFICACIA DE LOS SISTEMAS DE INFORMACION Y DE CONTROL INTERNO DE LOS PROCEDIMIENTOS DE GESTION DE TESORERIA DEL AYUNTAMIENTO DE ALICANTE. EJERCICIOS 2011-2013"

Página 1. Tercera Alegación.-

Al Apartado. 4. Documento de Seguridad L.O.P.D. Pág.11.

DOCUMENTOS:

Nº.1- Fotocopia compulsada del decreto de nombramiento del responsable de Seguridad de la Información en el Ayuntamiento de Alicante

Nº.2-Documento acreditativo de la recepción del Documento de Seguridad del Ayuntamiento de Alicante

Página 2.Cuarta Alegación.-

Al Apartado 6. Procedimiento de identificación y comunicación de las necesidades de software y gestión de cambios en las aplicaciones. Pág. 12.

DOCUMENTO:

Nº.3- fotocopia compulsada del documento de referencia.

Página 3. Quinta Alegación.-

Al Apartado. 7. Operaciones de los sistemas de Información. Gestión de los proveedores de servicios y cláusulas de confidencialidad. Pág. 13.

DOCUMENTO:

Nº.4- La Base 18 de Ejecución de Presupuesto Municipal



AYUNTAMIENTO DE ALICANTE

Página 6. Décima alegación.-

Al Apartado 6 - punto 5.- página 21.-

DOCUMENTOS:

Nº. 5.- Pantalla demostrativa de bloqueo de fecha de registro.-

Nº.6.- Pantalla control de disponible en facturas.-

Nº.7- Pantallas demostrativas control de I.V.A.

Página 7.- Décimo Primera Alegación.-

Al Apartado 6- punto 6.- página 22.-

DOCUMENTOS:

Nº.8- Pantallas demostrativas procesos fiscalización.-

Nº.9- Pantallas demostrativas control CIF/ NIF y cuentas bancarias.-

Nº.10- Pantalla demostrativa control Orden de pago sobre Obligación Reconocida.

ANEXO IV

INFORME SOBRE LAS ALEGACIONES PRESENTADAS

ANÁLISIS DE LAS ALEGACIONES EFECTUADAS AL BORRADOR DE INFORME DE FISCALIZACIÓN DE AUDITORÍA DE EFICACIA DE LOS SISTEMAS DE INFORMACIÓN Y DE CONTROL INTERNO DE LOS PROCEDIMIENTOS DE GESTIÓN DE LA TESORERÍA DEL AYUNTAMIENTO DE ALICANTE. EJERCICIOS 2011-2013

Se han analizado las alegaciones recibidas el 7 de febrero de 2014 y con respecto a las mismas se informa lo siguiente:

Primera alegación

Apartado 1 del borrador de Informe. Marco Organizativo.

Comentarios:

En la alegación se hace una afirmación en el sentido de que ya se encuentran elaborados los documentos que integran la política de seguridad que se encuentran pendientes de aprobación.

No se aporta documentación acreditativa de que se haya aprobado una política general de seguridad. Los documentos aportados hacen referencia a una política de seguridad de los datos personales que constituye sólo una parte de la política general de seguridad.

Consecuencias en el Informe:

No procede modificación.

Segunda alegación

Apartado 3. Planes de adecuación a los esquemas nacionales de Seguridad.

Comentarios:

Se indica en la alegación que se tiene previsto aprobar en 2014 el plan de adecuación al RD 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad, pero no se aporta documentación acreditativa de que se haya elaborado.

Consecuencias en el Informe:

No procede modificación.

Tercera alegación

Apartado 4. Documento de Seguridad L.O.P.D.

Comentarios:

Se alega que el Ayuntamiento ya dispone del Documento de Seguridad de la Información exigido por la LO 15/1999, de 13 de diciembre. En la documentación se aporta una certificación sobre la recepción del documento en el Ayuntamiento, pero no se aporta el propio documento ni su acuerdo de aprobación.

Consecuencias en el Informe:

No procede modificación.

Cuarta alegación

Apartado 6. Procedimiento de identificación y comunicación de las necesidades de Software y gestión de cambios en las aplicaciones.

Comentarios:

Se indica en las alegaciones que sí existe un procedimiento para identificación y comunicación de necesidades de software y para los cambios en aplicaciones.

No se aporta documentación en relación con el procedimiento de identificación y comunicación de necesidades de software.

En relación con el procedimiento de gestión de cambios en aplicaciones el documento aportado, esquemático y breve, contempla algunos de los controles de un procedimiento de este tipo, pero no todos.

Consecuencias en el Informe:

Modificar el segundo párrafo del apartado 5.6 del borrador, que queda redactado como sigue:

“Respecto a la gestión de cambios, si bien se cuenta con procedimientos técnicos asociados queda pendiente el desarrollo de los siguientes aspectos:

- Creación de un entorno de pruebas.
- Inclusión en el procedimiento de las pruebas a realizar y su aprobación previa al pase a producción.
- Definición de un proceso de emergencia para revertir posibles cambios defectuosos.
- Registro de cambios realizados.”

Quinta alegación

Apartado 7. Operaciones de los sistemas de Información. Gestión de los proveedores de servicios y cláusulas de confidencialidad.

Comentarios:

Se indica que en la legislación de contratos y la base 18ª se prevé la figura del responsable del contrato y que en todos los contratos tramitados que sean mínimamente relevantes se incluye una cláusula de confidencialidad.

Sin embargo, en la revisión realizada se observó la existencia de contratos de los que no existían cláusulas sobre niveles de servicio y/o de confidencialidad, entre ellos el de la aplicación Sicalwin.

Consecuencias en el Informe:

No procede modificación.

Sexta alegación

Apartado 8. Seguridad en los accesos a los centros de proceso de datos (CPD).

Comentarios:

En la alegación se indica que se ha corregido alguna de los factores de riesgo sobre la seguridad del Centro de Proceso de Datos (CPD).

Las conclusiones y recomendaciones se refieren a la fecha de revisión. No se aporta evidencia de las mejoras realizadas.

Consecuencias en el Informe:

No procede modificación.

Séptima alegación

Apartado 12.

Comentarios:

Se indica que existen diversos sistemas para el almacenamiento de eventos ocurridos en los sistemas de información señalando que se almacenan “los que se han considerado más relevantes” y por un año.

No se aporta acreditación de la modificación de directivas de auditoría ni de la activación del registro de auditoría y no consta que se haya

aprobado un procedimiento de revisión periódica de eventos y actividades en la red. Además, el periodo de retención de un año no se considera suficiente.

Consecuencias en el Informe:

No procede modificación.

Octava alegación

Apartado 13. Continuidad del servicio.

Comentarios:

En la alegación se hace referencia a una serie de sistemas, técnicas y configuraciones en alta disponibilidad de diferentes sistemas críticos que se identificaron durante el trabajo realizado.

Sin embargo en el informe se hace referencia a un plan de continuidad aprobado a alto nivel directivo, que incluye la aprobación de una serie de previsiones (sobre sistemas críticos, tiempos de recuperación y periodos de retención de la información) que no están definidas en las técnicas descritas en la alegación. Tampoco se indica nada en la alegación sobre la realización de pruebas periódicas.

Consecuencias en el Informe:

No procede modificación.

Novena alegación

Apartado 6, punto1.

Comentarios:

La alegación detalla una serie de procedimientos seguidos en el Ayuntamiento para la elaboración del presupuesto que, de acuerdo con su criterio, garantizan que no existan errores y que se revisan a posteriori los datos introducidos a través de la fiscalización de la Intervención General.

La incidencia puesta de manifiesto en el informe se centra en la utilización de una aplicación externa a la aplicación contable Sicalwin que permite la grabación de datos sobre el presupuesto de forma directa sobre la base de datos de esta última aplicación. Los controles descritos en la alegación no garantizan que, una vez realizados los procesos de revisión, no se modifiquen los importes consignados.

Consecuencias en el Informe:

No procede modificación.

Décima alegación

Apartado 6, punto 5.

Comentarios:

Se indica que para determinados supuestos es necesario desbloquear los datos de registro de facturas y que la fecha de emisión de la factura sólo se puede modificar hasta que se contabiliza. Respecto a los cálculos de IVA se indica que no se verifican por economía en la entrada de datos.

Los controles de integridad en la entrada de datos de documentos tales como las facturas, son esenciales para garantizar la fiabilidad de los datos procesados en el sistema contable. Los recomendados en este apartado del informe son los habituales en los procesos de gestión de compras. Respecto a la fecha de registro, una interfaz con el registro general de entrada mejoraría el control de la integridad sobre este dato.

Consecuencias en el Informe:

No procede modificación.

Décimo primera alegación

Apartado 6, punto 6.

Comentarios:

Se señala en la alegación que los procesos de fiscalización están definidos en la aplicación de fiscalización utilizada y en el circuito de tramitación de documentos de Sicalwin. Se indican controles específicos sobre NIFs y cuentas bancarias así como sobre los saldos de obligaciones en los pagos a realizar.

No obstante, de acuerdo con la revisión realizada, la aplicación de fiscalización permite gestionar sin considerar todos los controles previstos en la misma y la firma de los documentos en Sicalwin no garantiza, por si misma, que la fiscalización se haya realizado correctamente. Para este fin, la existencia de procedimientos de fiscalización aprobados es un control deseable.

Consecuencias en el Informe:

No procede modificación.