tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

043

AUDITORÍA INFORMÁTICA EN LA ADMINISTRACIÓN: UN RETO PARA LOS PROFESIONALES TIC

Fernando Rodríguez Rivadulla
Colaborador de Auditoría - CISA
Agencia Estatal de Administración Tributaria

Fernando Rodríguez Rivadulla

Palabras clave

Auditoría informática
Auditoría de sistemas de información
Calidad de los servicios públicos
Construcción de confianza en los servicios públicos
Control interno

Resumen de su Comunicación

Las organizaciones exitosas son aquellas que, entre otras cosas, reconocen los beneficios que las TIC les proporcionan para cumplir sus objetivos. Además, comprenden la necesidad de administrar los riesgos del empleo de las TIC, ya que la información es uno de sus activos más importantes.

La función de la Auditoría Informática en dichas organizaciones, comienza con la implantación de un proceso para supervisar el control de las tecnologías y de los procesos asociados, y evoluciona hacia un enfoque proactivo participando en otras fases del ciclo de control.

Los profesionales TIC, auditores informáticos, pasan por ser los recursos cualificados para contribuir a la construcción de la confianza en la Administración Electrónica, configurándose como los garantes de la prestación de servicios de calidad, y en la consecución de las políticas públicas relacionadas.

Fernando Rodríguez Rivadulla

AUDITORÍA INFORMÁTICA EN LA ADMINISTRACIÓN: UN RETO PARA LOS PROFESIONALES TIC

1. Introducción

Las distintas áreas operativas de las organizaciones se sostienen y apoyan cada vez más en los servicios de las tecnologías de la información y las comunicaciones (TIC), que han acompañado la automatización y el crecimiento de todos los procesos productivos, y la prestación de nuevos servicios.

Como consecuencia, son muchas las organizaciones en las que la información y la tecnología que la soporta representan los activos más valiosos, y a su vez, reconocen los beneficios potenciales que las nuevas tecnologías les pueden proporcionar. La productividad de cualquier organización depende del funcionamiento ininterrumpido de los sistemas TIC, transformando a todo el entorno como un proceso crítico adicional.

Por tanto, se requiere contar con una efectiva administración de los riesgos asociados con las TIC, y que viene dada por:

- La necesidad de dar respuestas adecuadas a los problemas planteados por la creciente dependencia de la información y de los sistemas que la proporcionan.

- El incremento de la vulnerabilidad de los sistemas, por el amplio espectro de amenazas a las que están expuestos.

- La importancia y magnitud de los costes y las inversiones TIC.

- La desconfianza que los procedimientos automatizados o los servicios electrónicos pudieran provocar en el colectivo usuario y en los ciudadanos en general.

- El potencial de las nuevas tecnologías de la información es tal que pueden llegar a introducir importantes cambios en la organización, y en las prácticas de su actividad, para crear nuevas oportunidades y reducir costes.

Resulta de ello el rol básico que debe desempeñar la función de Auditoría Informática, o Auditoría de los Sistemas de Información, en una organización: supervisión de los controles efectivamente implementados y determinación de la eficiencia de los mismos.

Dada la especialización de los controles a supervisar, es indudable que en la Administración Pública el perfil de los profesionales TIC es el idóneo para asumir y realizar directamente esas funciones, ayudando a las organizaciones a fortalecer la confianza en los servicios prestados, en especial los enmarcados dentro de la Administración Electrónica.

Es así que los profesionales TIC de la Administración tienen ante si un reto en su carrera profesional: realizar tareas propias de la función de auditoría, para contribuir a la mejora de la calidad de los servicios prestados a los ciudadanos.

2. Factores Críticos de Éxito

A continuación, se relacionarán los factores críticos a tener en cuenta para poder desplegar con éxito la función de Auditoría Informática en una organización.

2.1. Participación de la Dirección

Las organizaciones exitosas, además de lo antes señalado, comprenden y gestionan los riesgos asociados con la implementación de las nuevas tecnologías. Para ello, la dirección de una organización necesita poder apreciar y poseer un conocimiento básico de los riesgos y los límites de las TIC para proveer una dirección eficaz y los controles adecuados. También debe pronunciarse sobre cual es la inversión razonable en seguridad y control, y sobre cómo balancear el riesgo y el control de las inversiones.

En el caso concreto de la Administración Pública que presta servicios electrónicos a los ciudadanos, se requiere el establecimiento de medidas tanto técnicas como organizativas que aseguren el mantenimiento de las garantías en los procedimientos y que fortalezcan la confianza de los usuarios y de los administrados.

En definitiva, es imprescindible que los órganos de dirección de la Administración entiendan la implicación de una gestión de riesgos en general, y los relacionados con las TIC en particular, y aseguren el establecimiento de un sistema de control apropiado para la organización que dirigen. Es un requisito previo para poder realizar cualquier tipo de auditoría que la organización tenga definida, documentada, conocida por todo el personal y aplicada, una política de control.

2.2. Estructura Organizativa

En esta comunicación no se abordará la problemática relativa al reconocimiento de la función TIC como una unidad estratégica dentro de las organizaciones de la Administración, que salvo en contados casos, a diferencia del sector privado, no se ve reconocida orgánicamente como tal. No obstante, se señala como un condicionante para el despliegue de la función de Auditoría Informática, ya que si la operativa TIC no interviene en la definición de la estrategia de la Administración Electrónica, difícilmente la Auditoría Informática pueda desplegarse eficientemente en la supervisión del control.

Al conformar la estructura organizativa de la unidad que asuma la función de la Auditoría Informática deben asegurarse unos requisitos básicos para poder cumplir con éxito sus propósitos. Por un lado, la independencia del órgano que tenga asignadas las funciones operativas TIC, dado que la participación en tareas ejecutivas comprometería su función durante las auditorías. Por otro lado, el reconocimiento de la autoridad de los auditores, los que deberán disponer de acceso no restringido a la información requerida para el ejercicio de sus funciones auditoras, manteniendo la discreción y la confidencialidad de los asuntos tratados.

También es fundamental que los auditados, en nuestro caso los profesionales de los centros TIC, además de su deber de colaboración, vean en la Auditoría Informática una herramienta más de control que emplea una organización que asume y gestiona sus riesgos.

De lo anterior, se ve la necesidad de encuadrar la función Auditoría Informática dentro de una unidad con suficiente rango dentro de la organización, que no dependiera de las áreas operativas que fuera a auditar, y dotada del personal con autoridad y nivel técnico adecuado.

2.3. Marco Metodológico

El incremento masivo en el uso de medios informáticos, ya sea de ordenadores en los puestos de trabajo como en las aplicaciones de tecnología cada vez más sofisticada, y en la prestación de servicios a los ciudadanos mediante la Administración Electrónica, han llevado a la necesidad de adaptar las técnicas de auditoría tradicionales para poder hacer frente a esos cambios.

Una vez planteadas y reconocidas las nuevas exigencias de control, surge la necesidad de contar con un marco metodológico para organizar las actividades de Auditoría Informática, y así definir las pautas y los controles a considerar en las futuras actuaciones de auditoría. Esto se sustenta en el hecho que el uso de una metodología contrastada contribuye a:

- Salvar las brechas existentes entre riesgos del proceso de gestión, necesidades de control y aspectos técnicos. Esto es debido a que los riesgos de un proceso de gestión no son los mismos que los riesgos a que se expone el sistema de información que le da apoyo. La Auditoría Informática debe intentar asegurar que ambos están controlados, o sea, ajustados a las necesidades de control, o a lo que se asuma controlar, y a los medios y recursos técnicos disponibles.

- Determinar el alcance de la tarea de auditoría e identificar los controles mínimos, que debe estar dirigida no sólo a auditores informáticos, sino también a los gestores y a los usuarios.

- Observar e incorporar los estándares y regulaciones nacionales o internacionales.

Al contar con una metodología se podrán tener predefinidos los procedimientos de actuación, que aunque sólo lleguen a definir el qué y el cómo hacer las actuaciones, permitirán generar resultados homogéneos por los distintos miembros del equipo auditor. Asimismo, el marco metodológico adoptado tendrá que definir las pautas y los controles a realizar con relación a los sistemas de información, tecnologías de hardware, seguridad, planificación, desarrollo de sistemas, etc.

Las metodologías e instrumentos de normalización que pueden ser considerados por el auditor informático como referentes, y que debe conocer, y en su caso aplicar, son:

Instrumentos de normalización de las Administraciones Públicas

- Normas de Auditoría del Sector Público de la IGAE, aunque no son específicas de la Auditoría Informática, establecen un marco organizativo (www.igae.minhac.es).

- Serie del Centro Criptográfico Nacional sobre la Seguridad de las Tecnologías de la Información (CNN-STIC), que incluye políticas, procedimientos, normas, instrucciones técnicas y guías de implantación(www.oc.ccn.cni.es).

- Information Technology Infrastructure Library (ITIL) desarrollada por Office of Government Commerce del H.M.Teasury de UK Government, constituye una guía de las mejores prácticas para la gestión de servicios de tecnologías de la información (www.ogc.gov.uk).

- Serie de publicaciones especiales SP-800 del Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU. (http://ers.nist.gov).

Prácticas y recomendaciones del ámbito de asociaciones internacionales

- Control Objectives for Information and Related Technologies (COBIT) de la Asociación de Auditoría y Control de Sistemas de Información (ISACA), establecen un marco para la Auditoría Informática (www.cobit.com).

- IS Standards, Guidelines and Procedures for Auditing and Control Professionals de ISACA (www.isaca.com).

- Common Criteria for Information Technology Evaluation Version 2.3 de CSE (Canadá), SCI (Francia), BSI (Alemania), NLNCSA (Holanda), GESG (Reino Unido), NIST (EE.UU.) y NSA (EE.UU.).

Normalización internacional

- Código de buenas prácticas para la gestión de la seguridad de la información, actual ISO/IEC 17799:2005, y futura ISO/IEC 27002 Controles de seguridad prevista para 2007.

- Especificaciones para los sistemas de gestión de la seguridad de la información ISO/IEC 27001:2005.

- Criterios comunes de evaluación de la seguridad de las tecnologías de la información ISO/IEC 15408.

Procedimiento administrativo

- Real Decreto 263/1996 que regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado BOE 29/02/1996.

- Legislación sobre registros telemáticos: Real Decreto 72/1999 que regula la presentación de solicitudes, escritos y comunicaciones ante la AGE, la expedición de copias de documentos y devolución de originales y el régimen de registros, BOE 22/05/1999; Real Decreto 209/2003 que regula los registros y notificaciones telemáticas, utilización de medios telemáticos para la sustitución de certificados, BOE 28/02/2003, y la Orden PRE/1551/2003 que desarrolla su disposición final primera, BOE 13/06/2003.

- Resolución de la Secretaría de Estado de Administración Pública de 26 de mayo de 2003 que dispone la publicación del acuerdo del Pleno de la Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos que aprobó los criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la AGE en el ejercicio de sus potestades (www.csi.map.es/csi/pg5c10.htm).

- MAGERIT versión 2, Metodología de análisis y gestión de riesgos de los sistemas de información (http://www.csi.map.es/csi/pg5m20.htm).

Protección de datos de carácter personal

- Ley Orgánica 15/1999 de protección datos de carácter personal, BOE 14/12/1999.

- Reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de carácter personal, BOE 25/06/1999 (se espera su actualización en 2006).

2.4. Proceso de Auditoría

Las actuaciones de Auditoría Informática requieren una planificación en tres niveles. En el primero se define qué se debe auditar, apoyándose en un análisis de riesgos de la organización, en requerimientos legales o en prioridades de la dirección para la consecución de sus metas. En el segundo nivel se decide cuándo auditar, priorizando las actuaciones a realizar, y ajustando el alcance de las mismas a los recursos disponibles. Esta planificación se suele reflejar en un documento de planificación periódica de la unidad de auditoría. Por último, en el tercer nivel se estipula el detalle de cómo realizar las actuaciones previstas en ese plan, que se desarrollarán en actuaciones concretas.

Esta planificación debe seguir un proceso estructurado en las siguientes fases:

Planificación de las Actuaciones de Auditoría

El equipo de auditoría designado deberá definir los trabajos a realizar para poder cumplir los objetivos perseguidos con la actuación, obteniendo toda la información preliminar sobre la actividad llevada a cabo por el área sujeta a la auditoría. Si el área ha sido auditada con anterioridad, debe revisarse la documentación previa e identificar todos los cambios realizados desde entonces.

Con la información previa se podrán definir los objetivos detallados de la actuación, el calendario tentativo, identificar los interlocutores, establecer el tipo de información a solicitar, y las verificaciones o pruebas de campo a efectuar durante la actuación.

Formalización del Inicio de la Actuación

Se realiza mediante una notificación del responsable de la unidad de auditoría dirigida al responsable de la unidad auditada, en la que se identifica al equipo auditor y el objeto de la acción a llevar a cabo, aunque pueden darse circunstancias que lleven a que no se envíe notificación previa.

Los trabajos comenzarán con una reunión entre el equipo auditor con el máximo responsable de la unidad auditada, para dejar establecido el alcance y la planificación de los trabajos. Durante la entrevista se describirá la información a recopilar durante la actuación, las pruebas y verificaciones a realizar.

El trabajo de los auditores debe minimizar las interferencias con la operativa del área auditada, evitando realizar la actuación durante períodos de trabajo estacional. Los auditados deben tener presente su deber de colaboración con el equipo auditor.

Trabajos de Campo

Se recopilará información sobre el proceso objeto de la actuación con el fin de obtener evidencias e identificar hallazgos que reflejarán las conclusiones de la actuación, aplicando alguna o varias técnicas de auditoría:

- Revisión de documentos: Permitirá que el equipo auditor adquiera el entendimiento del entorno a auditar. Los documentos a estudiar serán aquellos que especifiquen la estructura organizativa, las políticas, normas y estándares y la documentación general de los sistemas o procesos a auditar.

- Entrevistas: Tienen como finalidad la obtención de información y determinar el grado de conocimiento que tienen los entrevistados sobre el sistema de control aplicado. Deben organizarse con antelación suficiente, siguiendo un patrón, y documentarse preferentemente con notas escritas. Como material de apoyo pueden emplearse listas de verificación o cuestionarios.

- Pruebas y verificaciones de campo: El propósito será determinar si los controles internos se encuentran operativos y funcionando según lo previsto. Para concluir que ello ocurre y se lleva a cabo, deben obtenerse evidencias de una muestra significativa que permita cuantificar el nivel de cumplimiento. Los tipos de pruebas dependerán de la naturaleza de la auditoría.

- Observación del trabajo realizado: Permite identificar la falta de formación, mejoras para aumentar la productividad, simplificación de procesos, entendimiento de lo que realizan, carencias o vicios adquiridos, etc. En ningún momento el equipo auditor debe obstruir el trabajo realizado, y debe documentar lo que considere relevante con los medios adecuados (notas, fotografías, etc.).

- Uso de herramientas: Los entornos informáticos plantean un desafío al auditor TIC para obtener evidencias, ya que generalmente están en medios y soportes electrónicos. Las herramientas recolectan esa información, y dada su diversidad, en muchos casos sería imposible la recolección y el análisis posterior. Además, facilitan la generación de muestras, se emplean para interrogar los sistemas de información, para extraer información, y para ordenarla según criterios, asegurando objetividad en el proceso de recolección de los datos.

Evaluación de la información

En esta fase se valorará el cumplimiento de las normas, de los procedimientos o de los estándares reconocidos, y se determinará si los sistemas tienen una estructura de control adecuada, efectiva en términos económicos, que provea una adecuada seguridad que las tareas se realizan según lo previsto, y que el objetivo de control se cumple. También se podrán identificar los procesos de control para compensar las desviaciones sobre lo previsto, para así obtener una estructura de control completa. Todo el análisis debe estar justificado con evidencias recogidas en la actuación.

Comunicación de los resultados

Al final del proceso de la auditoría se mantendrá una reunión de cierre con el máximo responsable de la unidad auditada, para informarle de los principales hallazgos de la actuación. El auditado tiene la oportunidad de influir en las recomendaciones que incluirá el informe final, dado que es imprescindible contar con su opinión para asegurar que los resultados y las recomendaciones sean razonables y posibles de llevarse a cabo.

A continuación, se redacta el borrador del informe, que incluirá todos los hechos, hallazgos, conclusiones y recomendaciones. En la redacción del documento se empelará un lenguaje claro, exento de tecnicismos, y el detalle técnico de las pruebas y evidencias se acompañará en anexos. El borrador se remitirá a la dirección del área auditada, para que remita los comentarios por escrito que estime convenientes.

Después de revisar y en su caso tomar en consideración las observaciones remitidas sobre el borrador, se elaborará el informe final de la auditoría. Si el equipo de auditoría no coincidiese con alguno de los comentarios realizados sobre el borrador, deberán ser explicadas las razones e incluidas en el informe final.

Las recomendaciones del informe podrán dar lugar a instrucciones dirigidas a la dirección de la unidad auditada, sugiriendo acciones para resolver las incidencias señaladas.

Seguimiento

Las recomendaciones incluidas en las instrucciones tendrán que ser llevadas a cabo en un período de tiempo determinado después de la recepción del informe. El trabajo de auditoría no se podrá dar por finalizado hasta que no se compruebe la ejecución de las recomendaciones, lo que dará lugar a un informe de cumplimento. La oportunidad para realizar un seguimiento dependerá de la gravedad de los hallazgos, y estará sujeta al criterio del auditor o de su dirección.

2.5. Auditores Informáticos

Los profesionales que por su formación y capacitación profesional deben asumir la función de Auditoría Informática son sin lugar a duda los profesionales TIC. En el ámbito del sector privado existen organizaciones profesionales que habilitan a un profesional como auditor informático mediante la certificación profesional que gestionan. El modelo de currículo que dichas organizaciones definen, y que un profesional debería

acreditar para ser reconocido como un auditor informático, se basa en áreas de conocimiento, las que suelen ser:

- Técnica o metodología de Auditoría Informática.

- Gestión, planificación y organización de las tecnologías de la información.

- Infraestructura técnica, prácticas operativas y protección de activos informáticos.

- Recuperación de desastres y continuidad de la actividad soportada por los sistemas de información.

- Desarrollo, adquisición, implantación y mantenimiento de sistemas de información.

- Evaluación de procesos de negocio y gestión de riesgos.

La certificación se obtiene después de aprobar un examen sobre esas materias, acreditar una experiencia profesional adecuada en el campo de las TIC y aceptar un código de ética profesional; y se mantiene acreditando una formación continua en la materia.

En la AGE ya se están dando los pasos hacia la preparación de profesionales como auditores TIC, ya que los planes de formación del INAP incluyen cursos específicos sobre técnicas de auditoría y sobre técnicas de control de sistemas informáticos. Se cubriría así que el auditor informático, como un técnico o especialista informático más, recibiese una formación constante para actualizar sus conocimientos, capacidades y habilidades.

No obstante, caben señalar otras áreas no relacionadas con las TIC o la auditoría, que son igualmente fundamentales para cubrir el perfil del profesional del auditor informático, tales como la capacidad para poder:

- Comprender los procesos de gestión de los servicios públicos y la normativa legal en que se apoyan los sistemas de información.

- Evaluar programas y políticas públicas.

- Revisar y evaluar riesgos de áreas gestionadas por las TIC.

- Identificar o diagnosticar problemas y plantear soluciones.

- Llenar el vacío de comunicación entre usuarios y técnicos.

- Saber comunicar los temas claves a la dirección.

- Saber negociar y resolver situaciones de conflicto.

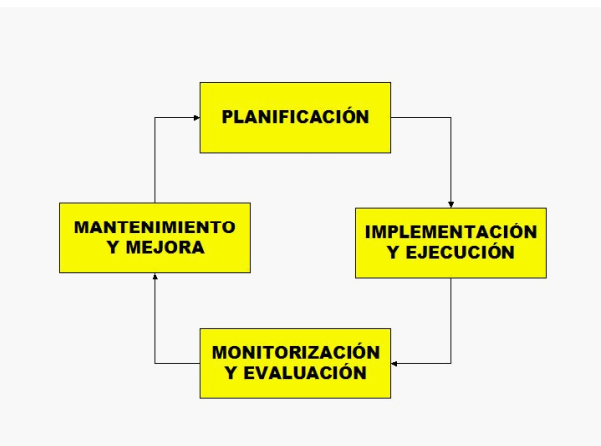
- Saber cuando solicitar asistencia de profesionales especializados.

Finalmente señalar que los trabajos de auditoría más exitosos serán aquellos en los cuales el equipo auditor y los auditados se consideren asimismo como consultores y clientes respectivamente. El entendimiento y aplicación de este concepto tiende a establecer una relación de trabajo más constructiva, y puede resultar en la mejora de la operativa de la unidad bajo revisión.

3. Actuaciones de Auditoría Informática

Teniendo presente que el principal objetivo de la función de Auditoría Informática debe ser asistir a los miembros de la organización en el efectivo desempeño de sus responsabilidades, de forma que se garantice la construcción de la confianza hacia la Administración Electrónica, los auditores informáticos deben proveer análisis, apreciaciones, recomendaciones, consejos e información concernientes a las actividades revisadas.

Sobre este particular, debe tenerse presente el ciclo de gestión de control, en el cual la función de auditoría tendría la misión de analizar la implementación de los controles y corregir la gestión proponiendo, en su caso, mejoras, y que se resume en el siguiente esquema:



La función de Auditoría Informática que se establezca dentro de una organización para examinar y evaluar sus actividades debe ser considerada como una apreciación independiente al servicio de la misma para supervisar el control establecido. Es un requisito previo para poder realizar Auditorías Informáticas que la organización tenga definida, documentada, conocida por todo el personal y aplicada, una política de control.

3.1. Supervisión del Control

El marco metodológico adoptado como instrumento para realizar las Auditorías Informáticas contemplará una serie de puntos de control de riesgos que podrán ser identificados como aquellos a tener en cuenta en la actuación y que serán objeto de verificación en función del alcance de la misma.

Las Auditorías Informáticas suelen dirigirse al análisis de situaciones de riesgos informáticos en áreas de actividades concretas. La naturaleza de las auditorías siempre dependerá del análisis de riesgos que se haya realizado en la organización, de los requerimientos legales a cumplir o de las prioridades de control establecidas por la dirección de la organización.

A modo de ejemplo, se enumeran algunos tipos de Auditorías Informáticas:

- Auditoría de la Dirección de las Tecnologías de la Información.

- Auditoría de la Seguridad: sistema de gestión de la seguridad, seguridad física o seguridad lógica, seguridad en las redes de comunicaciones.

- Auditoría del Equipamiento Informático: planificación infraestructuras, puestos de trabajo, redes de área local, mantenimiento del parque e inventario.

- Auditoría de los Desarrollos y Mantenimiento de los Sistemas de Información.

- Auditoría de Calidad de los Productos Desarrollados.

- Auditoría de la Explotación de los Sistemas de Información.

- Auditoría de la Contratación de Bienes y Servicios de Tecnologías de la Información.

- Auditoría de Control de Accesos a los sistemas de información.

- Auditoría de Técnica de Sistemas: sistemas operativos, bases de datos, etc.

- Auditoría de la Gestión de la Continuidad del Servicio Informático.

- Acreditación de Servicios de Confianza.

- Auditorías de Cumplimiento de Requerimientos Legales: protección de datos, aprobación de programas que ejercen potestades, registros telemáticos, etc.

3.2. Participación Proactiva

El enfoque tradicional de la función de la auditoría ha ido evolucionando, se ha vuelto más participativa, dando prioridad a un enfoque preventivo e intentando actuar antes o durante el hecho. La tendencia actual, en el ámbito de la Auditoría Informática apunta a participar más activamente en todos los proyectos y decisiones, y en todos los aspectos de la tecnología relacionada, para asegurar que los activos de la organización están siendo protegidos y que se establezcan los controles internos adecuados para proteger los recursos informáticos.

Además de la supervisión del control, sería deseable que la función de Auditoría Informática tuviera alguna participación en otras fases del ciclo de control, como en la planificación y en la implantación de los controles, pero siempre asegurando el principio de independencia, ya que no es éticamente aceptable auditar los controles que haya definido.

Así, se podría configurar una participación de la función de Auditoría Informática apoyando puntualmente a la unidad de la organización con competencias TIC en la planificación y el desarrollo o en el mantenimiento de los sistemas de información de la organización, así como en la definición de los procedimientos a que dan soporte, por ejemplo, en las siguientes tareas:

- Asegurando la existencia de controles internos razonables y adecuados.

- Divulgando y fomentando el uso de buenas prácticas del sector.

- Verificando la completa y apropiada documentación de los sistemas y procedimientos.

- Asesorando sobre la implementación de pistas de auditoría adecuadas, es decir que las aplicaciones registren información específica para una futura auditoría del proceso al que sirven, y que la información registrada guarde relación con los riesgos relacionados con el proceso.

- Señalando una adecuada salvaguarda de los activos de la organización y el seguimiento de procedimientos adecuados.

- Asegurando la eficiencia de la gestión de los recursos, evitando recurrir a sistemas onerosos o a posteriores cambios de procedimientos.

Conviene señalar que la Auditoría Informática no debe perseguir como fin único la identificación de deficiencias, errores, actos ilegales, fraudes, etc., sino que también tendrá que poner de manifiesto las mejoras más sustanciales alcanzadas o las buenas prácticas seguidas por la unidad auditada.

4. Conclusiones

Las organizaciones exitosas son aquellas que, entre otras cosas, reconocen los beneficios que las TIC les proporcionan para cumplir sus objetivos. Además, comprenden la necesidad de administrar los riesgos del empleo de las TIC, ya que la información es uno de sus activos más importantes.

La función de la Auditoría Informática en dichas organizaciones, comienza con la implantación de un proceso para supervisar el control de las tecnologías y de los procesos asociados, y evoluciona hacia un enfoque proactivo participando en todas las fases del ciclo de gestión del control.

Los profesionales TIC, auditores informáticos, pasan por ser los recursos cualificados para contribuir a la construcción de la confianza en la Administración Electrónica, configurándose como los garantes de la prestación de servicios de calidad, y en la consecución de las políticas públicas relacionadas.

Las organizaciones públicas deben tomar conciencia de ello y potenciar los factores señalados para el despliegue de la función de Auditoría Informática.