AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Cobertura del Riesgo Tecnológico: hacia una Auditoría Interna de TI Integrada

The Institute of Internal Auditors

Instituto de Auditores Internos de España

AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Cobertura del Riesgo Tecnológico: hacia una Auditoría Interna de TI Integrada

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN: **Marina Touriño Troitiño, CIA, CRMA, CISA.**
MARINA TOURIÑO & ASOCIADOS, S.L.

Anxo Cebro Barreiro, CISA. MAPFRE

Andrés de Benito Orbañanos, CIA, CISA. LOGISTA GROUP

Juan José Huerta Díaz, CIA, CISA. MUTUA MADRILEÑA

Ricardo Martínez Martínez, CISA. DELOITTE

Ramiro Mirones Gómez, CISA. EY

Marc Muntañá Vergés, CISA. MUTUA UNIVERSAL

José Manuel Vidal Formoso, CISA. BBVA

The Institute of Internal Auditors

Instituto de Auditores Internos de España

Presentamos un nuevo documento de LA FÁBRICA DE PENSAMIENTO realizado íntegramente por una Comisión Técnica constituida por socios expertos en el ámbito de la Auditoría Interna de TI (Tecnologías de la Información) con una dilatada trayectoria profesional.

Este documento se ha apoyado en una encuesta realizada por el Instituto de Auditores Internos de España y pone de manifiesto la importancia que ha adquirido la cobertura de los riesgos tecnológicos en las organizaciones y la necesidad de contar con expertos adecuadamente formados.

La función de Auditoría Interna de TI es clave en el apoyo a la organización, gobierno y control de los riesgos de TI.

Quiero agradecer una vez más a los miembros de esta Comisión la elaboración de este trabajo de enorme calidad que ayudará a entender la importancia de TI en el mundo del aseguramiento y, en concreto, de la Auditoría Interna.

José Manuel Muries

Presidente del Instituto de Auditores Internos de España

Índice

RESUMEN EJECUTIVO 06

OBJETIVOS DEL DOCUMENTO 07

SITUACIÓN ACTUAL DE LA COBERTURA DE RIESGOS TECNOLÓGICOS EN AUDITORÍA INTERNA EN ESPAÑA 07

LOS RIESGOS TECNOLÓGICOS EN EL NEGOCIO 10
Definición de riesgo tecnológico 10
Percepción del riesgo tecnológico 11
Categorías de riesgos tecnológicos 11
Universo de Auditoría Interna de TI 13

INTEGRACIÓN DE LA COBERTURA DE TI EN AUDITORÍA INTERNA 14
Objetivos de la integración de la Auditoría Interna de TI 14
Auditorías integradas vs. Auditorías puras de TI 15
Estrategias de integración de la Auditoría Interna de TI 17
Madurez en la integración de la Auditoría Interna de TI 17
Perfil del auditor interno de TI 19
Metodología de trabajo 20
Relación de Auditoría Interna de TI con el área de Tecnología 20

ENFOQUE DE LAS AUDITORÍAS INTERNAS DE TECNOLOGÍA DE LA INFORMACIÓN 21

HERRAMIENTAS DE SOPORTE A LAS AUDITORÍAS INTERNAS DE TECNOLOGÍA DE LA INFORMACIÓN 22

ANEXOS 26
Anexo 1. Glosario · Acrónimos 26
Anexo 2. Bibliografía 28

Resumen Ejecutivo

La dependencia respecto a la tecnología en la toma de decisiones hace imprescindible la valoración de los riesgos tecnológicos.

Las organizaciones dependen cada vez más de la Tecnología de la Información (TI[1], en adelante), pero no todas las organizaciones perciben ni actúan de igual forma ante la urgencia de los riesgos asociados al progreso tecnológico. Cada vez resulta más relevante poder confiar tanto en la información almacenada en los sistemas como sustento en una efectiva y adecuada toma de decisiones, como en el propio funcionamiento de los sistemas que dan soporte.

Las diferencias en la percepción del riesgo suelen deberse a la distinta penetración de la tecnología y al diferente impacto en los negocios, o bien a que no hay una clara conciencia sobre el impacto que estos riesgos provocan. Según una encuesta del Instituto de Auditores Internos de España, el 31% de las organizaciones no cuentan con un área / unidad de Auditoría Interna de TI específica dentro de la Dirección de Auditoría Interna; el 64% tienen sólo "uno" o "ningún" auditor interno de TI en su organización, y sólo el 15% tiene previsto incorporar "algún" auditor interno de TI en los próximos años.

La encuesta de Instituto de Auditores Internos de España identifica los diferentes enfoques de la Auditoría Interna de TI: desde su integración total en la Dirección de Auditoría Interna, hasta su total externalización, pasando por un sistema mixto. La encuesta también permite observar los diferentes grados de madurez de la función de Auditoría Interna de TI: desde su enfoque totalmente aislado, hasta las "auditorías integradas", que combinan los recursos de la auditoría del negocio con los propios de la Auditoría Interna de TI.

1. Esta acepción es usada en este documento también como equivalente a "sistemas de información". Ambas expresiones son utilizadas habitualmente como sinónimos en distintos documentos, normas, legislación, etc.

Objetivos del Documento

Este documento proporciona a la Dirección de Auditoría Interna unas directrices básicas sobre Auditoría Interna de TI, pero no pretende ser una guía exhaustiva de implementación de la función. Es de ámbito generalista, ya que se abordan temas como la gestión de las relaciones entre Auditoría Interna de TI y el área de TI, o las herramientas que habitualmente se utilizan en esta tipología de trabajos. Tampoco pretende sustituir a las guías y normas oficiales para la auditoría de la tecnología de la información que se incluyen al final del documento, en la bibliografía.

Los objetivos del documento incluyen:

- Una visión general del riesgo tecnológico.
- La exposición del impacto que este área de procesos de una organización tiene para la planificación y cobertura de Auditoría Interna.
- Las tendencias a nivel nacional de la cobertura de TI por los Departamentos de Auditoría Interna en organizaciones de distinta dimensión y modelos de negocio diferentes.
- Los aspectos más significativos que un Departamento de Auditoría Interna debería considerar en su cobertura y planificación, y relación con los "clientes" de TI.
- Los elementos diferenciadores y análogos de la cobertura de Auditoría Interna de TI con respecto al resto de las tareas del área.
- Un esquema para integrar la Auditoría Interna de TI dentro de Auditoría Interna, o para evaluar el planteamiento actual, si existe la función.

Este documento propone un esquema para integrar la Auditoría Interna de TI dentro de la Dirección de Auditoría Interna.

Situación actual de la cobertura de riesgos tecnológicos en Auditoría Interna en España

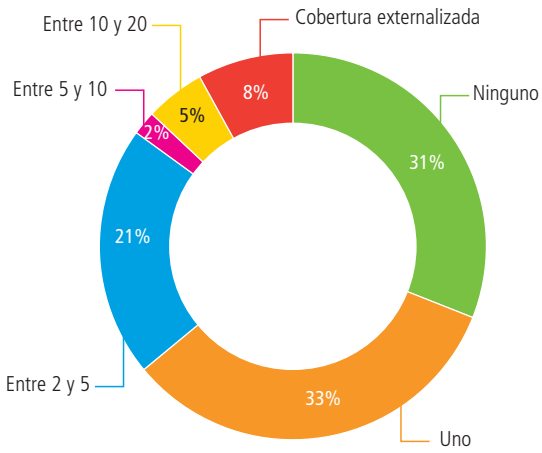
El Instituto de Auditores Internos de España evaluó en abril de 2013, a través de su encuesta, la madurez de la Auditoría Interna de TI en España. El 44% de las respuestas corresponden a entidades financieras o de seguros; el 41% a entidades con actividades relacionadas con bienes de consumo y distribución, fabricación, transporte y logística, sanidad, construcción, servicios y hostelería y turismo; y el 15% a otras actividades (tecnología, medios, energía y administraciones públicas).

Los resultados de la encuesta realizada permiten observar cambios en la función de la

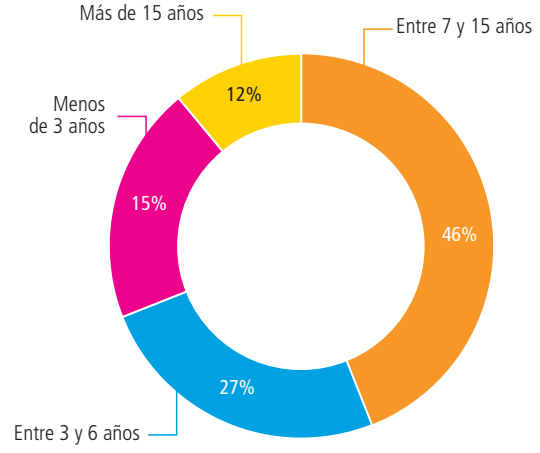
Auditoría Interna de TI. Se ha incrementado un 36% la participación de Auditoría Interna de TI en la definición, desarrollo, implantación y seguimiento de proyectos . En el 80% de los casos, el plan de Auditoría Interna de TI se basa en riesgos: a) en un 42% el análisis de riesgos es realizado de forma independiente por Auditoría Interna; b) en el 39% el análisis de riesgos es realizado por el negocio pero revisado por Auditoría Interna y; c) en el 19% restante el análisis de riesgos es realizado sólo por el negocio o por TI.

Se observa la necesidad de una mayor integración de la función de Auditoría Interna de TI en la realización de auditorías integradas (operativas, financieras, etc.). De las organizaciones que han respondido a la encuesta, un 66% realiza menos de un 25% de auditorías integradas.

NÚMERO DE AUDITORES INTERNOS DE TI EN PLANTILLA DENTRO DE LA FUNCIÓN DE AUDITORÍA INTERNA



GRADO DE EXPERIENCIA DE LOS AUDITORES INTERNOS DE TI EN LA FUNCIÓN DE AUDITORÍA INTERNA

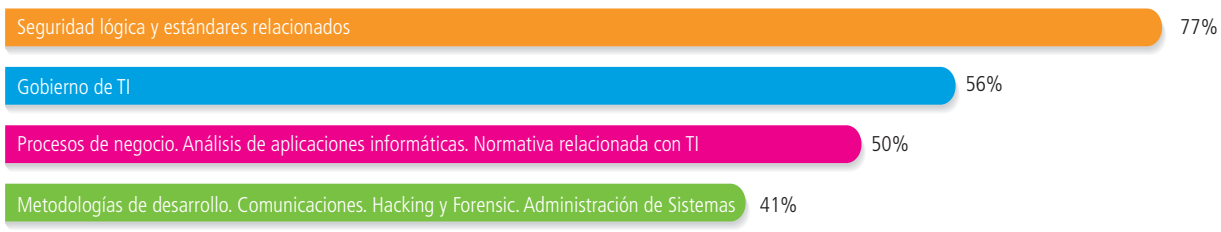


- **Niveles de cobertura y presencia** de Auditoría Interna de TI:
  - El 31% de las organizaciones no tiene función de Auditoría Interna de TI.
  - En el 33% de los casos sólo cuentan con 1 Auditor Interno de TI, y el 21% de las organizaciones cuenta con, al menos, entre 2 y 5 Auditores Internos de TI. Sólo el 5% tiene entre 10 y 20 Auditores Internos de TI. El 8% tiene totalmente subcontratada esta función.
  - Un 15% de las organizaciones tiene planes para incrementar el número de auditores internos de TI en el próximo ejercicio.
  - Un 56% no recurre a apoyo externo, mientras que un 44% muestra algún grado de externalización.
- **La externalización,** total o parcial, de las actividades de Auditoría Interna de TI, está motivada:
  - En el 33% de los casos por necesidades de un alto grado de especialización y actualización tecnológica.
  - En el 26% de los casos por la limitación de recursos.
- El **nivel medio de experiencia** actual de los auditores internos de TI: el 46% tienen entre 7 y 15 años de experiencia.

- La **experiencia práctica y conocimientos** de los auditores internos de TI se centran:
  - 84% en la Seguridad Lógica.
  - 79% en Continuidad de Negocio.
  - 74% desarrollo de Sistemas.
  - 63% ERPs.
  - 59% en Seguridad Física y Explotación de Sistemas.
  - 47% Comunicaciones, Externalización de TI, Normativa relacionada con TI.
- En cuanto a su **procedencia:**
  - El 45% proceden de la misma organización.
  - El 55% de otras compañías, principalmente de servicios profesionales de Auditoría o bien de Auditoría Interna de TI de otras organizaciones.
- En cuanto a las **certificaciones:**
  - El 88% de las organizaciones indica que sus auditores internos de TI disponen de la certificación CISA.
  - El 41% indica que sus auditores de TI tienen la certificación CIA.
  - El 23% que tienen la certificación COBIT Foundation.
  - El 61% de las organizaciones ha manifestado que no requiere ninguna certificación específica como prioritaria.
  - El 39% de las organizaciones indica que requiere las certificaciones de CISA y CIA.
- Al seleccionar Auditores Internos de TI, las organizaciones buscan **conocimientos** en:
  - El 77% en seguridad lógica y estándares relacionados.
  - El 56% en gobierno de TI.
  - El 50% en procesos de negocio, análisis de aplicaciones informáticas, normativa relacionada con TI.
  - El 41% en metodologías de desarrollo, comunicaciones, hacking y forensic, y administración de sistemas.
- En cuanto a la **formación:**
  - El 46% de las organizaciones sí establecen formación específica para los auditores internos.
  - En el 80% de los casos la formación está enfocada a tecnologías o certificaciones relacionadas.
- Los **destinatarios de los informes** emitidos por Auditoría Interna de TI son:
  - En el 77% de los casos, las Direcciones Generales y los Comités de Auditoría.
  - En menor medida, las Direcciones de TI.
- Respecto a las **herramientas de apoyo** a la labor del auditor interno de TI, se observa cierta madurez en la utilización de herramientas de análisis masivo de datos y un menor desarrollo en el uso de herramientas de análisis de riesgos o de auditoría continua.

La encuesta revela que en el 77% de los casos los informes emitidos por Auditoría Interna de TI van dirigidos a las Direcciones Generales y los Comités de Auditoría y, en menor medida, a las Direcciones de TI.

HABILIDADES ESPECÍFICAS/CONOCIMIENTOS IMPORTANTES CONSIDERADOS EN LA SELECCIÓN DE AUDITORES INTERNOS DE TI



Los Riesgos Tecnológicos en el Negocio

No se debe entender el riesgo tecnológico como un riesgo independiente, sino está íntimamente ligado al negocio.

Las organizaciones cada vez tienen una mayor dependencia de las Tecnologías de la Información Su rápido desarrollo ha motivado la creación de nuevos modelos de negocio impensables hace muy pocos años. Algunos de los nuevos modelos de negocio, basados en esta evolución de la tecnología de la información, se basan en el acceso y la disponibilidad de información y servicios desde cualquier dispositivo.

Este desarrollo genera grandes oportunidades de negocio, a la vez que también introduce grandes riesgos: el incremento de los casos de espionaje, robos de información y ataques a través de las redes telemáticas y canales de venta en Internet; la preocupación creciente en materia de privacidad, confidencialidad de la información y cumplimiento de las legislaciones, nacionales e internacionales; el aumento de los casos de suplantación de identidad (cuentas de usuarios, etc.), fraude electrónico, entre otros.

DEFINICIÓN DE RIESGO TECNOLÓGICO

ISACA define el riesgo tecnológico[2] como *"El riesgo de negocio asociado al uso, propiedad, operación, participación, influencia y adopción de las tecnologías de la información (TI) en la organización"*. Desde este punto de vista, no se debe entender el riesgo tecnológico como un riesgo independiente, sino como un riesgo que está íntimamente vinculado al uso de la tecnología como parte del modelo de negocio.

La adopción de cualquier tecnología entraña riesgos y ante su evolución exponencial en los últimos años, es lógico intentar controlarlos y gestionarlos de forma adecuada. El riesgo tecnológico viene condicionado tanto por factores técnicos como humanos. Por un lado, los riesgos ligados a la propia tecnología: el hecho de que las organizaciones demanden soluciones más complejas, en mercados cada vez más competitivos, hace que se generen riesgos asociados a este rápido progreso que, de no ser detectados y mitigados, pueden tener un impacto negativo en la organización. Por otro lado, las organizaciones están forma-

2. The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

das por personas, cuyas motivaciones y capacidades son totalmente heterogéneas: esta diversidad provoca que, a menudo, el mayor riesgo sea el propio usuario, ya sea por errores involuntarios o por actividades malintencionadas.

PERCEPCIÓN DEL RIESGO TECNOLÓGICO

No existen dos organizaciones que tengan la misma percepción del riesgo de TI. La evaluación depende de la tipología de negocio, del apetito de riesgo de la Dirección y de la cultura corporativa en materia de riesgos. Aunque, paradójicamente, a veces la definición de metas y objetivos de una organización no se fundamenta en la tecnología, cuando desde el punto de vista de la gestión de TI son esenciales para alcanzar esas metas y objetivos.

La prestación de servicios, el desarrollo de productos, el mantenimiento de la operativa e incluso la continuidad del negocio, dependen del cuidado y conservación de la base tecnológica y del personal que la opera. El GTAG-1 muestra que todo entorno de TI es único y particular y, por lo tanto, representa una serie y asociación de riesgos únicos; los riesgos tecnológicos evolucionan a medida que aumenta el ritmo de desarrollo tecnológico y la proliferación de los riesgos está relacionada con la naturaleza sumatoria de los riesgos de TI, en la medida en que la suma del riesgo, considerados conjuntamente, es mayor que la suma de los riesgos individuales.

El gobierno de TI reside en que la estructura organizativa, el liderazgo y los procesos garantizan que las tecnologías de la información soportan las estrategias y objetivos de una organización.

CATEGORÍAS DE RIESGOS TECNOLÓGICOS

Una posible categorización de los riesgos asociados al uso de TI, basada en quién tiene la responsabilidad de establecer y mantener los controles necesarios para su gestión, podría ser: riesgos asociados al gobierno de TI, a la organización y gestión de TI (procesos de gestión) y a la capa técnica (implementaciones de tipo técnico).

Riesgos asociados al gobierno de TI

El gobierno de TI reside en que la estructura organizativa, el liderazgo y los procesos garantizan que las tecnologías de la información soportan las estrategias y objetivos de una organización. Los cinco componentes del gobierno de TI son la organización y estructuras de gobierno, el liderazgo ejecutivo y soporte, la planificación estratégica y operacional, la entrega y medición del servicio y la organización y gestión de riesgos de TI. Las políticas y estándares establecidos por la organización, deben establecer las formas de trabajo para alcanzar los objetivos. La adopción y cumplimiento de estas normas promueve la eficiencia y asegura la consistencia del entorno operativo de TI.

Algunos riesgos relacionados con el gobierno de TI son:

- La ausencia de planificación efectiva y de sistemas de monitorización del cumplimiento de las normas.
- La incapacidad de cumplir la misión de la organización.
- La pérdida de oportunidades de negocio y el escaso retorno de las inversiones en TI.
- La incapacidad para lograr los objetivos estratégicos de TI.
- Las potenciales ineficiencias en los procesos operativos de la organización.
- La falta de alineamiento entre los resultados de la organización y los objetivos estratégicos.

Riesgos asociados a la organización y gestión de TI (procesos)

Una estructura organizativa de reporte y responsabilidad que permite implementar un sistema eficaz de control, entre otras cosas, debe tener en cuenta:

- La segregación de funciones: las personas involucradas en el desarrollo de los sistemas están separadas de las dedicadas a operaciones de TI.
- La importancia de la gestión financiera de las inversiones.
- La gestión y el control de los proveedores, especialmente con un alto grado de externalización.
- La gestión del entorno físico, tanto del centro de proceso de datos, como de los equipos de usuario.

Así puede controlar de forma eficaz los riesgos organizativos y de gestión como:

- La asignación de privilegios de acceso excesivos a determinadas funciones clave, y evitar situaciones de fraude u omisiones inadvertidas en tiempo.
- El diseño incorrecto de indicadores económicos para medir el ROI.
- La monitorización inadecuada de los proveedores externos.
- El análisis incorrecto de riesgos medioambientales de seguridad del centro de proceso de datos.

Riesgos asociados a la capa técnica (implementaciones de tipo técnico)

La infraestructura técnica abarca los sistemas operativos, el diseño de redes internas, el software de comunicaciones, software de seguridad y protección y bases de datos, entre otros. El objetivo es asegurar que la información es completa, adecuada y exacta. Como ejemplos de riesgos relacionados con la capa técnica se pueden citar:

- Una inadecuada segregación de funciones por asignación de privilegios en el sistema que permita realizar acciones conflictivas o fraudulentas.
- Falta de un proceso adecuado de aprovisionamiento y gestión de usuarios, que entorpezca el desarrollo de la operativa.
- Ausencia de segregación de accesos, sin control de la actividad de usuarios y técnicos.
- Un inadecuado proceso de aplicación de actualizaciones de la infraestructura, sin

pruebas previas, transfiriendo problemas y vulnerabilidades a producción.

- Adquisición o mantenimiento de sistemas no establecidos formalmente, o implantación de sistemas no probados correctamente.
- Cambios en los sistemas de gestión o aplicación no probados y validados antes de su pase a producción.

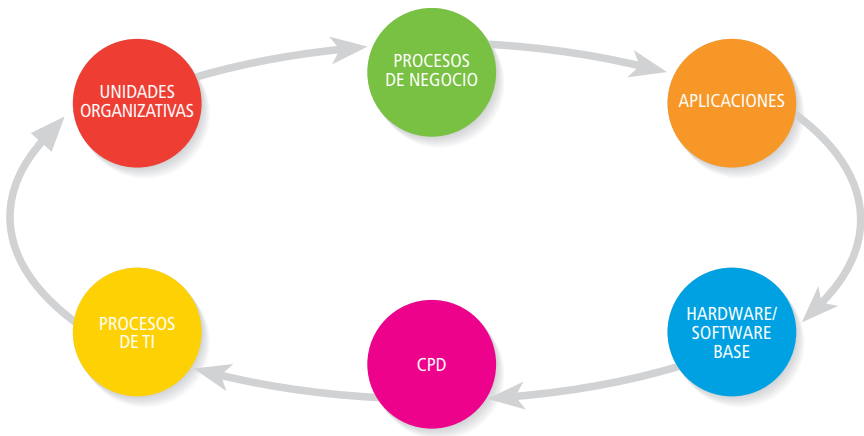
UNIVERSO DE AUDITORÍA INTERNA DE TI

El universo de Auditoría Interna de TI es un universo complejo, con múltiples dimensiones que abarcan los riesgos que pueden producirse en las unidades organizativas, los procesos de negocios, las aplicaciones, en el hardware, el software, los centros de proceso de datos, y los procesos TI. Este universo es el punto de partida para llevar a cabo una posterior evaluación de riesgos de los elementos que lo conforman y establecer un plan de Auditoría Interna sobre los mismos. Todos estos elementos están íntimamente relacionados y, por ejemplo, se puede definir el universo de Auditoría Interna de TI teniendo en cuenta las siguientes pautas:

- Obtener la relación y descripción de los procesos de negocio de cada organización.
- Confeccionar el mapa de las aplicaciones que soportan los procesos de negocio.
- Inventariar los equipos en los que se ejecutan las aplicaciones, tanto en centros de proceso de datos propios como externos.

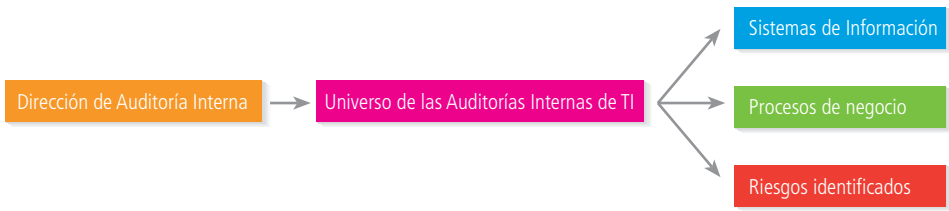
La definición del universo de Auditoría Interna de TI es el punto de partida para llevar a cabo una evaluación de riesgos y establecer un plan de Auditoría Interna sobre los mismos.

UNIVERSO DE AUDITORÍA INTERNA DE TI - RIESGOS



- Identificar los procesos de TI empleados para la gestión de todos los elementos básicos de tecnología (equipos, centros de procesos de datos, aplicaciones, sistemas operativos, bases de datos, comunicaciones y seguridad).
- Definir los riesgos asociados a estos elementos, tanto tecnológicos como de otra naturaleza.
- Establecer procesos continuos de mantenimiento de toda la información recabada para disponer de un universo actualizado.

En base a esta información, la Dirección de Auditoría Interna puede definir el universo de las Auditorías Internas de TI: los sistemas de información, los procesos de negocio y los riesgos identificados en el mapa de riesgos corporativos o el mapa de riesgos de TI. Es preferible un enfoque integrado de evaluación de riesgos, en lugar de un análisis específico para TI. Así se aprovechan las sinergias que genera el conocimiento que Auditoría Interna dispone tanto del negocio como de la plataforma tecnológica.



Integración de la Cobertura de TI en Auditoría Interna

OBJETIVOS DE LA INTEGRACIÓN DE LA AUDITORÍA INTERNA DE TI

Auditoría Interna de TI es cualquier proceso de auditoría que revisa y evalúa los sistemas automáticos de procesamiento de la información. La misión del auditor interno de TI es proporcionar las recomendaciones necesarias a la Dirección para mejorar y lograr un adecuado control de la tecnología y los sistemas de información. También busca que se mejore la eficiencia operacional y administrativa, teniendo en cuenta tanto los requisitos legales como los objetivos de negocio de la organización.

Los principales objetivos de Auditoría Interna al integrar Auditoría Interna de TI[3] son:

- Evaluar los mecanismos que aseguran la integridad, confidencialidad y confiabilidad de la información, identificando riesgos y proponiendo controles.
- Proporcionar apoyo a la Dirección del área de TI y de la organización para lograr los objetivos estratégicos.
- Analizar la relación coste-beneficio de los sistemas de información y recomendar alternativas para su mejora.
- Evaluar los mecanismos para minimizar riesgos en los sistemas de información.
- Analizar la seguridad de los datos, el hardware, el software y las instalaciones, así como la concienciación en seguridad de los usuarios.
- Analizar el grado de satisfacción de los usuarios de los sistemas de información.

Esta lista no trata de ser una relación exhaustiva de elementos a considerar a la hora de la definición del universo auditable de Auditoría Interna de TI, pudiendo ser incorporados otros muchos en función de la naturaleza de la compañía, del sector en el que opere y de la evolución y madurez propia de la Dirección de Auditoría Interna en cuestión.

A la hora definir el enfoque un trabajo, es importante remarcar el nivel de integración existente entre las Auditorías Internas de TI y el resto de auditorías para determinar su alcance.

AUDITORÍAS INTEGRADAS *VS.* AUDITORÍAS PURAS DE TI

A la hora de definir el enfoque de un trabajo, es importante remarcar el nivel de integración existente entre las Auditorías Internas de TI y el resto de auditorías *(para más detalle, ver GTAG-11).* De esta manera, no serán iguales el alcance y el planteamiento de una auditoría pura de TI (por ejemplo: revisión del proceso de resolución de incidencias de explotación o la seguridad perimetral), que los aspectos de TI a revisar en una auditoría integrada (por ejemplo: revisión de la plataforma que soporta el proceso de compras).

Universo de Auditoría Interna	Plan de Auditoría Interna poco integrado	Plan de Auditoría Interna parcialmente integrado	Plan de Auditoría Interna altamente integrado
Procesos de Negocio - Operacionales - Financieros - Cumplimiento	Auditorías Internas de Negocio	Auditorías Internas de Negocio	Auditoría Interna Integrada
Aplicaciones y Software - Controles de Aplicaciones - Controles Generales	Auditoría Interna de TI exclusivamente	Auditoría Interna Integrada	Auditoría Interna Integrada
Controles de Infraestructura - Base de Datos - Sistemas Operativos - Elementos de Red	Auditoría Interna de TI exclusivamente	Auditoría Interna de TI exclusivamente	Auditoría Interna Integrada

3. Consejos para la Práctica IAI 2010-1 y 2210-1del *Marco Internacional para la Práctica Profesional de la Auditoría Interna.* Instituto de Auditores Internos.

Una visión integral del Plan de Auditoría interna permite al Director de Auditoría Interna analizar la relación existente entre los diferentes procesos de negocio y los procesos y activos de TI.

Un enfoque de baja integración entre los trabajos de Auditoría Interna de TI y el del resto de las áreas de Auditoría Interna, conlleva a una evaluación aislada de los riesgos relacionados con TI, dificultando la interrelación de los resultados obtenidos (por ejemplo: ¿Cómo afecta al proceso de ventas que el entorno Windows esté mal securizado, o que el diseño funcional de la base de datos esté mal diseñado o gestionado?) y dando como resultado un menor nivel de certeza en las conclusiones obtenidas a nivel global.

Este nivel de certeza se irá incrementando según se aumente el nivel de integración entre el Plan de Auditoría Interna de TI y el de negocio, alcanzando su máximo nivel una vez que los trabajos de Auditoría Interna de TI se integran o se relacionan con las otras auditorías del negocio. Esto permite obtener una visión integral y completa de los riesgos bajo análisis.

Esta visión integral del Plan de Auditoría Interna permite al Director de Auditoría Interna analizar la relación existente entre los diferentes procesos de negocio, y los distintos procesos y activos de tecnología que soportan su funcionamiento. Así, será posible abarcar de manera conjunta todos los riesgos que afectan a un determinado proceso o área de negocio, obteniendo una visión más completa de su situación y de su exposición real, aumentando, por tanto, el nivel de aseguramiento arrojado por las conclusiones que se obtendrán de los trabajos.

Hay que tener en cuenta que esta aproximación no descarta la ejecución de ciertas auditorías puras (tanto de TI como de negocio), siempre y cuando exista una justificación suficiente para ello (por ejemplo: resultado del análisis de riesgos o petición expresa de la Dirección).

En todo caso, siempre es importante definir de antemano la interrelación que los resultados de estos trabajos tendrán con el resto de riesgos o procesos del universo de Auditoría Interna.

ESTRATEGIAS DE INTEGRACIÓN DE LA AUDITORÍA INTERNA DE TI

La estrategia de integración de Auditoría Interna de TI depende del grado de madurez de Auditoría Interna en la organización, de la complejidad de TI y de los recursos económicos disponibles.

Existen diversas posibilidades, aportando cada una de ellas beneficios e inconvenientes implícitos.

Evaluando las necesidades y recursos disponibles, la organización deberá determinar cuál de las estrategias presentadas se adecua más a su planteamiento de Auditoría Interna de TI.

La elección de una estrategia inicial puede evolucionar con el paso del tiempo.

Estrategia	Beneficios	Inconvenientes
Incorporación de personal en plantilla	- Adquisición de un mayor conocimiento de los flujos de negocio de la organización, procesos de TI y plataformas tecnológicas de la misma. - Mayor integración con el equipo actual de Auditoría Interna. - Lograr la incorporación de un perfil polivalente que puede dinamizar la práctica de Auditoría Interna.	- Posible desactualización de los conocimientos en determinadas tecnologías emergentes a lo largo del tiempo en caso de no exista un proceso de formación continua en TI.
Contratación de un proveedor externo	- Aportación de conocimientos externos por la ejecución de trabajos en distintas organizaciones y conocimientos tecnológicos más actualizados. - Flexibilidad de contratación según necesidades, sin coste fijo. - Reducción del riesgo en el proceso de contratación o incorporación interna, si el perfil no es el adecuado.	- Dependiendo de la complejidad del negocio, pueden aparecer dificultades para entender la actividad de la organización y sus procesos de negocio. - Posibilidad de que el conocimiento adquirido durante el proyecto se pierda al finalizar la prestación del servicio.
Enfoque mixto	- Posibilidad de abordar proyectos cuyo conocimiento no dispone la función de Auditoría Interna de TI. - Transferencia de la carga de trabajo del equipo interno a personal externo. - Transferencia de conocimientos al personal interno. - Auditoría Interna siempre retiene las labores de supervisión.	- Posibilidad de aumentar las horas invertidas en los proyectos de auditoría si no se aplica un protocolo estricto de supervisión y control de las distintas participaciones. - Incorporar un aspecto de desmoralización en el personal interno si no existe una real transferencia de conocimientos.

MADUREZ EN LA INTEGRACIÓN DE LA AUDITORÍA INTERNA DE TI

La forma de integrar la función de Auditoría Interna de TI dentro de las Direcciones de Auditoría Interna ha ido evolucionando la actualidad, cobrando cada vez un mayor peso específico. Existen tres niveles de integración de Auditoría Interna de TI, en función de la ma-

durez de la Dirección de Auditoría Interna con respecto a la cobertura de la Auditoría TI:

- **Básico.** Es el de aquellas Direcciones de Auditoría Interna que emplean auditores financieros para evaluar la efectividad de los controles de los sistemas de información. Al no disponer de auditores internos especialmente cualificados en TI, se focalizan en la revisión a alto nivel de riesgos y controles generales asociados a la gestión de la tecnología de la información. Este planteamiento se centra básicamente en el gobierno de TI. No tienen capacidad para valorar la "gestión" o la "capa técnica". Pueden producirse ineficiencias en la ejecución de las Auditorías Internas de TI por la falta de conocimiento y/o práctica, o por la imposibilidad de analizar alcances o sistemas amplios o complejos.

- **Medio.** Es el de aquellas Direcciones de Auditoría Interna que disponen de auditores internos con conocimientos de tecnología que, entre otras tareas de revisión de los sistemas de información, apoyan al Departamento de Auditoría Interna en la extracción de información de los sistemas, tratamiento y análisis de datos para auditorías financieras y de procesos, y evaluación de los riesgos y controles asociados a procesos de TI. En este nivel medio de integración se observan sinergias con el resto de trabajos de Auditoría Interna y se genera la capacidad de valorar componentes de la "capa de gestión".

- **Avanzado.** Es el de aquellas Direcciones de Auditoría Interna que disponen de Auditores Internos de TI integrados en el equipo de Auditoría Interna (financieros, procesos, crédito, mercados, etc...) para acometer revisiones integrales de procesos de negocio, que incluyan dentro de su alcance la revisión de los riesgos y controles asociados a las aplicaciones que los soportan. Los auditores internos de TI disponen de conocimientos profundos tanto de los procesos de negocio, como del funcionamiento de las aplicaciones. La realización de las Auditorías Internas empleando equipos integrados por auditores financieros y de TI permite opinar de una forma global sobre la efectividad de los controles manuales y automáticos existentes en un proceso e incluso evaluar el nivel de la "capa técnica".

ESQUEMA DE MADUREZ DEL NIVEL DE INTEGRACIÓN DE LA AUDITORÍA INTERNA DE TI

Una de las decisiones más importantes de los Directores de Auditoría Interna y de las Comisiones de Auditoría para minimizar los riesgos asociados a la cobertura de los procesos tecnológicos de la organización, es la creación de la función de Auditoría Interna de TI dentro de las Direcciones de Auditoría Interna, decidir el nivel de integración de dicha función (básico, medio o alto), y fijar la adecuada dotación de recursos humanos, técnicos y económicos.

PERFIL DEL AUDITOR INTERNO DE TI

No existe una carrera universitaria que se oriente específicamente a la disciplina de la Auditoría Interna de TI, pero es tendencia en el mercado que los perfiles demandados cuenten primordialmente con estudios universitarios y con una importante experiencia tecnológica. Adicionalmente, existe formación complementaria de postgrado en materia de Auditoría Interna de TI y un gran número de certificaciones profesionales. Una de las más reconocidas mundialmente es la certificación CISA, expedida por ISACA. Cada día más auditores internos de TI obtienen la certificación CIA del IIA (Institute of Internal Auditors).

Los conocimientos y habilidades con los que debería contar un auditor interno de TI, son:

- Independencia en la ejecución de sus trabajos, junto con capacidad de análisis e interpretación de las evidencias.

Conocimientos técnicos

- Normas y estándares para la práctica de la Auditoría Interna.
- Técnicas de evaluación de riesgos.
- Conocimientos de tecnología: programación, redes y comunicaciones, explotación, seguridad informática, planes de continuidad, etc…
- Recopilación y tratamiento de grandes cantidades de información.
- Identificación de desviaciones en procesos que implican riesgos para la organización.
- Monitorización de actividades de informática y TI en general.
- Técnicas estadísticas y de muestreo.

Conocimientos del negocio

- Plataformas tecnológicas de la organización.
- Capacidad de asimilar y entender los procesos de la organización.
- Conocimiento de los interlocutores clave, especialmente en el ámbito de TI.
- Identificación de los sistemas e infraestructuras que dan soporte a los procesos de negocio de la organización.

Habilidades

- Dotes de expresión oral y escrita para una presentación clara y objetiva de informes y opiniones.
- Habilidad para el trabajo en equipo, capacidad analítica y síntesis, autonomía, y proactividad.
- Habilidad para relacionarse con grupos de trabajo de diferentes niveles jerárquicos y conocimiento de la organización.
- Habilidades de negociación que le permitan argumentar sus puntos de vista.

Cada día más auditores internos de TI obtienen la certificación CIA del IIA (Institute of Internal Auditors).

METODOLOGÍA DE TRABAJO

La Auditoría Interna de TI debe encuadrase dentro de las normas generales de la organización para Auditoría Interna, con el referente específico del *Marco Internacional para la Práctica Profesional de la Auditoría Interna* del Instituto de Auditores Internos, y complementariamente, las normas y estándares promovidas por la ISACA. Estas normas determinan la ética profesional de la auditoría, la independencia, objetividad y diligencia. La Auditoría Interna de TI sigue la metodología de trabajo definida por la propia Dirección de Auditoría Interna, en cuanto a directrices y procedimientos (modo de documentar, elaboración de entregables, etc...).

RELACIÓN DE AUDITORÍA INTERNA DE TI CON EL ÁREA DE TECNOLOGÍA

Es necesario establecer los límites entre la función de Auditoría Interna de TI y las áreas de TI para facilitar la gestión diaria y aprovechar las sinergias entre ambas unidades, sin comprometer su independencia. Auditoría Interna no es responsable de la ejecución de funciones TI, ni de la realización de controles periódicos. En el estatuto de Auditoría Interna suele figurar que la Dirección de Auditoría Interna puede requerir acceso a todos los datos y sistemas informáticos para realizar sus funciones.

Independientemente de esta afirmación, la relación entre ambos departamentos se basa en los siguientes aspectos:

Auditoría Interna de TI *vs.* Área de TI

- Evalúa el cumplimiento: detecta incidencias, ineficiencias y efectúa recomendaciones de valor añadido.
- Promueve las mejores prácticas de TI.
- Colabora en la difusión de las políticas de TI de la organización.
- Es asesor especialista en riesgos, con una visión global del negocio.

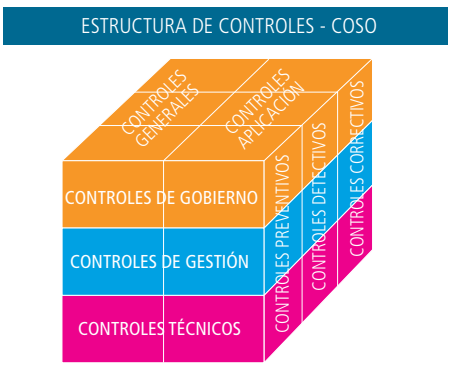
Área de TI *vs.* Auditoría Interna de TI

- Facilita la estandarización de la metodología de Auditoría Interna mediante herramientas informáticas (conectividad, accesos, recopilación de información de registros informáticos, y datos de negocio, etc.).
- Capacita para el manejo de altos volúmenes de información.
- Promueve análisis de los riesgos de TI.
- Posibilita procesos de supervisión y revisión.
- Realiza el seguimiento de la implantación de las recomendaciones de Auditoría Interna.

El auditor interno de TI tiene que estar preparado para enfrentarse a procesos y sistemas, y estar familiarizado con el lenguaje y la comunicación en términos de TI. En aquellos casos en que el Departamento de TI realice "auto-auditorías" o contrate a proveedores externos parar realizar auditorías dentro de su área, Auditoría Interna debería estar informada y tener acceso a los papeles de trabajo y a los informes.

Enfoque de las Auditorías Internas de TI

El enfoque a tomar en la ejecución de una Auditoría Interna de TI depende en gran medida del área y/o procesos a analizar y evaluar, y de las habilidades y conocimientos que se necesitan en el auditor interno de TI para la Auditoría Interna a realizar. No es lo mismo revisar la gestión de un proyecto de TI –para cuya ejecución se necesitarán habilidades y conocimientos menos técnicos y más orientados a los de un gestor– que una revisión del nivel de seguridad de los servidores Unix expuestos en la DMZ, para cuya tarea de evaluación se necesitará un dominio de aspectos mucho más técnicos sobre esa tecnología en concreto.



Es importante diferenciar tres clases de trabajos de Auditoría Interna de TI según el tipo de controles a evaluar:

Auditorías Internas del gobierno de TI

Trabajos orientados a la evaluación de aquellos controles establecidos para la supervisión de una correcta gestión de la información, el establecimiento del *"tone at the top"*, así como de las políticas que marcan las guías generales de la organización con relación a TI.

Auditorías Internas de la organización y gestión de TI

Enfocadas a revisar aspectos generales de la gestión de TI, tales como la protección física de los activos de TI, la gestión de cambios, la gestión del outsourcing (externalización), la gestión de proyectos de TI o la gestión financiera de TI.

Auditorías Internas de la capa técnica

Engloban aquellos trabajos que requieren conocimientos específicos de la plataforma tecnológica (sistemas operativos, bases de datos, elementos de comunicaciones…). Tam-

bién pueden incluir la revisión de aquellos controles de determinada aplicación que requiera un conocimiento profundo y "técnico" de su funcionamiento.

Adicionalmente, y aunque no sean Auditorías Internas de TI, habría que considerar los trabajos de análisis masivo de datos mediante el uso de herramientas tales como ACL o IDEA (por ejemplo: apoyo a investigaciones de fraude, SAS99). Estos trabajos han recaído históricamente bajo la responsabilidad de los auditores internos de TI, aunque, recientemente –debido al mayor conocimiento en sistemas y a la formación específica recibida por las nuevas generaciones de los auditores de negocio– la ejecución de dichos trabajos va, poco a poco, pasando a ser responsabilidad de estos últimos.

Herramientas de Soporte a las Auditorías Internas de TI

En este apartado se realiza una catalogación y breve descripción de las herramientas software que puede utilizar una Dirección de Auditoría Interna para la gestión, planificación y ejecución de Auditorías Internas de TI.

Herramientas para la gestión de la Dirección de Auditoría Interna

- Herramientas que facilitan la **gestión del Departamento** de Auditoría Interna incorporando funcionalidades como:
  - Definición del Plan Auditoría Interna basado riesgos.
  - Interrelación con la herramienta de gestión de riesgos corporativos.
  - Planificación y seguimiento de los trabajos en curso, en términos de calendario, recursos asignados, tiempo y costes.
  - Seguimiento de la implantación de los aspectos de mejora detectados en los trabajos.
  - Gestión de personal del equipo, en términos de:
    - Formación.
    - Evaluación anual y por trabajo.
- Herramientas de **análisis de riesgos** automatizado. Son inestimables para toda la Dirección de Auditoría Interna ya que permiten realizar análisis en entornos de TI com-

plejos, que no suelen ser fáciles sin la ayuda de herramientas automatizadas. Deben incorporar funcionalidades como:

- Integración con la herramienta de gestión de riesgos corporativos.
- Posibilidad de creación y definición de riesgos.
- Definición del universo auditable de TI.
- Facilidad para incorporar la valoración de los riesgos por parte de las personas interesadas.
- Definición de factores de ponderación de los riesgos definidos.
- Reportes gráficos de las áreas con más riesgos.
- Propuesta de trabajos a realizar en base el análisis de riesgos realizado.

- Herramientas que facilitan la **gestión del ciclo de vida de una Auditoría Interna** incorporando funcionalidades como:
  - Planificación del trabajo (desglose de tareas, asignación de recursos, evaluación de riesgos).
  - Apertura y comunicación del inicio del trabajo.
  - Control y seguimiento de la ejecución del trabajo relativo a progreso, imputaciones de horas, desviaciones, etc.
  - Progreso de las tareas.
  - Imputaciones de tiempo por recurso y/o tarea.
  - Desviaciones en alcance, tiempo y coste del trabajo.
  - Materialización de los riesgos.
  - Gestión centralizada de los papeles de trabajo manteniendo una trazabilidad sobre la documentación.
  - Cierre electrónico del trabajo y emisión del informe.
  - Seguimiento del progreso de la implantación de los plantes correctivos –previa asignación de los responsables– de la documentación a entregar y de las fechas de comprometidas.

Herramientas para la ejecución del trabajo de campo de una Auditoría Interna de TI

- Herramientas de **análisis de datos** que permiten al equipo de Auditoría Interna realizar un análisis estadístico sólido sobre grandes volúmenes de datos. Pueden emplearse como soporte para las auditorías internas de TI o de negocio. Algunas de sus funcionalidades son:
  - Acceso a datos de distintos entornos y sistemas.
  - Analizar el 100% de la población de datos.
  - Funciones propias de Auditoría Interna como estratificación, identificación de duplicados, faltantes, muestreo estadístico, comparaciones, cálculos, etc.
  - Automatización de tareas repetitivas.
  - Resultados gráficos.
  - Protección de los datos originales.

La existencia de un Auditor Interno de TI experto en determinadas herramientas de software, no implica tener implantada la función de Auditoría Interna de TI.

- Herramientas de **análisis de la seguridad.** Pueden clasificarse en función del ámbito de aplicabilidad:
  - Herramientas de **análisis de redes.** Son programas que pueden ser ejecutados en una red informática que recopilan datos sobre ella. Pueden ser utilizadas para verificar la exactitud de los diagramas de la red o identificar los dispositivos de red más vulnerables a ataques.
  - Herramientas de **hacking.** La mayoría de las tecnologías poseen vulnerabilidades estándar (identificaciones, contraseñas o parámetros por defecto cuando se instala la tecnología sin personalizarla). Las herramientas de hacking proporcionan un método automático para la verificación de las vulnerabilidades estándar. Dichas herramientas, tras fijar los objetivos de la infraestructura de TI (cortafuegos, servidores, redes y sistemas operativos), proporcionan un listado de las vulnerabilidades de los mismos.

    La importancia de estas herramientas radica en que son utilizadas por intrusos para atacar organizaciones. Con el fin de repeler estos ataques, la organización debe tener acceso a la misma información. Ya que el uso de estas herramientas puede ser potencialmente peligroso de cara a la integridad de los sistemas que analizan, el auditor interno de TI debe coordinar con el área de TI la planificación y el alcance de la prueba, para no afectar al normal funcionamiento de los sistemas.
  - Herramientas **específicas para ciertos entornos.** Estas herramientas sirven para el análisis de la seguridad para determinados entornos. Muchas de ellas tienden a ser especializadas para un entorno (PeopleSoft, SAP, o Oracle), analizando la seguridad de usuarios contra reglas preconfiguradas. Estas herramientas también pueden evaluar la segregación de funciones dentro de la aplicación. Además cuentan con unos parámetros preconfigurados, o las "mejores prácticas" promovidas por el proveedor, que deberían ser adaptados a la realidad del negocio.
- Herramientas **transversales** que por su heterogeneidad no han sido incluidas en las categorías anteriores:
  - Sistemas de mensajería y comunicación.
  - Programa para la realización de diagramas de flujo.
  - Herramientas de cifrado.
  - Plataforma colaborativa de trabajo.
  - Etc.

Auditoría con medios informáticos *vs.* Auditoría Interna de TI

La existencia de auditores internos usando una herramienta de software como apoyo a auditorías de negocio, no significa que se estén cubriendo los riesgos asociados a TI y, por lo tanto, no se puede considerar que se estén realizando Auditorías Internas de TI. Por eso la existencia de un Auditor Interno de TI experto en determinadas herramientas de software (por ejemplo: extracción de datos o tratamiento de grandes volúmenes de información financiera) no implica tener implantada la función de Auditoría Interna de TI. Para que así sea, los auditores internos de TI deben

centrar la mayor parte de su actividad en la evaluación relacionada con los activos de TI (personas, procesos y sistemas) con el fin de verificar si cumplen con los objetivos asignados y si están alineados con los fines de la organización.

Gestión de las herramientas de software de la Dirección de Auditoría Interna

Las herramientas de software de la Dirección de Auditoría Interna deben ser gestionadas con el mayor rigor posible, para cumplir las normas y/o políticas de la organización y las buenas prácticas del negocio. Debe establecerse un estricto control del proceso de aprovisionamiento de usuarios, especialmente en las bajas, para evitar accesos no autorizados; hay que gestionar correctamente el proceso de licencias (si aplica); y realizar con una periodicidad adecuada el proceso de copias de seguridad.

Algunas de las herramientas de software, sobre todo las orientadas a la gestión de la Dirección de Auditoría Interna, almacenan evidencias asociadas a los procesos de auditoría que se han ejecutado. Es de vital importancia que esta herramienta esté correctamente gestionada y securizada, debido a la importancia de la información almacenada. A su vez, hay que evaluar si la gestión de alguna de las herramientas se quiere internalizar dentro de la Dirección de Auditoría Interna (un recurso total o parcialmente dedicado a tareas de gestión y mantenimiento) o externalizar en el área de TI, evaluando, en este caso, los riesgos de confidencialidad.

Las herramientas de software de Auditoría Interna deben estar correctamente gestionadas y securizadas, debido a la importancia de la información que almacenan.

Anexo 1 · Glosario - Acrónimos

ACL	Herramienta de tratamiento masivo de datos.
BASES DE DATOS	Programa informático que permite el almacenaje y posterior acceso a datos de manera rápida y estructurada.
CIA	Certified Internal Auditor (Auditor Interno Certificado). Certificación profesional emitida por el IIA.
CISA	Certified Information Systems Auditor (Auditor de Sistema de Información Certificado). Certificación profesional emitida por ISACA.
CORTAFUEGOS	Firewall. Elemento de red cuya función principal es el filtrado de las comunicaciones entre las diferentes redes, autorizándolas o denegándolas en función de las reglas que le hayan sido configuradas.
COBIT	*Control Objectives for Information and Related Technology* (Objetivos de Control para Información y Tecnologías Relacionadas) es un marco de gobierno para las tecnologías de la información, publicado por ISACA.
COSO	Committee of Sponsoring Organizations of the Treadway Commission. Entidad formada por una unión de entidades del sector privado, incluido el IIA, emisora de los marcos de control interno *(Internal Control-Integrated framework)* y gestión de riesgos *(Enterprise Risk Management-Integrated framework).*
DMZ	*Demilitarized Zone.* Zona de la red de una compañía en la que se suelen ubicar aquellos servidores que pueden ser accesibles desde el exterior, estando éstos, por lo tanto, expuestos a un mayor riesgo.
ELEMENTOS DE RED	Dispositivos que permiten la comunicación entre los diferentes sistemas informáticos y que conforman las redes de comunicaciones (por ejemplo, router).
ERP (SAP)	*Enterprise Resource Planning* o Sistema de Planificación de Recursos. Sistemas informáticos que integran y dan soporte a los procesos de negocio de manera conjunta y coordinada (por ejemplo, SAP).
GTAG	*Global Technology Audit Guidelines* - Guías publicadas por el IIA para la Auditoría Interna de los sistemas de información.
HACKING	Cualquier acción encaminada a obtener acceso, de forma ilegal y sin el consentimiento del propietario, a un sistema informático con el objetivo de sustraer información. Se conoce como "hacking ético" los accesos de este tipo autorizados para la realización de auditorías de seguridad.
IDEA	Herramienta de tratamiento masivo de datos.

ISACA	Information Systems Audit and Control Association (Asociación de Auditoría y Control de los Sistemas de Información). Asociación internacional para el desarrollo de metodologías para la realización de actividades de auditoría y control en los sistemas de información, Asociación independiente, global y sin ánimo de lucro, involucrada en el desarrollo, adopción y utilización de buenas prácticas globalmente aceptadas para los sistemas de información.
ROI	*Return on investment.* Retorno de la inversión.
SAS99	Statement on Auditing Standards nº 99. *Consideraciones sobre fraude en auditorías de los estados financieros,* emitido por The American Institute of Certified Public Accountants.
SISTEMAS OPERATIVOS	Software de base instalado en un sistema informático que interactúa con el hardware y permite la ejecución de las aplicaciones instaladas en él (por ejemplo: Windows 8 o Red Hat Enterprise Linux).
TONE AT THE TOP	Camino que marca la Dirección de la Organización.
UNIX	Familia de sistemas operativos multiusuario y multitarea, tanto para ordenadores personales como para mainframes.

Anexo 2 · Bibliografía

Guías Globales de Auditoría Interna de Tecnologías de la Información (GTAG) (www.globaliia.org).

- GTAG-1 *Information Technology Risks and Control* - 2nd Edition
- GTAG-2 *Change and Patch Management Controls: Critical for Organizational Success* - 2nd Edition
- GTAG-3 *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*
- GTAG-4 *Management of IT Auditing.* 2nd Edition
- GTAG 5 *Auditing Privacy Risks* - 2nd Edition
- GTAG-7 *Information Technology Outsourcing*
- GTAG-8 *Auditing Application Controls*
- GTAG-9 *Identity and Access Management*
- GTAG-10 *Business Continuity Management*
- GTAG-11 *Developing the IT Audit Plan*
- GTAG-12 *Auditing IT Projects*
- GTAG-13 *Fraud Prevention and Detection in an Automated World*
- GTAG-14 *Auditing User-developed Applications*
- GTAG-15 *Information Security Governance*
- GTAG-16 *Data Analysis Technologies*
- GTAG-17 *Auditing IT Governance*

Guías para la Evaluación del Riesgo de TI (GAIT) (www.globaliia.org).

- GAIT The GAIT Methodology.
- GAIT for IT General Control Deficiency Assessment.
- GAIT for Business and IT Risk.

Marco Internacional para la Práctica Profesional de la Auditoría Interna (www.auditoresinternos.es).

Internal Control-Integrated Framework – COSO (Committee of Sponsoring Organizations of the Treadway Comisión) – 2013 (www.coso.org).

COBIT 5 The framework for governance and management of enterprise IT (www.isaca.org).

Estándares, Guías, Técnicas y Procedimientos para la Auditoría de TI (www.isaca.org).

- **Estándares de auditoría y aseguramiento de SI:** 1001 Audit Charter; 1002 Organizational Independence; 1003 Professional Independence; 1004 Reasonable Expectation; 1005 Due Professional Care; 1006 Competence; 1007 Assertions; 1008 Criteria; 1201 Engagement Planning; 1202 Risk Assessment in Audit Planning; 1203 Performance and Supervision; 1204 Materiality; 1205 Evidence; 1206 Using the Work of Other Experts; 1207 Irregularity and Illegal Acts; 1401 Reporting; 1402 Follow-up Activities.
- **Directrices y Guías de auditoría y aseguramiento de SI:** 2001 Audit Charter (G5); 2002 Organisational Independence (G12); 2003 Professional's Independence (G17); 2004 Reasonable Expectation In development; 2005 Due Professional Care (G7); 2006 Proficiency (G30); 2007 Assertions In development; 2008 Criteria In development; 2201 Engagement Planning (G15); 2202 Risk Assessment in Audit Planning (G13); 2203 Performance and Supervision (G8); 2204 Materiality (G6); 2205 Evidence (G2); 2206 Using the Work of Other Experts (G1); 2207 Irregularity and Illegal Acts (G9); 2208 Audit Sampling (G10); 2401 Reporting (G20); 2402 Follow-up Activities (G35).
- **Técnicas y herramientas para la auditoría de TI y el aseguramiento**
  - COBIT 5 family of products
  - IS Audit and Assurance Programmes
  - IT Audit Basics
  - Technical and Risk Management Reference Series
  - White papers

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Primera producción de LA FÁBRICA DE PENSAMIENTO que aborda el mundo de la tecnología en Auditoría Interna.

La importancia que han adquirido las Tecnologías de la Información (TI) en las organizaciones ha sido un factor diferenciador en el posicionamiento en el mercado, pero también lo está siendo en el mundo del aseguramiento y, en concreto, de la Auditoría Interna.

Este documento destaca la importancia de la figura de la función de Auditoría Interna de TI en su apoyo a la organización en la gestión, gobierno y control de los riesgos de TI.

Se han estudiado temas relacionados con la gestión de las relaciones entre Auditoría Interna de TI y el área de TI, destinatarios de los informes de Auditoría Interna de TI o las herramientas que habitualmente se utilizan en esta tipología de trabajos.

El documento pretende ser de utilidad tanto al Director de Auditoría Interna (DAI) como a las más altas instancias de la Dirección de una organización, en la implantación de la función de Auditoría Interna de TI, como un elemento más de Auditoría Interna. Incluye una bibliografía para aquéllos que quieran profundizar sus conocimientos sobre la temática tratada.

Instituto de Auditores Internos de España

The Institute of Internal Auditors