Auditoría de Ofimatica

Introducción

La ofimática se entiende como el sistema informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento de la oficina.

El concepto nace a comienzos de la década de los 90, y las primeras aplicaciones se desarrollan sobre las computadoras centrales de las organizaciones. Las oficinas siempre han sido consideradas como pioneras en la utilización de herramientas informáticas para el desarrollo de sus actividades. Ejemplos de ello son: las aplicaciones específicas para la gestión de tareas, como hojas de cálculo o procesadores de textos; herramientas para la gestión de documentos, como control de expedientes; agendas y bases de datos personales.

La evolución sufrida en el entorno microinformático ha condicionado el desarrollo de los sistemas ofimáticos actuales. El aumento de la potencia de cálculo, la alta calidad de los productos y la reducción de costes de los computadores personales, ha desplazado el desarrollo de aplicaciones ofimáticas a plataformas microinformáticas y redes de área local. Hoy en día, parece incuestionable que los productos desarrollados en plataformas microinformáticas ofrecen unas prestaciones y una relación coste/beneficio muy superior a las soluciones sobre computadoras centralizadas.

Podemos aproximar el concepto de escritorio virtual como un único panel, representado por la pantalla del computador, que sustituya la mesa de trabajo tradicional, y donde se encuentre disponibles todas las herramientas necesarias para desarrollar las actividades del oficinista. La totalidad de los paquetes ofimáticos presentes en el mercado se han desarrollado siguiendo el paradigma del escritorio virtual alcanzando un grado de desarrollo aceptable incluso facilitando la integración con otros productos de diferentes fabricantes.

Controles de auditoría

Existen dos características peculiares de los entornos ofimáticos: la distribución de las aplicaciones por los diferentes departamentos de la organización en lugar de encontrarse en una única ubicación centralizada; y el traslado de la responsabilidad sobre ciertos controles de los sistemas de información a usuarios finales no dedicados profesionalmente a la informática, que pueden no comprender de un modo adecuado la importancia de los mismos y la forma de realizarlos.

Como consecuencia, se ha generado una problemática propia de este tipo de entornos: adquisiciones poco planificadas; desarrollos ineficaces e ineficientes, incluso en procesos críticos para el correcto funcionamiento de la organización; falta de conciencia de los usuarios acerca de la seguridad de la información; utilización de copias ilegales de aplicaciones; procedimientos de copias de seguridad deficientes; escasa formación del personal; ausencia de documentación suficientes; etc.

Considerando los problemas expuestos, se ha elaborado una relación de controles de auditorías básicos, han sido descriptos de tal modo que puedan ser de aplicación a cualquier organización, adaptándolos a las características de la misma.

Los controles, que se presentan agrupados siguiendo los criterios relacionados con aspectos de economía, eficacia y eficiencia; seguridad y condicionantes legales, son lo suficientemente generales para servir de base en la elaboración del guion de trabajo de la labor del equipo auditor.

Economía, eficacia y eficiencia

Determinar si el inventario ofimático refleja con exactitud los equipos y aplicaciones existentes en la organización.

A causa del bajo coste de muchos componentes, resulta difícil mantener un registro fiable de todas las compras que realiza la organización. Con frecuencia algunos departamentos sortean los procedimientos de autorizaciones de compra establecidos dentro de la organización, por ejemplo, utilizando facturas de adquisición de material no inventariable.

Un inventario poco fiable puede repercutir en el balance de la organización, posibilitando que no se detecten sustracciones de equipamiento informático o de licencias de programas contratadas. La fiabilidad del inventario resultara indispensable para auditar otros controles presentados posteriormente.

El equipo auditor comprobara que se han definido mecanismos para garantizar que todos los equipos adquiridos en la organización son debidamente inventariados.

Después, constatara la conciliación realizada en la última auditoría financiera entre el inventario oficial y las adquisiciones efectuadas. Más tarde, revisando todas las dependencias, almacenes y archivos, elaborara una relación exhaustiva de los equipos informáticos y de las aplicaciones y archivos que residen en los mismos.

Finalmente, identificara las diferencias reales entre la relación elaborada por el equipo auditor y el inventario oficial para proceder a la subsanación de los errores detectados.

Determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones.

Una política de adquisiciones descentralizada en la que cada departamento se encargue de realizar sus compras, ofrece ventajas en cuanto a flexibilidad y capacidad de reacción de los mismos, pero podría acarrear significativas pérdidas económicas para el conjunto de la organización,

El equipo auditor comprobara que en el procedimiento de adquisición se valoran los aspectos relativos a la necesidad real de los equipos solicitados y a la integración de dichos equipos con el sistema existente. En el caso de compra de paquetes o de contratación de desarrollos externos, determinara si las prestación ofrecidas por el producto solicitado se ajustan a las actividades que se pretenden desarrollar con él, si las plataformas en las que van a ser instaladas las aplicaciones tienen suficiente capacidad para soportarlas de un modo eficiente; si los nuevos productos pueden configurarse, en caso de necesidad, para obtener suficientes pistas de auditoria que permitan efectuar un seguimiento de las anomalías producidas durante su ejecución; y la experiencia y solvencia del proveedor.

Partiendo del inventario debidamente actualizado, analizara los procedimientos para la adquisición de los productos seguidos en los diversos departamentos de la organización y determinara la existencia de equipos y aplicaciones similares. En caso de que los diversos departamentos de la compañía realicen pedidos sobre equipos y complementos de manera independiente, estudiara si se está desaprovechando la posibilidad de negociar descuentos mediante la aplicación de una política centralizada de compras. Del mismo modo, considerara otros mecanismos que pudieran reducir los costes de la organización como podría ser la negociación centralizada de compra de licencias de aplicaciones.

Determinar y evaluar la política de mantenimiento definida en la organización.

Los procedimientos descentralizados han propiciado que, en ocasiones, los equipos adquiridos no sean incluidos ni en el inventario ni en los contratos de mantenimiento. Incluso podría llegar a suceder que el personal de la organización encargado del mantenimiento no dispusiera de los conocimientos necesarios para llevarlo a cabo.

El equipo auditor examinara la utilización de las garantías de los productos adquiridos, comprobando que no se realizan pagos innecesarios por asistencias de equipos y aplicaciones que se encuentren en garantía.

Por lo que respecta a productos cuya garantía haya caducado, determinara cuales disponen de contratos de mantenimientos vigentes con empresas externas y cuales son aquellos en los que la responsabilidad del mantenimiento recae en la propia organización. En las contrataciones de mantenimiento con empresas externas, verificara si se han incluido en el contrato aspectos como el tiempo máximo de respuesta, recambios y mano de obra. También comprobara que el personal, tanto interno como externo, asignado a en tareas de mantenimiento tiene suficientes conocimientos de las plataformas que debe mantener, y que recibe la formación adecuada sobre los nuevos productos instalados en la organización.

En relación con la gestión de incidencias producidas, el equipo auditor comprobara la existencia de un registro de las mismas, los procedimientos establecidos para asignar recursos para solucionarlas, los guiones preparados para solventas las incidencias más frecuentes y el seguimientos de las mismas hasta su resolución. También valorara si el tiempo empleado para atender las solicitudes y resolver las incidencias producidas puede llegar a afectar al funcionamiento de la organización.

Evaluar la calidad de las aplicaciones del entorno ofimático desarrollada por personal de la propia organización.

El uso de herramientas ofimáticas ha propiciado el desarrollo de aplicaciones, en muchos casos sin las debidas garantías de fiabilidad, cuyo mal funcionamiento puede repercutir en la actividad de la organización. Por otra parte, es común que no hayan seguido los controles de calidad y seguridad.

El equipo auditor determinara la existencia de un departamento responsable de controlar el desarrollo de aplicaciones de toda la organización, o bien si los departamentos han desarrollado aplicaciones de uso interno, sin control de un departamento responsable. En el caso de desarrollos realizados por personal de los propios departamentos, el equipo auditor tendrá que determinar si la metodología empleada y los test de pruebas se ajustan a lo dispuesto en la organización.

Comprobara que las aplicaciones puedan configurarse para obtener las suficientes pistas de auditoria que permita efectuar un seguimiento de las anomalías producidas durante su ejecución, Asimismo, verificara que los desarrollos se realizan sobre un entorno de desarrollo, evitando operar directamente sobre los datos reales de explotación.

También deben examinar el reporte de incidencias de las aplicaciones, así como las reclamaciones manifestadas por los clientes y usuarios.

Evaluar la corrección del procedimiento existente para la realización de cambios de versiones y aplicaciones.

Los cambios de aplicaciones o de versiones pueden producir situaciones de falta de integración y de incompatibilidad entre los nuevos productos instalados y los existentes con anterioridad.

El equipo auditor determinara la existencia de procedimientos formalmente establecidos para la autorización, aprobación, adquisición de nuevas aplicaciones y cambios de versiones. Comprobara que las aplicaciones instaladas y los cambios de versiones han seguido todos los trámites exigidos en el procedimiento establecido.

También determinara si se han analizado los problemas de integración y las incompatibilidades que pueden plantear los nuevos productos, si se ha establecido algún plan para la formación de los usuarios finales que vayan a utilizar estos nuevos productos; y si los encargados de mantenerlos han adquirido los conocimientos suficientes para que los cambios no impacten negativamente en la organización.

Determinar si los usuarios cuentan con suficiente formación y la documentación de apoyo necesaria para desarrollar sus tareas de un modo eficaz y eficiente.

Un conocimiento deficiente por parte de los usuarios finales o encargados de mantenimiento, puede ocasionar pérdida de eficacia y eficiencia en la utilización de las mismas.

El equipo auditor determinara la existencia de un plan de formación para garantizar que todo el personal conoce los productos que tiene que utilizar. También comprobara que tras la realización de los cursos, se aplica algún mecanismo para determinar el aprovechamiento conseguido por los alumnos, y si se entrega a los usuarios documentación básica de la operativa de los productos, o si pueden acceder a ella fácilmente en caso de necesidad

Determinar si el sistema existente se ajusta a las necesidades reales de la organización.

La existencia de equipos obsoletos o infrautilizados puede ocasionar situaciones que, por mala distribución de los equipos a las necesidades de la organización, repercutan en el correcto funcionamiento de la misma.

El equipo auditor valorara el uso que se realiza con los equipos existentes, elaborando una relación de aquellos computadores que no se encuentren operativos. Revisará las actividades que se ejecutan en cada equipo, determinando aquellos puestos de trabajo que, por las tareas que desempeñan, necesitan ser automatizados o precisan actualizar los equipos existentes, así como aquellos puestos que, debido a su escasa actividad, se encuentran sobredimensionados.

Sobre los resultados obtenidos, elaborara una relación con recomendaciones sobre descatalogación de productos obsoletos, redistribuciones y adquisiciones de nuevos equipos y aplicaciones.

Seguridad

Determinar si existen garantías suficientes para proteger los accesos no autorizados a la información reservada de la empresa y la integridad de la misma.

Las aplicaciones de ofimáticas gestionan información reservada. Los accesos no autorizados o las inconsistencias en este tipo de información pueden comprometer el buen funcionamiento de la organización.

El equipo auditor examinara la documentación en materia de seguridad existente y comprobara que han sido definidos, al menos, procedimientos de clasificación de la información, control de acceso, identificación y autenticación, gestión de soportes, gestión de incidencias y controles de auditorías. Con posterioridad, pasara a comprobar si las medidas de seguridad definidas se encuentran realmente operativas.

Determinará si el procedimiento de clasificación de la información establecido ha sido elaborado atendiendo a la sensibilidad e importancia de la misma.

Comprobara que se han adoptado las medidas necesarias para que todo el personal conozca tanto aquellas que afecten al desempeño de su actividad como las responsabilidades en que pudiera incurrir en caso de incumplirlas.

Comprobara que cada usuario tiene autorización para acceder únicamente a aquellos datos y recursos informáticos que precisa para el desarrollo de sus funciones.

El equipo auditor deberá comprobar si se han establecido procedimientos de identificación y autenticación para el acceso al sistema. También, determinara si los usuarios desconectan sus puestos de trabajo al finalizar la jornada, o si existe un mecanismo de desconexión automática.

Comprobara que todos los soportes informáticos permiten identificar la información que contienen son inventariaros y se almacenan en un lugar de acceso restringido. Verificara que la salida de soportes informáticos fuera de la organización es debidamente autorizada.

Determinar si el procedimiento de generación de las copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad.

La información generada por el sistema debe estar disponible en todo momento. La no disponibilidad de datos, especialmente de aquellos procedimientos críticos para la organización, además de pérdidas económicas, podría llevar a la paralización del departamento.

El equipo auditor examinara el procedimiento de copias de seguridad, verificando la periodicidad, la correcta asignación de responsabilidades y el adecuado almacenamiento de los soportes.

Comprobara que la responsabilidad de realizar las copias de seguridad está asignada y que cada responsable realiza copias de la información que se encuentra bajo su responsabilidad. Verificara la existencia de un inventario de los soportes que contienen las copias de seguridad y de la información salvaguardada.

Posteriormente, determinara si la seguridad implementada para garantizar la confidencialidad e integridad de las copias de salvaguarda ofrece garantías equivalentes a las definidas para la información que contienen.

Finalmente, controlara la eficacia del procedimiento definido para la recuperación de las copias de seguridad, de forma que el resultado final sea un fiel reflejo de la situación anterior.

Determinar si está garantizado el funcionamiento ininterrumpido de aquellas aplicaciones cuya caída podría suponer perdidas de integridad de la información y aplicaciones.

En las organizaciones se desarrollan procesos en los que una caída de tensión podría ocasionar perdidas de integridad de la información y aplicaciones manejadas en ocasiones irrecuperables.

El equipo auditor determinara la existencia de sistemas de alimentación ininterrumpida, y si estos cubren el funcionamiento de aquellos equipos en los que se ejecutan procesos cuya interrupción podría ocasionar graves repercusiones. Verificar ante una caída de tensión, si los equipos entran en funcionamiento y si el tiempo que proporcionan es suficiente para la finalización de procesos críticos y desconexión del sistema.

Determinar el grado de exposición ante la posibilidad de intrusión de virus.

Los costos de la intrusión de virus: perdida de la información y empleo de recursos y tiempo para restablecer el sistema, llegando en algunos casos a la paralización temporal del departamento.

El equipo auditor analizara la protección establecida en cada uno de los puntos del sistema por los que podrían introducirse virus: módems, accesos a redes, etc. y revisara la normativa para la instalación y actualización de antivirus.

Analizara la configuración de los equipos y la instalación de programas que permitan detectar la existencia de virus, en caso de ser detectado algún virus, se adoptaran medidas para evitar que el virus se propague.

El equipo auditor deberá comprobar la adecuación y validez de los procedimientos establecidos para garantizar el cumplimiento de las leyes vigentes.

Determinar si en el entorno ofimático se producen situaciones que puedan suponer infracciones a lo dispuesto sobre la propiedad intelectual.

El hecho de usar copias ilegales, puede provocar que aquellos afectados sufran algún tipo de daño o perjuicio y presenten reclamaciones ante los Tribunales de Justicia.

El equipo auditor deberá elaborar una relación exhaustiva de las aplicaciones residentes en equipos ofimáticos, que precisen licencia para su utilización. Se contrastara con el inventario para verificar que coinciden, y, en caso contrario, deberá averiguar cuáles son las copias ilegalmente utilizadas.

Se ocupara de verificar la definición y aplicación de medidas con carácter preventivo, tales como: la existencia de un régimen disciplinario que sea conocido por todos los empleados.

Comprobara la definición de medidas correctivas tales como: la eliminación de las copias ilegales, definir medidas para que no se repita de nuevo, y adoptar las acciones disciplinarias pertinentes.