

# Clases y tipos de auditoría

---



Auditoría de  
Sistemas

UNIVERSIDAD

**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**

# » Auditoría de sistemas

La auditoría de sistemas es clave por la relevancia que tienen los sistemas de información para los objetivos de todo tipo de organizaciones e industrias.

La auditoría es una actividad necesaria y, en muchos casos, requerida legalmente, en las organizaciones y empresas de la actualidad. La auditoría informática busca evaluar el diseño de control y la efectividad de los sistemas de información internos, que incluyen los protocolos de seguridad y eficiencia, procesos de desarrollo, gobierno IT (Tecnología Informática) y demás áreas informáticas que posea la organización.

Asimismo, la auditoría informática se enfoca en ayudar a las organizaciones a cumplir sus metas y planes, verificando que los activos informáticos se usen adecuadamente para lograr el objetivo de la organización.

## Definición inicial

La auditoría puede definirse como **un proceso sistemático de revisión y evaluación objetiva, realizada sobre las actividades de una organización, con el objetivo de verificar su cumplimiento a las normas y condiciones pre establecidas.**

Debe ser efectuada por un auditor calificado e independiente, el que recolecta evidencias y emite una opinión profesional para determinar el grado de fiabilidad del objeto analizado. Es decir que por medio de su observación, considera si las actividades realizadas por la organización representan adecuadamente las condiciones o las expectativas que le son atribuidas.

Los conceptos elementales a tener en cuenta en la definición anterior son:

- el contenido de una auditoría será una opinión comunicada en un informe y elevada a las personas interesadas;
- la condición de una auditoría es que sea de carácter profesional, es decir, realizada por una persona que posea los conocimientos y las habilidades técnicas necesarias para la actividad;
- la justificación de una auditoría está sustentada en procedimientos. para su correcta elaboración, además, cuenta con herramientas tecnológicas de soporte;
- el objetivo de una auditoría es comunicar la información obtenida por los procedimientos realizados;
- la finalidad de una auditoría es informar el grado de adecuación a la realidad y a las expectativas del objeto en estudio.

La auditoría no es un proceso que busca detectar fraudes ni tampoco juzgar las conductas de las personas. Sin embargo, el auditor debe sistemáticamente recoger evidencias, agruparlas y evaluarlas, para estudiar los mecanismos y procedimientos reales ejecutados por una organización. Luego, se debe presentar una evaluación profesional del grado de eficiencia y eficacia en el logro de los objetivos establecidos por los niveles gerenciales.

Es fundamental la condición y la característica de objetividad e independencia en el rol del auditor con respecto a la organización analizada. El boletín de la comisión de normas y asuntos profesionales del Instituto de Auditores Internos de Argentina define que el área encargada de realizar la auditoría debe reportar jerárquicamente a un nivel en la organización que no le condicione en absoluto la posibilidad de determinar libremente el alcance y de emitir opiniones imparciales, neutrales, objetivas y equilibradas.

Cuando hablamos de objetividad, nos referimos a que se debería apreciar la actitud de neutralidad e imparcialidad en quien se desempeñe como auditor interno, quien no debería tener intereses de ninguna índole, que le provoque un conflicto en cuanto a su labor de auditoría. **Con relación al tema de *conflicto de intereses*, las normas indican que el auditor interno no debería realizar evaluaciones sobre actividades que él mismo haya realizado para la organización durante el último año.**

La auditoría se basa en la afirmación de que la información a estudiar es *verificable*. El informe del auditor representa su visión formal y sistemática, orientada a acciones correctivas de la estructura organizacional, los planes y procedimientos, la forma de operar, el uso de los recursos humanos y físicos y el cumplimiento a las leyes y regulaciones establecidas.

## Clases de auditoría

Inicialmente, la auditoría se limitaba a verificar los flujos financieros de las organizaciones. Más adelante, el concepto se extendió a otras actividades. Actualmente, existen numerosas divisiones o clases de esta actividad. Las siguientes son algunas de ellas:

- **Auditoría financiera:** realizada por un profesional experto en contabilidad de los libros y registros financieros, con el propósito de opinar sobre la veracidad de la información contenida en ellos y sobre el cumplimiento de las normas contables vigentes en el país. El auditor presenta su opinión sobre los estados contables y su reflejo de la realidad patrimonial y financiera del ente auditado.

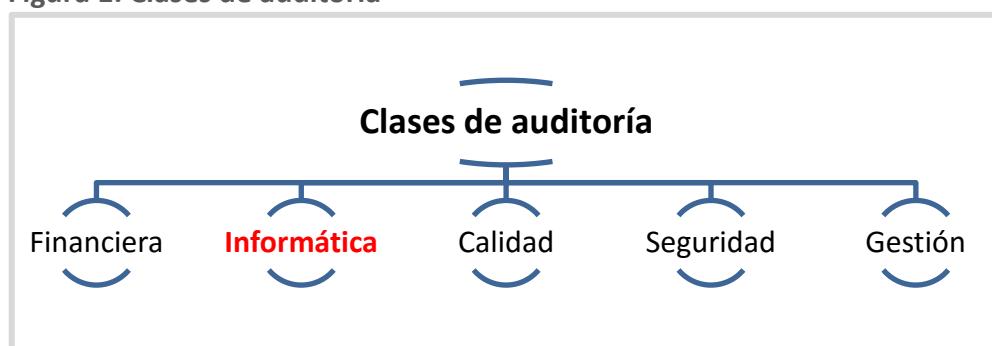
- **Auditoría de seguridad:** analiza los sistemas, principalmente los informáticos, y la capacidad de poder gestionar la seguridad de una forma que permita identificar y luego hacer las correcciones de las distintas vulnerabilidades que pudieran existir en la organización. Además, valida las medidas de protección que se llevan a cabo basadas en la política de seguridad y verifica que las reglas de esta política se apliquen correctamente.
- **Auditoría de calidad:** por una parte, verifica el cumplimiento del sistema de calidad existente y su efectividad. Por otra parte, verifica el nivel de cumplimiento a los requerimientos por parte de los servicios o productos elaborados, así como el grado de satisfacción de las necesidades de los clientes. En ambos casos, el objetivo es maximizar la efectividad del sistema auditado para conseguir un producto de calidad.
- **Auditoría informática:** evalúa los sistemas de información para verificar la integridad de los datos que administra y el cumplimiento tanto de los objetivos organizacionales, como de las políticas, estándares, normas y leyes vigentes. Se aplican procedimientos para auditar el uso y el mantenimiento del *software* y el *hardware* de la organización.
- **Auditoría de gestión:** es la combinación de la auditoría administrativa y a la auditoría operacional, las cuales son reemplazadas por la auditoría de gestión. Se enfoca en evaluar los objetivos, planes y políticas de toda la empresa y su cumplimiento. Controla la existencia y el correcto seguimiento de los métodos operacionales y la correcta administración de los recursos disponibles.



**Auditoría informática:** evalúa los sistemas de información para verificar la integridad de los datos que administra y el cumplimiento tanto de los objetivos organizacionales, como de las políticas, estándares, normas y leyes vigentes. Se aplica procedimientos para auditar el uso y el mantenimiento del *software* y el *hardware* de la organización.



**Figura 1: Clases de auditoría**

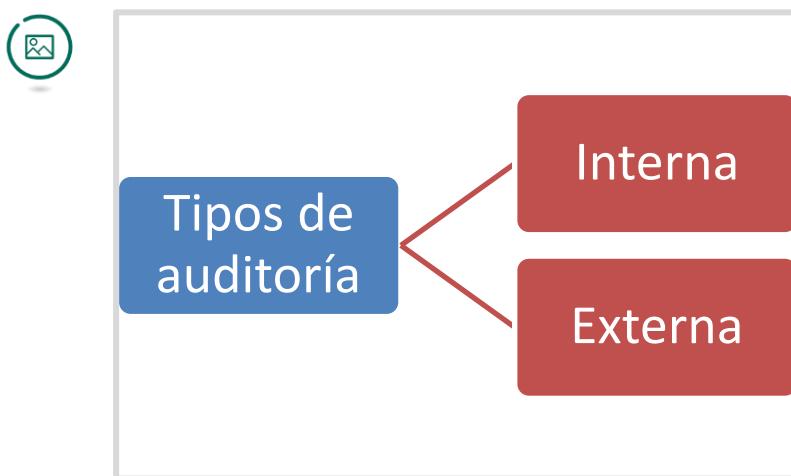


Fuente: elaboración propia.

## Tipos de auditoría

Dependiendo de la ubicación organizativa del auditor, es posible clasificar a la auditoría en dos categorías: interna y externa. La auditoría interna es generalmente realizada por personal de la misma organización que es auditada, mientras que la auditoría externa la efectúa otra organización contratada para tal fin y, generalmente, especializada en este tipo de actividades. Otra diferencia fundamental de la auditoría interna y de la externa son sus enfoques: **la externa busca expresar una opinión profesional independiente, habitualmente, sobre las cuentas de una entidad, mientras que el objetivo principal de la auditoría interna es comprobar y evaluar el cumplimiento de las normas y procedimientos establecidos para el control interno.**

Figura 2: Tipos de auditoría



Fuente: elaboración propia.

**La auditoría interna verifica el grado de exactitud en la observancia a las políticas, procedimientos, métodos, normas y leyes, así como el desempeño de todas las áreas de la estructura organizativa. Evalúa el trabajo del personal y el funcionamiento de los equipos y los sistemas.** Generalmente, la auditoría interna intenta encontrar e identificar pequeños inconvenientes antes que se conviertan en grandes problemas o sean descubiertos por los auditores externos.

**Mientras que en el caso de la auditoría externa, la realiza una empresa externa a la organización,** la cual es contratada para llevar a cabo este servicio. Se pueden encontrar varios beneficios que motivan a las organizaciones a buscar estas prestaciones. Uno de ellos es la **experiencia y el conocimiento que poseen las prestatarias**, puesto que son empresas

especializadas en auditorías. Ellas pueden efectuar la actividad en menor tiempo y de manera más eficiente que si lo hiciera internamente la organización con sus propios recursos.

Otro motivo para buscar una empresa de auditoría externa es que el juicio que ellos realicen no estará sesgado por presiones ni intereses internos, sino que será más objetivo y más real al momento de opinar sobre las tareas que deban corregirse en la organización.

En algunos casos, es un requisito legal, o en cumplimiento a una normativa, el hecho de que sea una empresa acreditada y externa quien efectúe la auditoría. Como es el caso de las normas ISO 9000 e ISO 14000 ya nombradas en la auditoría interna, o en industrias como la farmacéutica, alimenticia o financiera. En estos casos, el auditor externo actúa en calidad de regulador o inspector para confirmar que todos los requerimientos normativos sean cumplidos.

Se puede mejorar la efectividad de los procesos de auditoría al hacer uso de las fortalezas que poseen tanto los auditores internos como los externos. Por ejemplo, los auditores internos tienen un mejor entendimiento del trabajo y la cultura de la compañía, debido a que trabajan en ella y con este conocimiento, pueden ayudar a los auditores externos en sus visitas a ver cosas que ellos no verían por sí mismos. Los auditores externos trabajan con múltiples clientes, lo que les permite estar expuestos a una variedad de problemas y experiencias de diferentes organizaciones, por lo que se encuentran mejor preparados para descubrir y solucionar problemas en comparación con los auditores internos.

Al coordinar la labor de los auditores internos y externos se consigue un trabajo más eficiente, los auditores externos pueden generar esfuerzos duplicados si desconocen las tareas ya efectuadas por los auditores internos, o viceversa.

## Referencias

Blanco, E. L. J. (2005). *Auditoría y sistemas informáticos*. La Habana, CU: Editorial Félix Varela.

# Procedimientos de auditoría

---



Auditoría de  
Sistemas

UNIVERSIDAD  
**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**



# Procedimientos de auditoría

Para que una auditoría logre resultados acordes con los objetivos planteados, los procedimientos de auditoría deben basarse en la combinación de las técnicas de auditoría requeridas para la situación en particular.

Los procedimientos son el conjunto de las técnicas de auditoría a ser aplicados a los artefactos revisados en una actividad de auditoría. Se podría decir que las técnicas son las herramientas de trabajo de un auditor y los procedimientos son la combinación de estas herramientas, aplicadas a una situación en particular. Por lo tanto, si las técnicas no son las adecuadas, los procedimientos serán incorrectos y se fallará en el resultado final del trabajo de auditoría.

Asimismo, las técnicas de auditoría son los métodos disponibles para obtener el material de evidencia. Es decir que es el conjunto de métodos de investigación y prueba utilizados por el auditor para fundamentar, con evidencias, sus resultados, en forma de opiniones y conclusiones. Deben ser empleados dependiendo de las circunstancias y basándose en el criterio o juicio del auditor.



**Figura 1: Relación entre conceptos claves para la auditoría**



Fuente: elaboración propia.

## Técnicas de auditoría

En la etapa de ejecución, se ejecutarán los procedimientos definidos en la etapa de planificación de la auditoría. Estos procedimientos están compuestos por un conjunto de técnicas también seleccionadas en la etapa previa. Las técnicas son las herramientas que el auditor utiliza para obtener la evidencia necesaria, a fin de formar su juicio profesional. Existen algunas técnicas que son empleadas con más frecuencia que otras, dependiendo

del criterio o juicio del auditor sobre las circunstancias del momento. Podemos agrupar las técnicas de la siguiente manera:

**Verificación ocular:**

- Observación: es utilizada por el auditor para percibir los hechos o las circunstancias y la aplica en casi todas las etapas de la auditoría.
- Comparación: se refiere a focalizar la atención en distintos objetos con el fin de detectar sus relaciones de similitudes o diferencias.
- Rastro: en este caso, el auditor sigue una transacción durante todo procesamiento (desde su origen a su finalización).
- Revisión Selectiva: mediante una examinación visual, el auditor trata de discriminar aquellos temas habituales, de los que ameritan especial atención.

**Verificación verbal:**

- Indagación: se refiere a recopilar verbalmente información de distintas maneras (conversando, entrevistando, averiguando, etc). El inconveniente respecto a esta técnica, es que no representa una evidencia sólida.

**Verificación física:**

- Inspección: consiste en examinar activos y diversos tipos y clases de documentación con el fin de verificar que los mismos existen y que son auténticos.

**Verificación documental:**

- Comprobación: en estos casos, el auditor verificará la documentación que respalda como evidencia a una transacción u operación, de forma tal de poder demostrar que la misma es legal y que ha sido autorizada por el responsable correspondiente.
- Computación: se refiere a la verificación mediante cálculos matemáticos de la exactitud de las transacciones efectuadas.
- Análisis: en este caso el auditor aplicará distintos métodos analíticos para segmentar las transacciones que son objeto de su examen.
- Confirmación: se refiere a conseguir que un tercero (como fuente independiente respecto a la organización) responda ratificando o rectificando información (por ejemplo, el saldo de su cuenta).

## Ejemplos de procedimientos de auditoría

Los procedimientos hacen uso de las técnicas de auditoría para recolectar las evidencias. El siguiente ejemplo muestra algunos procedimientos que podrían componer una auditoría:

- 1) inspeccionar el inventario de la organización;
- 2) observar los procedimientos de producción, fabricación o desarrollo;
- 3) indagación para conocer la situación de los proyectos actualmente en desarrollo;
- 4) comprobar la legalidad de la documentación de tales proyectos.

Otra clasificación los divide en **procedimientos de control** y **procedimientos analíticos**.



Figura 2: Clasificación de procedimientos de auditoría



Fuente: elaboración propia.

**Procedimientos de control:** son los procedimientos que permiten atenuar el riesgo material, incluyendo el riesgo inherente y el riesgo de control. Se pueden realizar de tres formas:

- 1) al conocer el ambiente de la organización, con el propósito de lograr una evaluación razonable del riesgo material existente;
- 2) al conocer los procesos existentes de control interno de la organización;

- 3) al verificar la eficiencia operativa del control interno en la prevención y detección de errores materiales.

**Procedimientos analíticos:** son los procedimientos destinados a disminuir los riesgos analíticos, también denominados sustantivos. Son verificaciones detalladas y específicas de algún proceso o componente del sistema de información.

## Naturaleza de los procedimientos de auditoría

La naturaleza es el tipo de procedimiento que debe aplicarse a la circunstancia particular de la auditoría. En otras palabras, el auditor no puede utilizar los mismos métodos, técnicas y procedimientos en todas las situaciones por igual. Así también, hay ocasiones en las que el auditor debe aplicar varios métodos, técnicas o procedimientos a los mismos artefactos o conjunto de hechos para sustentar su opinión, es decir, usar procedimientos de distinta *naturaleza*. El auditor, de acuerdo con su criterio profesional, debe contar con flexibilidad en la toma de decisión en cuanto a qué procedimiento, o combinación de los mismos, aplicar a las situaciones particulares de cada auditoría.

## Alcance de los procedimientos de auditoría

**El alcance es la amplitud, intensidad y profundidad con que se realiza el procedimiento de auditoría.** Tiene su fundamento en que no siempre es posible revisar detalladamente todas las transacciones de una partida global en un análisis de auditoría. **Muchas veces las cantidades de operaciones de una organización son repetitivas y numerosas.** En estos casos, se debe tomar muestras representativas del conjunto para derivar el resultado global de la partida. En el campo de las auditorías, esto se denomina *pruebas selectivas*, y el porcentaje o la relación entre casos analizados en comparación con el total del universo es lo que se conoce como alcance o extensión del procedimiento de auditoría.

Es muy importante determinar correctamente el alcance durante las etapas de análisis y diseño, dado que si se considera un alcance muy reducido, se seleccionarán muestras de la población que no lograrán representar el comportamiento real del conjunto. O caso contrario, con un gran número de ejemplares a analizar, el tiempo y esfuerzo que deban emplearse resultará inviable económicamente para la organización.

Por ejemplo, en una organización dedicada al desarrollo de *software*, donde se lleva a cabo un número considerable de proyectos por trimestre y

donde cada proyecto tiene un tamaño tal, resulta físicamente imposible para un auditor examinar toda la documentación de cada uno de ellos en el tiempo asignado a la auditoría. En este caso, se deberán seleccionar solo algunos proyectos y sobre ellos analizar todos los ítems a ser verificados en la auditoría. El resultado se presentará como la opinión del auditor sobre todo el proceso de desarrollo de *software* de la organización, tal como si se hubiese revisado cada componente.

## Oportunidad de los procedimientos de auditoría

La oportunidad es la época o punto en el tiempo en que debe realizarse la auditoría. Dependiendo de la organización y del tipo de auditoría requerida, existen períodos de tiempo en que no es conveniente efectuar un procedimiento de auditoría. Es más, hay ocasiones donde resulta de mayor utilidad y se aplica mejor. Por ejemplo, luego de terminado un trimestre de proyectos y luego del cierre del año fiscal de la corporación.

## Procedimientos de auditoría. Organizaciones

Existen procedimientos de auditoría estándares, confeccionados por organizaciones internacionales de profesionales de la auditoría, tales como:

- **ISACA**: Asociación de Auditoría y Control de Sistemas de Información (*Information Systems Audits and Control Association*). Con sede en Chicago, E.E. U.U., desarrolla estándares para la auditoría de sistemas y brinda conocimientos y capacitación para auditores. Para más información se puede consultar en <http://www.isaca.org>. Algunos ejemplos de procedimientos publicados por ISACA son:
  - P3-Detección de intrusos.
  - P4-Virus y otros códigos maliciosos.
  - P6-Firewalls.
  - P8-Evaluación de la seguridad.
- **IIA**: El Instituto de Auditores Internos (*Institute of Internal Auditors*) elabora las GTAG, Guías de Auditoría de Tecnología Global. Para más información se puede consultar en: <http://theiia.org/technology>. La colección GTAG incluye, entre otras, las siguientes guías:
  - Guía 1: controles de tecnología de la información.
  - Guía 2: controles de gestión de parches y cambios: críticos para el éxito de la organización.
  - Guía 3: auditoría continua: implicancias para el aseguramiento, la supervisión y la evaluación de riesgos.
  - Guía 4: gestión de la auditoría de TI.
  - Guía 5: gestión y auditoría de riesgos de privacidad.

## Referencias

**Blanco, E. L. J.** (2005). *Auditoría y sistemas informáticos*. La Habana, CU: Editorial Félix Varela.

# Control interno informático

---



Auditoría de  
Sistemas

UNIVERSIDAD  
**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**



# Control interno informático

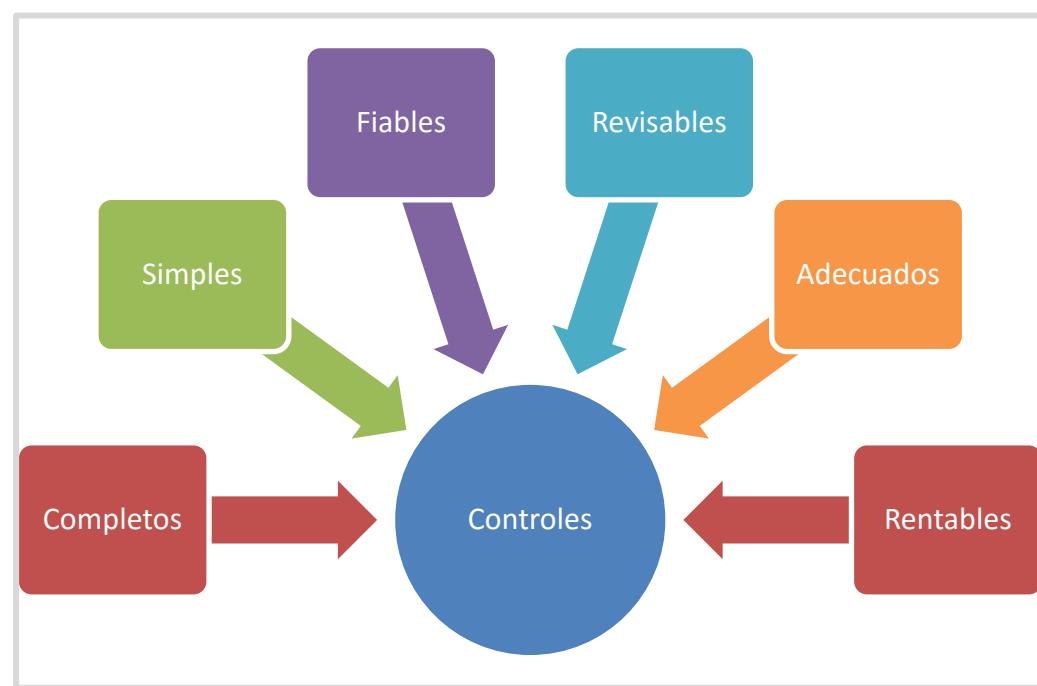
El control interno informático es un proceso constante de verificación que realiza la gerencia de sistemas para reducir el riesgo, mientras que la auditoría informática es una actividad en un punto particular del tiempo.

El concepto de control interno informático abarca políticas, prácticas, procedimientos y estructuras organizacionales diseñadas para brindar una seguridad razonable acerca de la consecución de los objetivos de negocio y la prevención (o detección y corrección) de aquellos eventos no deseados que pudieran comprometer el logro de dichos objetivos.

Es decir que el control interno se encarga de monitorear diariamente las actividades de los sistemas de información. Su función es verificar que se cumplan los procedimientos, las normas y los estándares definidos por la organización.

La gerencia (generalmente la gerencia de sistemas) es quien define ciertos requerimientos de alto nivel, que serán los objetivos a verificar por el control interno informático. Estos objetivos deben ser acciones específicas que la organización debe implementar para aumentar su valor y reducir su riesgo. Además, la gerencia debe decidir qué controles serán aplicados, cómo implementarlos (su frecuencia y alcance) y aceptar el riesgo de aquellos que se decide no implementar. Habitualmente, el personal del departamento de control interno depende jerárquicamente del departamento de sistemas de la organización.

**Figura 1: Características que deben poseer los controles**



Fuente: elaboración propia.

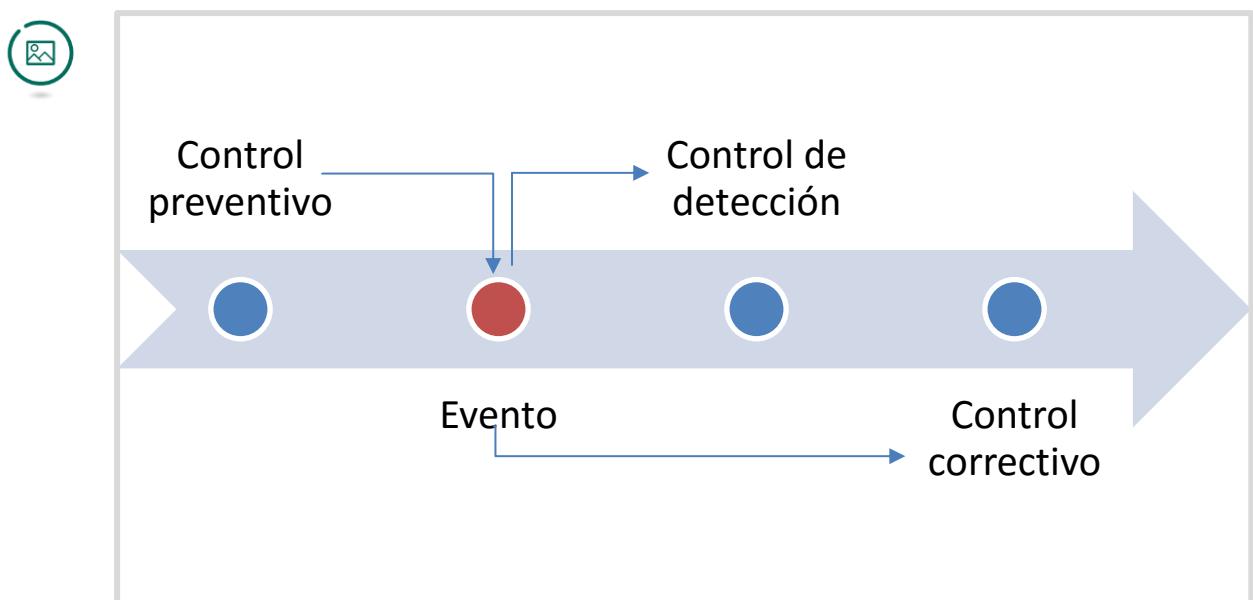
Los controles que se diseñen tienen que respetar determinados atributos de completitud, así como ser revisables, tener un grado de simplicidad que permita ser comprendidos, un adecuado nivel de confianza y una relación positiva en cuanto a costo y beneficios. La mayoría de los controles con los que cuentan las empresas son automáticos y vienen incluidos en las herramientas de *software* empresariales. Estos se vuelven cada vez más complejos a medida que aumentan las capacidades de los equipos informáticos. Sin embargo, existen controles que siguen siendo completamente manuales o algunos que son una combinación de procesos manuales y herramientas de *software* o *hardware*.

Podemos clasificar a los controles internos informáticos en tres categorías:

- **Controles preventivos:** se basan en evitar que ocurra una acción no deseada. Por ejemplo, la restricción de accesos por *software* a cierta información.
- **Controles de detección:** su función es dar a conocer y registrar la ocurrencia de algún evento. Por ejemplo, modificaciones a datos de producción por el personal de desarrollo o soporte.
- **Controles correctivos:** facilitan la vuelta a la actividad normal ante caídas del sistema, como son fallas en discos o suministro eléctrico.

Es importante destacar que los controles preventivos son orientados a reducir la probabilidad de ocurrencia de los riesgos, mientras que los controles de detección y correctivos se enfocan en reducir el impacto en el caso de que un evento de riesgo realmente ocurra.

**Figura 2: Línea de tiempo del momento en que actúa cada tipo de control**



Fuente: elaboración propia.

A continuación, se detalla una tabla, donde se incluyen ejemplos de controles preventivos, de detección y correctivos, para distintos tipos de activos de TI.

**Tabla 1: Ejemplos de distintos tipos de activos de TI y controles**



Tipos de activos informático	Controles preventivos	Controles de detección	Controles correctivos
<b>Aplicaciones</b>	Metodología de desarrollo	Reportes con totales de control	Procedimientos <i>rollback</i>
<b>Software de base</b>	Contraseñas complejas	Registros ( <i>Logs</i> ) de seguridad	Puntos de restauración
<b>Hardware</b>	Mantenimiento preventivo	Herramientas de diagnóstico	Soporte técnico para fallas
<b>Proveedores</b>	Casos de éxito previos	Revisiones a proveedores	Depósito de código fuente
<b>Telecomunicaciones</b>	<i>Firewalls</i>	IDS (detección de intrusiones)	Enrutamiento alternativo
<b>Instalaciones</b>	Guardias de seguridad	Cámaras de seguridad	Extintores de incendio
<b>Recursos Humanos</b>	Concientización en seguridad	Evaluación de desempeño	Esquema de sanciones
<b>Smartphones</b>	Encriptación con contraseña	Alertas por cambio de SIM	Localización remota

Fuente: elaboración propia.

Una característica interesante de los controles informáticos es que a medida que los sistemas han ido evolucionando, los controles internos pasaron a formar parte intrínseca de los productos de *software*, por lo que resulta difícil diferenciarlos de las características normalmente esperadas en los productos comerciales de administración TI. Por ejemplo, los podemos encontrar en los sistemas operativos para servidores de redes o también en el *software* de los equipos de comunicaciones. En muchos casos, un mismo grupo de métodos de control satisface a los tres tipos de controles descriptos.

## Objetivos del control interno

Los principales objetivos del control internos son:

- verificar que todas las actividades cumplan las normas (especialmente las legales) y los procedimientos establecidos;
- brindar asesoramiento sobre las normas a cumplir;
- ayudar y asesorar en las auditorías internas y externas;
- participar en el diseño, implantación y verificación de los mecanismos de control sobre los sistemas de información.

Los lugares donde se debe ejercer el control interno pueden incluir, entre otros, el control de cambios y versiones, producción, la calidad en el desarrollo de *software*, las redes de comunicación, el *software* de base, la seguridad informática, las licencias y los riesgos.

Dentro del control sobre la seguridad informática, podemos incluir asegurarse de que los usuarios del sistema, sus responsabilidades y sus perfiles se asignen y se mantengan adecuadamente. También, que se observen las normas de seguridad y de control de la información confidencial, así como el control dual de la información.

**¿Cuál es la relación entre el control interno y la auditoría informática?** En primera instancia, el área informática de la empresa define y monta los procesos que deben seguirse para mantener la integridad y la seguridad de los activos. Estos procedimientos deben ser obtenidos en base a una metodología apropiada para el tipo de organización y deben estar correctamente documentados y aprobados.

**El control interno se encarga de implementar los controles que verificarán que se empleen, en forma adecuada, los procesos definidos.**

**Finalmente, la auditoría evalúa cuál es el grado de control que existe realmente sobre los procesos informáticos.** En otras palabras, **identifica el nivel de exposición a los riesgos en los sistemas por la falta de controles y recomienda acciones correctivas para ellos.** Otra diferencia del control interno con la auditoría, es que el primero es un proceso constante de verificación y no solo una actividad en un punto particular del tiempo.

## Marcos de referencia de control interno

Los marcos de referencia son utilizados por la auditoría para describir a los sistemas de información, con un nivel de abstracción suficiente que le permita independizarse de la tecnología subyacente, de forma tal que el

modelo propuesto sea utilizable para diferentes organizaciones (ISACA, ITIL, ISO, etc.). Los *frameworks* brindan una descripción sistemática del control, por lo que consiguen facilitar la tarea de planificación y de supervisión en la labor de control y auditoría.

## Herramientas de control interno

Son instrumentos *hardware* y utilidades de *software* que deben manejar los profesionales de auditoría y control interno para verificar los sistemas informáticos. Es posible encuadrar a los marcos de referencia dentro de las herramientas de control.

## Materialidad por debilidad en el control

Las “Normas Generales para la Auditoría de los Sistemas de Información”, elaboradas por ISACA, establecen lo siguiente:

La debilidad en el control se considera “material” si la ausencia del mismo ocasiona que no exista una garantía razonable de que se cumplirá con el objetivo de control. Una debilidad clasificada como material implica que Los controles no están establecidos y/o no son utilizados y/o son inadecuados. Asimismo puede producir un escalamiento. Una debilidad material es una deficiencia importante o una combinación de deficiencias importantes que originan, con una probabilidad más que remota, que un evento indeseado no sea prevenido o detectado.

Existe una relación inversa entre materialidad y el nivel de riesgo de auditoría aceptable para el auditor de SI; es decir, cuanto mayor sea el nivel de materialidad, menor será la capacidad de aceptación del riesgo de auditoría, y viceversa. Esto permite al auditor de SI determinar la naturaleza, los plazos y el alcance de los procedimientos de auditoría lo cual será de suma utilidad para el Proceso de Auditoría. (ISACA, 2006, p.12, <https://goo.gl/PxdTyc>).

Basándose en la materialización para la planificación de las actividades del plan, el auditor puede identificar los objetivos de control que sean relevantes y determinar cuáles tienen que ser examinados (para más información, puedes consultar en la lectura del módulo 1 titulada Proceso de auditoría).



## Referencias

**Blanco, E. L. J.** (2005). *Auditoría y sistemas informáticos*. La Habana, CU: Editorial Félix Varela.

**IIA: Instituto de Auditores Internos:** <http://theiia.org/technology>

**ISACA Asociación de Auditoría y Control de Sistemas de Información, Normas Generales para la Auditoría de los Sistemas de Información, 2006, p.12,** <https://goo.gl/PxdTyc>

# Proceso de auditoría informática

---



Auditoría de  
Sistemas

UNIVERSIDAD  
**SIGLO 21** | MIEMBRO DE LA RED  
**ILUMNO**

# » Proceso de auditoría informática

El proceso de auditoría informática incluye, en forma habitual, actividades que se pueden agrupar en las siguientes etapas: planificación de la auditoría, ejecución o trabajo de campo, y conclusiones.

La asociación de contadores públicos de Estados Unidos, AICPA (*American Institute of Certified Public Accountants*), dedicada a desarrollar estándares técnicos y profesionales, ha adoptado el estándar **GAAS** (*Generally Accepted Auditing Standards*) para los profesionales que se dedican a las tareas de auditoría externa. Este modelo es el más conocido y de mayor aplicación en las auditorías financieras. Sin embargo, este estándar puede ser aplicado a la auditoría de sistemas de información con algunas adaptaciones necesarias. Resulta de mucha utilidad aplicar los principios descriptos por el GAAS en cualquier tipo de auditoría. Sus puntos principales son:

Estándares generales:

- 1) el auditor debe contar con la capacitación técnica y la competencia adecuada para realizar la auditoría;
- 2) el auditor debe mantener la independencia en la actitud mental en todos los aspectos relacionados con la auditoría;
- 3) el auditor debe ejercer la debida profesionalidad en el desempeño de la auditoría y en la preparación del informe.

Estándares de trabajo de campo:

- 1) el auditor debe contar con la capacitación técnica y la competencia adecuada para realizar la auditoría;
- 2) el auditor debe planear debidamente el trabajo y supervisar correctamente a cualquier asistente;
- 3) el auditor debe obtener la necesaria comprensión de la entidad y de su entorno, incluyendo su control interno;
- 4) a través de la ejecución de distintos procedimientos de auditoría, el auditor debe recopilar suficiente evidencia que le brinde un sustento adecuado para sus conclusiones respecto a lo auditado.

Estándares de presentación del informe:

- 1) El auditor deberá indicar en el informe si las declaraciones se presentan de conformidad con los principios aceptados por las mejores prácticas y normas aplicables.
- 2) Para la presentación del informe, el auditor debe especificar las cuestiones en que se hayan evidenciado inconsistencias respecto a los principios, relacionando el período actual y el anterior.
- 3) Cuando el auditor determina que la divulgación informativa no es razonablemente adecuada, debe hacerlo constar en el informe.

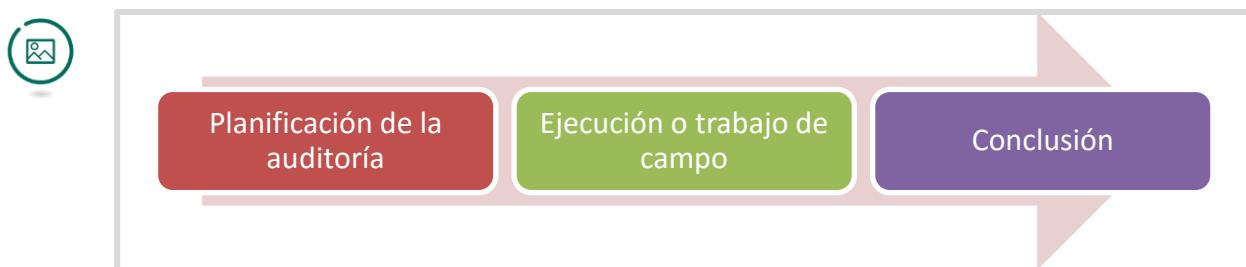
- 4) En el informe, el auditor debe expresar una opinión respecto a las declaraciones auditadas en su conjunto o declarar que una opinión profesional no puede ser expresada. Cuando el auditor no puede expresar una opinión general, debe exponer las razones de ello.

## Etapas del proceso de auditoría

Cada proceso de auditoría contiene particularidades en los procedimientos a seguir que dependen de la organización evaluada. Sin embargo, es habitual agrupar las diversas actividades en tres etapas principales:

- 1) **Planificación**: también llamada diagnóstico preliminar o programación. Algunas de sus actividades más importantes incluyen una visita previa con un diagnóstico preliminar, revisión de la documentación de auditorías anteriores, creación del plan de auditoría, redacción de cuestionarios de control interno y elaboración del programa de auditoría.
- 2) **Ejecución o trabajo de campo**: sus actividades abarcan el análisis de la organización-cliente con su sistema de control interno, la aplicación de los procedimientos de auditoría, la elaboración de los papeles de trabajo y la comunicación constante con la dirección.
- 3) **Conclusión**: informe de resultado o reporte de la auditoría. Incluye la preparación y presentación de un informe borrador sobre hallazgos y recomendaciones, así como la presentación del reporte final que contendrá un detalle de los hallazgos y las recomendaciones respectivas.

**Figura 1: Proceso de auditoría informática**



Fuente: elaboración propia.

## Etapa de planificación de auditoría

El documento de la norma S5 *Norma de Auditoría de SI Planeación* (ISACA) establece que el auditor de SI (Sistemas de Información) debe:

Planear la cobertura de la auditoría de sistemas de información para cubrir los objetivos de la auditoría y cumplir con las leyes aplicables y las normas profesionales de auditoría.

Desarrollar y documentar un enfoque de auditoría basado en riesgos.

Desarrollar y documentar un plan de auditoría que detalle la naturaleza y los objetivos de la auditoría, plazos, alcance y recursos requeridos.

Desarrollar un programa y/o plan de auditoría detallando naturaleza, plazos y alcance de procedimientos requeridos para la auditoría. (ISACA, 2006, p.5, <https://goo.gl/PxdTyc>).

**La primera tarea que se debe realizar en un proceso de auditoría es establecer el contrato o acuerdo entre el auditor y la organización**, donde sus términos y características dependerán del tipo de auditoría (interna o externa) y la forma de trabajo de la organización auditada.

Sin embargo, en cada caso, **debe definirse claramente cuál será el alcance y el objetivo del trabajo**, deben asentarse por escrito temas como la profundidad, la independencia y los entregables de la auditoría con fechas específicas. Además, debe definirse con cuánta responsabilidad contará el auditor y cuál será el nivel autoridad que tendrá para examinar la información corporativa.

Una vez cerrado el acuerdo para que se realice la auditoría, el auditor debe lograr un entendimiento de la organización y del entorno en que se encuentra, reuniendo información acerca de la naturaleza de los sistemas de información, su administración, gobierno, objetivos, estrategias y procesos de negocio. Debe revisar, en forma preliminar, las aplicaciones que sean significativas para obtener los datos a ser auditados. Esta información debe servirle de base al auditor para diseñar el plan de auditoría.

Especialmente, la información recolectada debe ser de utilidad para conocer los riesgos de la auditoría. Los principales riesgos a considerar incluyen: no contar con la información suficiente para lograr una opinión profesional representativa de la realidad, el hecho de que la corporación no pueda cumplir con sus objetivos de negocio y por último, la capacidad con que cuenta la empresa para responder a ellos. En este punto, el auditor realiza un juicio preliminar sobre los riesgos del cliente con el fin de establecer el alcance de la auditoría y poder planificarla. **El riesgo de auditoría es el riesgo de llegar a una conclusión errónea en base a los resultados de la auditoría. Los distintos tipos son:**

- **Riesgo inherente:** es la posibilidad de que las áreas auditadas contengan errores que puedan materializarse en fallas, independientemente de la existencia de los sistemas de control. Este riesgo se encuentra totalmente fuera del control del auditor y es propio de la operatoria del

ente. Un ejemplo de riesgo inherente es la existencia en el sistema de una numerosa devolución de un producto o de activos superados por la tecnología que le quiten competitividad a la empresa.

- **Riesgo de control:** se refiere a que existan errores materializados que no hayan podido ser prevenidos ni detectados, debido a fallas o debilidades en los controles realizados. Por ejemplo, la inexistencia de procedimientos de autorización.
- **Riesgos de detección:** es el riesgo de que una falla no sea detectada por aplicar incorrectamente un procedimiento por parte del auditor.

Con la estimación de los riesgos, el auditor está en una mejor posición para justificar y cuantificar los recursos del plan de auditoría. Además, contando con el conocimiento obtenido de los riesgos, se pueden priorizar las áreas y procesos a revisar en la auditoría.

Una vez entendida la naturaleza de las actividades de la organización y conocidos los riesgos presentes, el entorno y los objetivos de la auditoría, el auditor prepara el plan de auditoría. Este plan es el marco de referencia para todas las actividades de la auditoría. El auditor debe asegurarse de que sea diseñado de la manera más efectiva y eficiente posible y debe abarcar los sistemas de información y sus objetivos, además de cumplir con las leyes y estándares profesionales de auditoría. Finalmente, el plan deberá ser aprobado por un comité de auditoría, si se ha formado, o por la gerencia interesada en el proceso.

Resumiendo, el plan contiene el entendimiento del auditor sobre el cliente, los riesgos potenciales, un presupuesto de cómo se utilizarán los recursos y los procedimientos de auditoría a seguir. El plan detalla los objetivos de la auditoría y todos los pasos necesarios para asegurar que los asuntos importantes serán cubiertos. Este plan resulta de ayuda fundamental para que el auditor pueda tener éxito en su proceso.

## Etapa de ejecución de la auditoría

En esta etapa, el auditor comienza su trabajo de campo. Para ello, diseña, selecciona, evalúa y documenta evidencias de la entidad analizada para cumplir el objetivo de la auditoría. **Estas evidencias tienen que cumplir con las cualidades de ser suficientes, confiables y relevantes**, a fin de que puedan ser correctamente interpretables y sean capaces de soportar adecuadamente el análisis del auditor. Una vez llegado a este punto, el auditor está capacitado para plasmar sus conclusiones sobre los hallazgos, en un informe. El estándar S6 de ISACA para la ejecución de la auditoría establece estos conceptos claves:

**Supervisión**—El personal de auditoría de SI debe ser supervisado para

brindar una garantía razonable de que se lograrán los objetivos de la auditoría y que se cumplirán las normas profesionales de auditoría. Evidencia—Durante la ejecución, el auditor de SI debe obtener evidencia suficiente, confiable y pertinente para alcanzar los objetivos de auditoría. Los hallazgos y conclusiones de la auditoría deberán ser soportados mediante un apropiado análisis e interpretación de dicha evidencia. Documentación—El proceso de auditoría deberá documentarse, describiendo las labores de auditoría realizadas y la evidencia de auditoría que respalda los hallazgos y conclusiones del auditor de SI. (ISACA, 2006, p.6, <https://goo.gl/PxdTyc>).

Todos los integrantes del equipo de auditoría deben tener definidos sus roles y responsabilidades antes de iniciarse el proceso. Deben saber exactamente cuáles serán las actividades que deberán llevar a cabo y cuál será el grado de decisión que tendrán. Cada actividad de la auditoría debe seguir los procedimientos descriptos y documentados en el plan de auditoría. Esta información será de utilidad en aspectos como los objetivos y alcances de las tareas o del programa de pasos a seguir.

Al momento de efectuar cada actividad de la auditoría, se deben registrar los detalles de las tareas realizadas en los documentos preestablecidos en el plan. También, los datos de las tareas, las decisiones tomadas, los pasos efectuados y los resultados obtenidos. Las buenas prácticas de auditoría recomiendan que cada documento sea revisado por otro miembro del equipo de auditoría para evitar errores y mejorar la calidad del trabajo. La cantidad de documentación registrada y su nivel de detalle debe ser de una calidad tal, que una tercera empresa pueda tomar los mismos documentos y llegar a las mismas conclusiones y resultados, realizando nuevamente los procedimientos de auditoría.

### **Etapa de conclusión de la auditoría**

Esta es la última etapa de la auditoría, en donde el auditor analiza las evidencias recolectadas, alcanza las conclusiones y documenta e informa los resultados de los procedimientos de la auditoría en el reporte. El reporte de auditoría es el objetivo final de todos los procedimientos efectuados en la auditoría. Esta es la comunicación formal del auditor al cliente sobre la auditoría, con sus resultados y conclusiones.

El auditor separa las evidencias significativas, evaluadas por su relevancia e importancia. Se realiza el análisis profesional y ético de sus vinculaciones con los riesgos detectados, de acuerdo con el saber y entender del auditor informático. Es recomendable que el reporte que se confeccione sea claro, adecuado, suficiente y comprensible, y que esté escrito en un lenguaje

técnico informático. Su extensión y profundidad debe cubrir las expectativas de la gerencia. Con el reporte del auditor, el cliente debe ser capaz de realizar los cambios necesarios para lograr sus objetivos de control. (Para más información, puede consultar en la lectura del módulo 2 titulada Informe del auditor.)

## Referencias

**Blanco, E. L. J.** (2005). *Auditoría y sistemas informáticos*. La Habana, CU: Editorial Félix Varela.

**IIA: Instituto de Auditores Internos:** <http://theiia.org/technology>.

**ISACA Asociación de Auditoría y Control de Sistemas de Información, Normas Generales para la Auditoría de los Sistemas de Información, 2006, p.5-6,** <https://goo.gl/PxdTyc>

# Control interno

---



Auditoría de  
Sistemas

UNIVERSIDAD

**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**

# » Control interno

El control interno es un medio por el cual los recursos de una organización son dirigidos, supervisados y medidos. Es importante para prevenir y detectar fraudes y para proteger los recursos de la organización.

De acuerdo con el *Committee of Sponsoring Organizations of the Treadway Commission* de los Estados Unidos (COSO), a través del documento denominado *marco integrado*, conocido como el Modelo de Control COSO, se define al control interno como un proceso efectuado por la junta directiva de la entidad, por la administración y por otro personal, diseñado para proporcionar a la administración un aseguramiento razonable con respecto al logro de:

- los objetivos en efectividad y eficiencia de las operaciones;
- confiabilidad de los reportes financieros;
- cumplimiento de las leyes y reglamentos aplicables.

Entre algunas consideraciones a tener en cuenta con respecto al control, se puede indicar que **el control interno es solo un proceso, no un fin en sí mismo**. El control interno no es meramente documentación en los manuales de políticas, sino que existe para el uso del personal en todos los niveles de la organización. El control interno puede proveer solo un aseguramiento razonable, no un aseguramiento absoluto sobre una entidad. En fin, el control interno se enfoca en el cumplimiento de objetivos en una o más categorías separadas, pero superpuestas.

## Qué puede hacer el control interno

**El control interno puede ayudar a una entidad a alcanzar sus metas de rendimiento y de rentabilidad y prevenir la pérdida de sus recursos.** Puede contribuir a garantizar una información financiera fiable y a asegurar que la empresa cumple con las leyes y regulaciones, evitando daños a su reputación y otras consecuencias. Por último, puede ayudar a una organización a llegar a donde quiere ir y evitar problemas e inconvenientes en el camino.

## Qué no puede hacer el control interno

Lamentablemente, algunas personas tienen expectativas poco realistas. Buscan absolutos, creyendo que el control interno puede, por sí solo, asegurar el éxito de una organización, es decir, garantizar el logro de los objetivos de negocio básicos o, al menos, asegurar su supervivencia. Aunque sí es cierto que un control interno efectivo, por su propia cuenta, puede ayudar a una organización a alcanzar estos objetivos y puede proporcionar información de gestión sobre el progreso de la organización, o falta de ella.

No puede, sin embargo, transformar un gerenciamiento inherentemente pobre en uno bueno de un momento para otro. Asimismo, los cambios en la

política o programas del gobierno, las acciones de los competidores o las condiciones económicas se encuentran fuera del control gerencial. Por lo tanto, el control interno no puede garantizar el éxito o incluso la supervivencia.

También, la declaración que indica que el control interno puede garantizar la fiabilidad de la información financiera y el cumplimiento de las leyes y regulaciones no es totalmente garantida. No importa qué tan bien esté concebido y operado un sistema de control interno; en todo caso, puede proporcionar garantía solo razonable, no absoluta, a la gerencia y dirección, relativa a la consecución de los objetivos de la organización, dado que existen limitaciones inherentes a todos los sistemas de control interno. Por ejemplo, que los juicios en la toma de decisiones pueden ser defectuosos y que los desperfectos pueden ocurrir debido a simple error o equivocación.

Otro factor limitante es que el diseño de un sistema de control interno debe reflejar el hecho de que hay limitaciones de recursos, y los beneficios de los controles deben ser considerados en relación con sus costos. Así, mientras que el control interno puede ayudar a una organización a alcanzar sus objetivos, el control interno no es una panacea.

## Componentes del marco COSO para el control interno

El *framework* COSO consta de cinco partes componentes:

**Figura 1: Componentes del marco COSO para el control interno**



Fuente: Adaptado de COSO Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2013.

Estos componentes están interrelacionados y para ser efectivos, deben estar institucionalizados en la organización, es decir, ser parte de sus procesos administrativos cotidianos.

## Ambiente de control

El ambiente o entorno de control establece el tono de una organización e influye en la conciencia de control de su personal. Es la base para todos los demás componentes del control interno y proporciona disciplina y estructura. Busca estimular las actividades del personal con respecto a su control. Los factores de control del entorno incluyen:

- la integridad y los valores éticos del personal;
  - la competencia de las personas de la organización;
  - la filosofía de gestión y el estilo de operación;
  - la manera en que los gerentes asignan autoridad y responsabilidad, y organizan y desarrollan su personal;
  - la atención y la orientación proporcionada por el consejo directivo.
- (Migdalia, 2008)

## Evaluación de riesgos

Cada organización debe enfrentarse a diversos riesgos de fuentes externas e internas que requieren ser evaluados. Una condición fundamental previa para la evaluación de riesgos es el establecimiento de objetivos, relacionados entre sí e internamente consistentes. La evaluación de riesgos consiste en identificar y analizar los riesgos vinculados con el éxito en alcanzar los objetivos, generando una base para definir cómo los riesgos deben ser gestionados. (Migdalia, 2008)

Por lo tanto, la primera tarea que propone el *framework* es establecer los objetivos para todos los niveles de la organización. Conocidos los objetivos, se puede tener una base para identificar y analizar los factores de riesgos que pueden amenazar su consecución. De aquí la importancia de poseer una base sólida para el control interno efectivo, es decir, poseer criterios de evaluación y monitoreo de los riesgos identificados como probables.

## Actividades de control

Las actividades de control son las políticas y los procedimientos que ayudan a garantizar que las directivas gerenciales sean llevadas a cabo. Estas actividades también avalan las medidas necesarias para hacer frente a los riesgos, para la consecución de los objetivos de la organización. Las actividades de control se producen en toda la organización, en todos los niveles y en todas las funciones. Estas incluyen una amplia gama de tareas tan diversas como aprobaciones, autorizaciones, verificaciones,

conciliaciones, revisiones de desempeño operativo, seguridad de los activos y segregación de funciones.

Otras actividades de vital importancia son la protección de los recursos, la distribución de responsabilidades, el monitoreo continuo y la capacitación necesaria. Las actividades de control son de características diferentes: algunas pueden estar automatizadas, otras se realizan en forma manual, pueden ser preventivas o correctivas, generales o específicas, globales o de algún área en particular.

El informe COSO provee características a considerar en los controles de los sistemas de información. Estas abarcan los siguientes puntos:

- Controles generales: estos controles buscan garantizar la operatoria continua de la entidad y verifican los sectores de procesamiento de datos, seguridad lógica y física, administración de *hardware* y *software*. Además, comprenden las actividades de desarrollo de sistemas, mantenimiento y soporte, las bases de datos y las comunicaciones.
- Controles de aplicativos: se enfocan en las aplicaciones que corren en los sistemas de información. Verifican los mecanismos de autorización y validación e interfaces de intercambio de datos con otros sistemas.

## Información y comunicación

La información es el componente principal y vital para poder controlar y administrar una organización y poder tomar las decisiones correctas, utilizando los recursos adecuados. **La información debe ser oportuna, clara, asequible, relevante, completa y fidedigna.**

La información pertinente debe ser identificada, capturada y comunicada en forma y tiempo, a fin de permitir al personal de una entidad cumplir con sus responsabilidades. Los sistemas de información producen reportes que contienen información de los aspectos operativos, financieros y de cumplimiento regulatorio, que hacen posible poner en funcionamiento y controlar el negocio. Tratan no solo con los datos generados internamente, sino también con información acerca de los acontecimientos externos, actividades y condiciones necesarias para la toma de decisiones de negocio. (Migdalía, 2008)

Asimismo, los sistemas de información, actuando como sistemas de control, juegan una función muy importante para el éxito de la organización, al apoyar la implementación de las estrategias corporativas diseñadas por la dirección. Esto es posible debido a que los sistemas de información se encuentran integrados en las operaciones cotidianas de las empresas. Esta

integración posee distintos grados de complejidad, dependiendo de la organización donde se apliquen.

El sistema de comunicación de la organización es otro apartado indicado por el informe COSO. La comunicación efectiva también debe ocurrir en un sentido más amplio, fluyendo hacia abajo, hacia arriba y a través de la organización. También es necesaria la comunicación efectiva con las partes externas como clientes, proveedores y accionistas, conjuntamente con las entidades reguladores públicas que deben obtener información sobre las operaciones de la empresa, incluso el desempeño del sistema de control, por ejemplo, en las entidades financieras.

## Monitoreo. Supervisión y seguimiento

**Los sistemas de control interno deben ser supervisados y monitoreados**, es decir que se debe contar con un proceso que evalúe la calidad del desempeño del sistema en el tiempo. Esto se logra a través de actividades de monitoreo continuo, evaluaciones puntuales o una combinación de ambas.

El monitoreo continuo se produce en el curso de las operaciones, por ejemplo:

- documentación de autorizaciones, aprobaciones, informes, reportes;
- comprobación de los registros frente a la existencia física del bien;
- informes de auditorías, contaduría, diagnósticos;
- reportes generados por entidades externas;
- revisiones de operaciones relacionadas con efectividad de los controles;
- detección de fraudes internos o externos.

El siguiente componente se refiere a evaluaciones que se realizan en determinados momentos específicos. Estas actividades brindan valiosa información a la dirección sobre la efectividad del sistema de control. Deben poseer independencia, objetividad y enfocarse en medir la efectividad de los controles. El alcance y la frecuencia de las evaluaciones puntuales dependerán principalmente de la evaluación de los riesgos y la efectividad de los procedimientos de monitoreo y supervisión continua.

El tercer componente es una combinación del monitoreo y las evaluaciones. En ese caso, todo lo referido al sistema de control interno se interrelaciona con las operaciones habituales de la organización y tiene más efectividad cuando dichos controles se integran en la infraestructura de la organización, conformando una parte de la esencia misma de la empresa. (Migdalia, 2008)



## Referencias

**Blanco, E. L. J.** (2005). *Auditoría y sistemas informáticos*. La Habana, CU: Editorial Félix Varela.

**The Committee of Sponsoring Organizations of the Treadway Commission COSO (2013).** *Componentes del Control Interno*. <http://www.coso.org>.

**Magdalia, D.** (2008). Sistema de Control Interno - Auditoría. Recuperado de: <http://www.monografias.com/trabajos63/control-interno-auditoria/control-interno-auditoria2.shtml>

# Objetivos de control COBIT

---



Auditoría de  
Sistemas

UNIVERSIDAD  
**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**



# Objetivos de control. COBIT

COBIT 5 incluye una colección publicada de complementos para fines específicos: riesgos, auditoría, seguridad de la información, gestión de proveedores, revisión de modelo de madurez, *cloud computing*, etcétera.

Los Objetivos de Control pueden definirse como un resultado que se desea lograr a partir de procedimientos de control específicos implementados en una actividad de TI (Tecnología Informática).

## COBIT. Objetivos de control para la TI

Existen marcos de referencia con objetivos de control para la TI (Tecnología Informática), tales como COBIT (*Control Objectives for Information and Related Technology*), el que fue creado por la asociación profesional ISACA, fundada en Estados Unidos en 1967 por un grupo de profesionales que trabajaban en controles de auditoría para sistemas de computación.

Ellos se dieron cuenta de la importancia de su función para sus organizaciones y de la necesidad de contar con información y guía centralizada en la materia. El grupo se formalizó primeramente con el nombre de EDP Auditor Association (Asociación de auditores de procesamiento electrónico de datos), con Stuart Tyrnauer como su director. En 1976, la asociación formó una fundación educativa para enfocar sus esfuerzos en investigaciones de gran escala y así, expandir el conocimiento y el valor del campo del IT Governance y del control interno.

En la actualidad, ISACA cuenta con más de 115,000 miembros con certificaciones ISACA en más de 180 países. Sus miembros son auditores de sistemas, consultores, educadores, profesionales de seguridad de sistemas, entre otros similares, en distintos niveles gerenciales de las organizaciones.

Existen 170 capítulos de ISACA establecidos en 160 países que proveen educación, recursos, red de contactos y otros beneficios. Además, ISACA realiza eventos, conferencias y desarrolla estándares, aseguramiento y seguridad para que sus miembros puedan aprender de las experiencias de los demás e intercambiar puntos de vistas en diversos temas e industrias. ISACA también publica la revista técnica *ISACA Journal*, dedicada al campo del control informático.

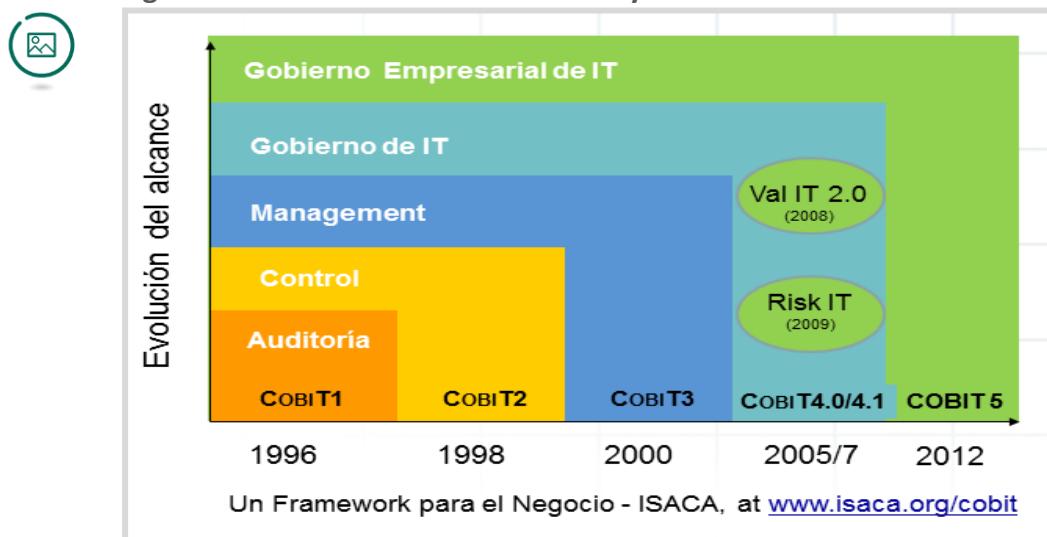
ISACA brinda una certificación reconocida internacionalmente como CISA (*Certified Information Systems Auditor*), orientada a auditores de sistemas de información, para mantener sus habilidades y monitorizar la efectividad de los programas de mantenimiento. Esta certificación ha sido formalmente aprobada por el Departamento de Defensa de los Estados Unidos, en la categoría de *aseguramiento de información técnica*. La poseen más de 115,000 profesionales en todo el mundo, de los cuales 2,440 corresponden a residentes de Latinoamérica.

En 1996, ISACA organizó ISACF (*Information System Audit and Control Foundation*), una organización internacional sin fines de lucro, para llevar a cabo investigaciones y dar a conocer los nuevos avances en la materia de control y gestión de las tecnologías de los sistemas de información e informar a los usuarios tecnológicos sobre la importancia del control interno en todas las organizaciones. ISACF publicó la primera versión del estándar COBIT en 1996, hoy mantenido por ITGI (IT Governance Institute). Este producto ha sido diseñado, principalmente, como una fuente de instrucción para los profesionales dedicados a las actividades de control.

COBIT proporciona un conjunto de objetivos de control aceptados por los gerentes de negocios y auditores, contribuyendo al desarrollo de un marco para la gestión, al comprender su sistema de información y poder determinar el nivel adecuado de seguridad y de control que se requiere para proteger a los activos de la organización.

En el año 2013, ISACA publicó la nueva versión de COBIT, denominada COBIT 5, producto de una *task force* global y de un equipo de desarrollo de ISACA. Fue revisado por un centenar de expertos a nivel mundial y se trató del cambio más significativo en los 16 años de historia del *framework* por excelencia, relacionado con objetivos de control de TI.

**Figura 1: Evolución histórica de COBIT y su alcance**



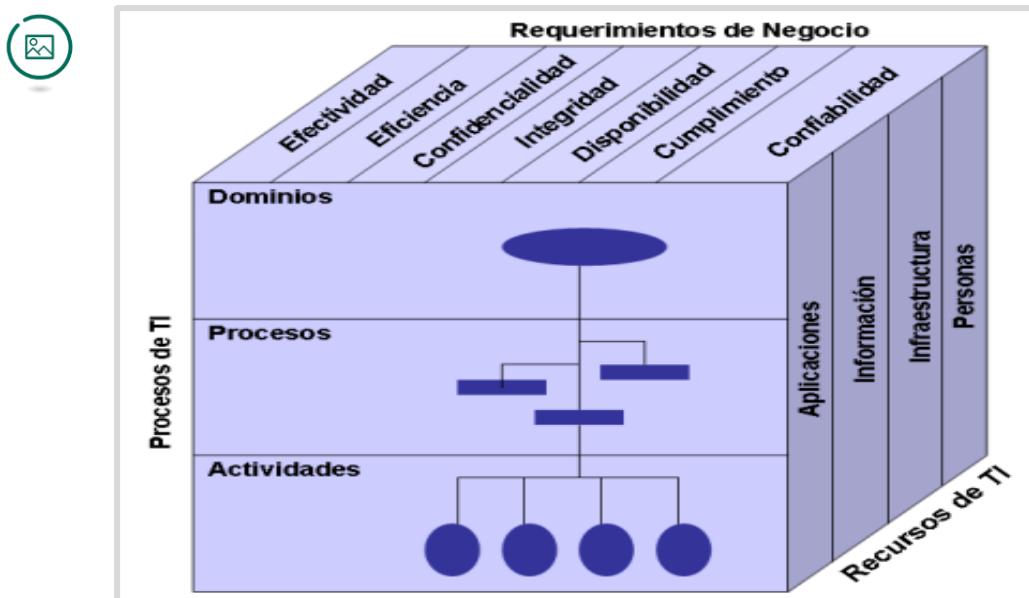
Fuente: ISACA, (2012), [www.isaca.org](http://www.isaca.org)

En la actualidad, numerosas organizaciones de Latinoamérica aún utilizan la versión de COBIT 4.1, a los fines de realizar auditorías de sistemas, debido a las siguientes características destacadas:

- Es ampliamente aceptado como marco de trabajo metodológico

- Fue utilizado como base para distintas regulaciones de diversas industrias en la mayor parte de Latinoamérica.
- Es de libre descarga, sin costo, desde el sitio web de ISACA ([www.isaca.org](http://www.isaca.org))
- Incluye 34 procesos con sus actividades y objetivos de control.
- Los objetivos de control de sus procesos están orientados a asegurar siete criterios de la información relacionados con requerimientos del negocio:
  - La **efectividad** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
  - La **eficiencia** consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
  - La **confidencialidad** se refiere a la protección de información sensitiva contra revelación no autorizada.
  - La **integridad** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
  - La **disponibilidad** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
  - El **cumplimiento** tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
  - La **confiabilidad** se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno. (IT Governance Institute, 2007, p. 10)
- Los procesos se encuentran agrupados en cuatro dominios:
  - **Planificación y Organización:** Proporciona dirección para la entrega de soluciones y la entrega de servicio.
  - **Adquisición e Implementación:** Proporciona las soluciones y las pasa para convertirlas en servicios.
  - **Entrega y Soporte:** Recibe las soluciones y las hace utilizables por los usuarios finales.
  - **Supervisión y Evaluación:** Supervisa todos los procesos para asegurar que se sigue la dirección provista. (IT Governance Institute, 2007, p. 12)
- Abarca los siguientes recursos relacionados con la TI:
  - aplicaciones;
  - información;
  - infraestructura;
  - personas.

Figura 2: El cubo que resume las características de COBIT 4.1



Fuente: ISACA. (2007). El Cubo de COBIT. [www.isaca.org](http://www.isaca.org)

El *framework* COBIT se basa en el hecho de que, para proporcionar la información que la empresa requiere para satisfacer sus necesidades y objetivos, debe invertir en administrar y controlar los recursos TI, usando procesos estructurados que provean la información de negocio requerida. El *framework* COBIT brinda herramientas para ayudar a las organizaciones a satisfacer sus requerimientos de negocio. A continuación, se detalla la totalidad de los procesos incluidos en COBIT:

- Planificación y organización:
  - PO1 Definir un Plan Estratégico de TI
  - PO2 Definir la Arquitectura de la Información
  - PO3 Determinar la Dirección Tecnológica
  - PO4 Definir los Procesos, Organización y Relaciones de TI
  - PO5 Administrar la Inversión en TI
  - PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia
  - PO7 Administrar Recursos Humanos de TI
  - PO8 Administrar la Calidad
  - PO9 Evaluar y Administrar los Riesgos de TI
  - PO10 Administrar Proyectos. (IT Governance Institute, 2007, p. 28)
- Adquisición e implementación:

- AI1 Identificar soluciones automatizadas
  - AI2 Adquirir y mantener software aplicativo
  - AI3 Adquirir y mantener infraestructura tecnológica
  - AI4 Facilitar la operación y el uso
  - AI5 Adquirir recursos de TI
  - AI6 Administrar cambios
  - AI7 Instalar y acreditar soluciones y cambios. (IT Governance Institute, 2007, p. 72)
- Entrega y soporte:
    - DS1 Definir y administrar los niveles de servicio
    - DS2 Administrar los servicios de terceros
    - DS3 Administrar el desempeño y la capacidad
    - DS4 Garantizar la continuidad del servicio
    - DS5 Garantizar la seguridad de los sistemas
    - DS6 Identificar y asignar costos
    - DS7 Educar y entrenar a los usuarios
    - DS8 Administrar la mesa de servicio y los incidentes
    - DS9 Administrar la configuración
    - DS10 Administrar los problemas
    - DS11 Administrar los datos
    - DS12 Administrar el ambiente físico
    - DS13 Administrar las operaciones. (IT Governance Institute, 2007, p. 100)
  - Monitorear: supervisión y evaluación:
    - ME1 Monitorear y Evaluar el Desempeño de TI
    - ME2 Monitorear y Evaluar el Control Interno
    - ME3 Garantizar el Cumplimiento Regulatorio
    - ME4 Proporcionar Gobierno de TI. (IT Governance Institute, 2007, p. 152)

A continuación, se presenta un cuadro resumen con las principales diferencias entre la versión 4.1 de COBIT y la nueva versión 5, publicada por ISACA.

**Tabla 1: Principales diferencias entre las versiones 4.1 y 5 de COBIT**



COBIT 4.1	COBIT 5
COBIT 4.1 (4 Dominios y 34 Procesos)	COBIT 5 (5 Dominios y 37 procesos)
Risk IT (3 Dominios y 9 Procesos)	
Val IT 2.0 (3 Dominios y 22 procesos)	
Planear y Organizar (10 procesos)	Alinear, Planear y Organizar (13 procesos)
Adquirir e Implementar (7 procesos)	Construir, Adquirir e Implementar (10 procesos)
Entrega de Servicio (13 procesos)	Entregar Servicio y Soportar (6 procesos)
Monitorear y Evaluar (4 procesos)	Monitorear y Evaluar (3 procesos)
Pentágono de Gobierno de TI	Dominio de Gobierno de TI (5 procesos)
Objetivos de Control de COBIT 4.1	Prácticas de Gobierno y/o Management
Prácticas de Control de COBIT 4.1 (por Obj.Control)	Actividades por cada Práctica de Gobierno/Management
Inputs y Outputs a nivel de Proceso	Inputs y Outputs a nivel de Práctica de cada Proceso
Matriz RACI con 11 Roles	Matriz RACI por Práctica ampliada con 26 Roles
Enfoque basado en Procesos	Enfoque basado en Facilitadores (incluyendo Procesos)
Gobierno de TI	Gobierno Empresarial de TI (GEIT alineado con ISO 38500)
Nivel más alto: Las Metas de Negocio	Nivel más alto: Necesidades de los Stakeholders
Mapeo entre Perspectivas (BSC), Metas del Negocio, Metas de TI y Procesos	Mapeo entre Perspectivas (BSC), Objetivos de Gobierno, Necesidades de los Stakeholders, Metas de la Empresa, Metas de TI y Procesos (Modelo de Objetivos en Cascada)
Métricas a nivel Actividades, Procesos y Metas de TI	Métricas (a nivel Prácticas) de Procesos y Metas de TI
Modelo de Madurez (CMM)	Modelo de Capacidad basado en ISO 15504 (diferente escala, más exigente y se podrá certificar), COBT PAM para COBIT4.1
7 Criterios de la Información	Modelo de Información con Criterios adicionales

Fuente: Adaptado de ISACA, 2012.

## Referencias

**Blanco, E. L. J.** (2005). *Auditoría y sistemas informáticos*. La Habana, CU: Editorial Félix Varela.

**IT Governance Institute (2007)**, COBIT 4.1, p. 10-12

**ISACA**, (2012), Evolución del alcance de COBIT, Recuperado de [www.isaca.org](http://www.isaca.org)

**ISACA**, (2007), El Cubo de COBIT, Recuperado de [www.isaca.org](http://www.isaca.org)

# Papeles de trabajo y evidencia



Auditoría de  
Sistemas

UNIVERSIDAD

**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**



## Papeles de trabajo y evidencia

El proceso de auditoría completo, con todas sus etapas, se documentará con papeles de trabajo que describirán las labores de auditoría realizadas y la evidencia de auditoría que respalda los hallazgos y conclusiones del auditor de SI.

Dentro del proceso de la auditoría, en la etapa de ejecución, el auditor comienza su trabajo de campo. Para ello, diseña, selecciona, evalúa y documenta evidencias de la entidad analizada para cumplir el objetivo de la auditoría. Estas evidencias tienen que cumplir con las cualidades de ser suficientes, confiables y relevantes, a fin de que puedan ser correctamente interpretables y sean capaces de soportar adecuadamente el análisis del auditor. Una vez llegado a este punto, el auditor está capacitado para plasmar sus conclusiones sobre los hallazgos en un informe.

Al momento de efectuar cada actividad de la auditoría, en la etapa de ejecución, se deben registrar los detalles de las tareas realizadas en los documentos preestablecidos en el plan. También, los datos de las tareas, las decisiones tomadas, los pasos efectuados y los resultados obtenidos.

Las buenas prácticas de auditoría recomiendan que cada documento sea revisado por otro miembro del equipo de auditoría para evitar errores y mejorar la calidad del trabajo. La cantidad de documentación registrada y su nivel de detalle debe ser de una calidad tal, que una tercera empresa tome los mismos documentos y pueda llegar a las mismas conclusiones y resultados, realizando nuevamente los procedimientos de auditoría.

Por ejemplo, en el caso de que se realice una auditoría por muestreo, debido a que el auditor está incapacitado para verificar el 100 % del universo de casos de la organización, por su gran tamaño, se deberá llevar un registro de todo el proceso de muestreo. En él se indicarán temas como cuáles fueron los objetivos del muestreo y cuál fue la metodología realizada. También se registrará la información pertinente para las fuentes de la población, parámetros de selección, ítems escogidos, detalles de las pruebas realizadas y las conclusiones alcanzadas.

### Características de la evidencia

Al seguir los procedimientos documentados en el plan, se obtiene información y otros elementos que servirán como fundamentos para las conclusiones y resultados. Las evidencias son pruebas que certifican el cumplimiento de procedimientos o normas establecidas para la actividad auditada.

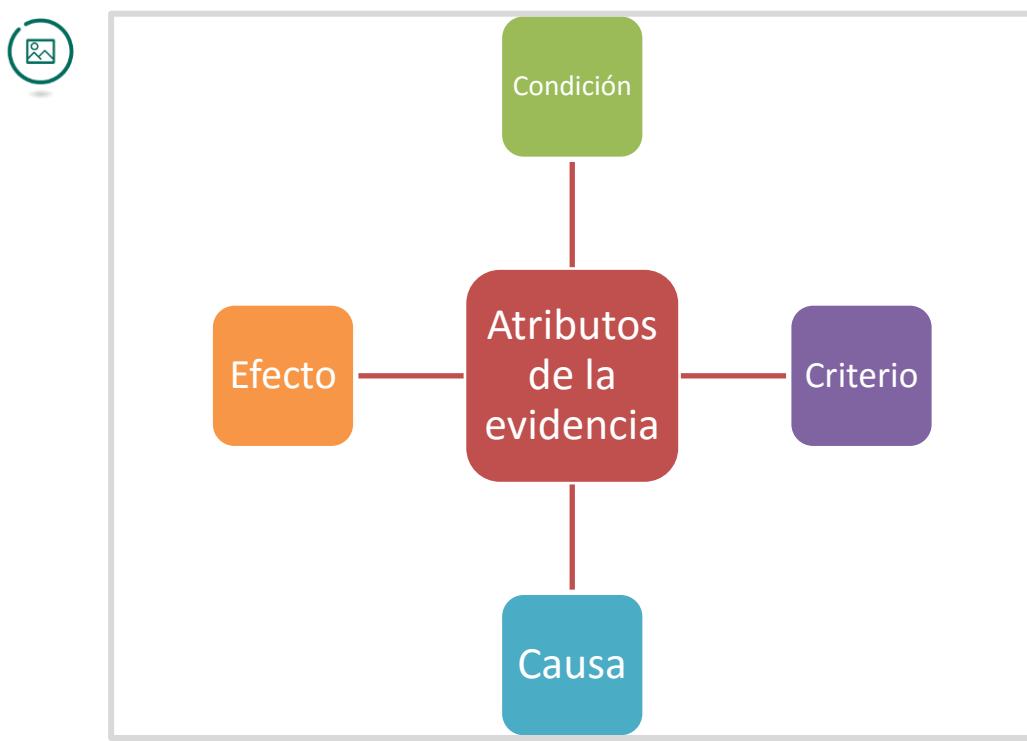
El estándar ISACA para las evidencias de las auditorías (S14) pone énfasis en que el auditor debe obtener evidencias de auditoría suficientes y apropiadas para llegar a conclusiones razonables, sobre las que luego basará los

resultados de la auditoría. Para tal fin, el auditor deberá evaluar la suficiencia de las evidencias obtenidas durante la auditoría.

Los atributos que deben poseer las evidencias incluyen:

- **La condición:** se resume en *lo que es*, es decir que describe la situación presente de la evidencia.
- **El criterio:** se resume en *lo que debe ser*. Son los estándares, normas o reglamentaciones que el objeto en estudio debería cumplir.
- **La causa:** se resume en *por qué sucedió*. Es el origen o motivo por el cual se produjo la situación actual del objeto.
- **El efecto:** se resume en *la diferencia entre lo que es y lo que debe ser*. Son las consecuencias que se produjeron en la organización.

**Figura 1: Atributos de la evidencia de auditoría**



Fuente: elaboración propia.

Asimismo, existe otra forma de clasificación de aquellas cualidades que deben poseer estas evidencias:

- evidencia relevante;
- evidencia apropiada;
- evidencia fiable;
- evidencia suficiente.

## **Evidencia relevante**

El hecho que la evidencia sea relevante significa que debe tener relación con el objetivo de la auditoría que se está llevando a cabo. Por ejemplo, en una auditoría de seguridad informática no tendrá mucho sentido recolectar información sobre el plan de asignación de recursos, que corresponde a la auditoría de gestión de proyectos, pero sí tendrá sentido lógico verificar el cumplimiento de las políticas de acceso a los servidores.

## **Evidencia apropiada**

La evidencia apropiada es la que influye en las conclusiones del auditor, de una manera cualitativa. Incluye a los procedimientos realizados por el auditor, los resultados, los documentos fuente (ya sean en formato electrónico o impresos en papel), los registros e información de corroboración utilizados para apoyar la auditoría y los hallazgos y resultados del trabajo de auditoría.

Además, la evidencia apropiada es la que demuestra que el trabajo fue realizado cumpliendo con las normas, políticas y estándares aplicables.

## **Evidencia fiable**

Son las evidencias válidas y objetivas. El auditor tiene que analizar la fuente y la naturaleza de la información recolectada para evaluar su fiabilidad. Estas evidencias poseen un nivel de confianza que depende de factores como el formato (si se encuentra documentado, en lugar de oral), la ubicación de fuentes (si la obtiene el auditor o ya viene dada por el sistema auditado), el grado de independencia de las fuentes y el grado de independencia del ente que mantiene y certifica la información recolectada.

## **Evidencia suficiente**

Esta evidencia influye de manera cuantitativa en las conclusiones del auditor, es decir, soporta todas las preguntas materiales pertinente al objetivo y al alcance de la auditoría. Como adicional al estándar S14, ISACA aclara que la suficiencia es una medida de la cantidad de evidencias de auditoría, mientras que lo apropiado es la medida de la calidad de la evidencia de auditoría, y ambos conceptos están totalmente relacionados entre sí.

En este contexto, cuando se obtiene información de la organización que es utilizada por el auditor de SI para realizar los procedimientos de auditoría, el auditor de SI debe también poner énfasis en la precisión y completitud de la información. (ISACA, 2006, p.12, <https://goo.gl/PxdTyc>).

## Procedimientos de recolección de evidencias

Recordemos que los procedimientos a seguir para recolectar las evidencias dependerán de lo auditado. Algunos procedimientos pueden ser:

- Consultas: generalmente son entrevistas a empleados para averiguar las actividades que realizan.
- Observación: los auditores pueden mirar tanto la forma de trabajo del personal como la actividad del sistema informático.
- Inspección: es cuando se analiza la documentación de la organización. Por ejemplo, en el desarrollo de *software*, el auditor puede examinar los repositorios de la gestión de configuración y control de versiones, o puede confirmar que cada cambio cuente todas con las aprobaciones requeridas por los procesos de calidad de la organización.
- Monitoreo: ver los resultados o salidas de los procesos para analizar sus puntos de control y medir su desempeño o buscar posibles fallas.

Asimismo, se pueden destacar otros procedimientos para la recolección de evidencias, tales como: consulta, confirmación, computación, procedimientos analíticos, repeticiones de ejecución y/o de cálculo, entre otros.

## Tipos de evidencias

La evidencia también puede ser catalogada de acuerdo con la forma en que es obtenida. Podemos nombrar los siguientes tipos de evidencia:

- **Evidencia de control**: se obtiene con pruebas de cumplimiento del sistema de control interno informático. Permite verificar si los controles están operando correctamente. Ejemplo de estas pruebas son: indagación al personal, verificación de documentación justificativa, observación de aplicación de controles.
- **Evidencia material**: se obtiene con las de pruebas de nivel de materialización. Con estas pruebas, el auditor obtiene evidencia directa sobre la validez de la integridad de los datos procesados por los sistemas de información.
- **Evidencia física**: se obtiene al visualizar los activos tangibles, como los mecanismos de seguridad por *hardware*.
- **Evidencia documental**: se obtiene al examinar la documentación existente.
- **Evidencia testimonial**: puede obtenerse por fuentes internas o externas a la empresa. Pueden ser confirmaciones, indagaciones, documentos judiciales, entre otros.

- **Evidencia analítica:** se obtiene al analizar el comportamiento para identificar una actividad diferente de la esperada.

**Figura 2: Tipos de evidencia de auditoría**



Fuente: elaboración propia.

La cantidad de evidencia que se debe recolectar estará en función de la materialidad del elemento y de los riesgos involucrados en la auditoría. Es importante verificar la completitud de esta, para que pueda apoyar el nivel de riesgo asociado a la entidad evaluada.

El proceso a implementar para obtener las evidencias dependerá de la temática auditada. Esto es así debido a que influyen factores como la naturaleza de la organización, los plazos de la auditoría y el tipo de juicio profesional que deba emitirse. El auditor es responsable de elegir el mejor procedimiento de autoría para cumplir con los objetivos establecidos.

Para esta selección, se debe escoger la forma más económica de realizar la recolección de las evidencias, evitando, sin embargo, que esto resulte en una traba para recoger la cantidad de información necesaria o que se omita un procedimiento necesario.

Al concentrarse en el proceso de recolección de evidencias, es necesario identificarlas, clasificarlas y obtener referencias cruzadas de manera adecuada. También se deben considerar las propiedades de los datos para validar su fiabilidad. Estas propiedades incluyen a sus fuentes de información, a su naturaleza (papel impreso, digital, visual, oral) y a sus componentes de autenticidad (firmas digitales, sellos, etc.).

Esta información se puede profundizar en la guía de auditoría y aseguramiento publicada por ISACA n° 2205 *Evidencia*.

## Referencias

**Blanco, E. L. J.** (2005). *Auditoría y sistemas informáticos*. La Habana, CU: Editorial Félix Varela.

**ISACA, (2014), Guía de Auditoría y Aseguramiento publicada por ISACA N° 2205 – “Evidencia”.** Recuperado de: [http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2205\\_gui\\_Spa\\_0415.pdf](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2205_gui_Spa_0415.pdf)

**ISACA Asociación de Auditoría y Control de Sistemas de Información, Normas Generales para la Auditoría de los Sistemas de Información, 2006, p.12,** <https://goo.gl/PxdTyc>

# El informe del auditor

---



Auditoría de  
Sistemas

UNIVERSIDAD

**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**



# El informe del auditor

El informe de auditoría es el producto final del proceso de auditoría, donde el auditor de sistemas reporta a la gerencia sus hallazgos y recomendaciones. Existen estándares para el formato del informe, pero podría variar en cada organización.

**El informe del auditor representa su visión formal y sistemática, orientada a acciones correctivas de la estructura organizacional, los planes y procedimientos, la forma de operar, el uso de los recursos humanos y físicos y el cumplimiento a las leyes y regulaciones establecidas.**

## Definiciones útiles referentes al informe de auditoría

Los siguientes son conceptos de términos utilizados en el lenguaje del informe de la auditoría. Las definiciones están enfocadas en la etapa de conclusión de la auditoría y la creación del informe.

**Actos ilegales:** transgresiones a leyes o regulaciones gubernamentales

**Error:** falsedad u omisión no intencional del estado o valor de una entidad.

**Fraude:** son las distorsiones intencionales en los estados de una entidad. Pueden provenir de informes fraudulentos o malversación de activos. Legalmente, el fraude es la presentación errónea de un hecho material por una persona, la cual sabe que es falso o cuya veracidad no verificó en forma responsable.

**Tema o área de actividad:** es el campo de actividad específico de la información contenida en el informe del auditor y en sus procedimientos asociados. Puede incluir temas como el diseño y la operación de los controles internos y el cumplimiento de normas, estándares, prácticas de privacidad y leyes gubernamentales.

**Informe de certificación:** es el caso particular de un informe que requiera que el auditor examine y de fe de sus hallazgos, referentes a un tema o a las aseveraciones de la gerencia sobre ese tema o área de actividad en particular. El informe del auditor, en este caso, consiste en la certificación de uno de los siguientes puntos:

- El área de actividad: estos son los informes que basan sus conclusiones en las evidencias encontradas en un área de actividad y no en las afirmaciones recibidas sobre esa área. Estos son los casos en que no se puede realizar una afirmación sobre un tema. Por ejemplo, cuando se contratan terceros para realizar servicios IT, no es posible realizar afirmaciones sobre los controles que esta empresa efectúa, sino que el auditor tendrá que informar directamente sobre el área de actividad auditada.
- La afirmación de la gerencia acerca de la eficacia de los procedimientos de control.

- Una evaluación del informe de certificación, donde se auditén las opiniones sobre un área de actividad. Estos trabajos pueden incluir informes sobre los controles aplicados por la administración y en la eficacia de funcionamiento.

**Objetivos del control:** son los objetivos definidos por la dirección de la organización, y sirven para el diseño y la creación de marcos de trabajo (*frameworks*) que implementarán los controles, es decir, los marcos de referencia sobre los que se basarán los procedimientos de control interno.

**Procedimientos de control:** son las políticas y procedimientos aplicados para alcanzar un objetivo de control.

**Debilidades del control:** son las deficiencias en el diseño o en la implementación de los procedimientos de control. El auditor debe evaluar si las debilidades encontradas resultan en riesgos relevantes para las áreas de actividad en donde se encuentren, y que sean reducidas a un nivel del riesgo aceptable. Los riesgos a considerar son aquellos que amenazan el cumplimiento de los objetivos de control.

**Criterios de auditoría:** son los estándares y puntos de referencia utilizados por el auditor para medir y calificar a las áreas de actividad. Los criterios de auditoría deben poseer las características de ser libres de prejuicios, ser medibles consistentemente, incluir a todos los factores necesarios para llegar a una conclusión y estar relacionados relevantemente con el área de actividad.

**Estrategia gerencial:** es la estrategia definida por la dirección de la organización para lograr los objetivos de negocio. Es el fundamento para el diseño y la implementación de los sistemas de información, los controles del entorno y los procedimientos de control.

## Limitaciones de la opinión del auditor

La opinión del auditor informático se basa en la utilización de determinados procedimientos necesarios para recolectar pruebas y evidencias suficientes y adecuadas, que sean de una naturaleza más bien convincente que concluyente. La garantía que una auditoría de sistemas de información puede brindar sobre la eficacia de los controles internos es, sin embargo, limitada. Esto se debe a la misma naturaleza de los controles internos y a las limitaciones inherentes a cualquier subconjunto de ellos y sus operaciones. Estas limitaciones incluyen:

- El requerimiento usual de la dirección de que el costo de los controles internos no excedan a los beneficios que generan.

- La mayoría de los controles internos tienden a ser dirigidos a la validación de transacciones y eventos rutinarios, en lugar de enfocarlos en los no rutinarios, donde estarían los mayores fraudes.
- La posibilidad de introducir un error humano debido al descuido, distracción o fatiga, falta de comprensión de las instrucciones o juicio equivocado.
- La posibilidad de elusión de los controles internos a través de asociaciones ilícitas entre los empleados, o entre ellos y personas ajenas a la organización.
- La posibilidad de que una persona encargada de ejercer un control interno abuse de esa responsabilidad. Por ejemplo, un miembro de la dirección que altera un procedimiento de control.
- La posibilidad de que la dirección no esté sujeta a los mismos controles internos aplicables al resto del personal.
- La posibilidad de que los controles internos lleguen a quedar inadecuados, debido a cambios en las condiciones del entorno.
- Uno de los factores que puede mitigar las irregularidades en una organización, especialmente, por parte de la dirección, son los sistemas corporativos de *IT governance*. Sin embargo, ellos no son disuasivos determinantes para los fraudes. Un control efectivo de todo el ambiente también resulta de gran ayuda. Este puede incluir a un órgano de gobierno efectivo, comités de auditoría y la función de auditoría interna, los que pueden limitar la conducta inapropiada de la dirección.

Alternativamente, un control inefectivo del entorno puede anular la eficacia de los procedimientos de control dentro de la estructura de control interno de la empresa. Por ejemplo, por más que la organización posea procedimientos de control adecuados, para el cumplimiento de las regulaciones legislativas, la dirección puede tener una fuerte tendencia a suprimir información de incumplimientos que impacten negativamente en la imagen pública de la organización.

La eficacia o la relevancia de los controles internos también podrían verse afectadas por factores tales como un cambio de propietarios, cambios en la gerencia u otro personal, la evolución del mercado o la industria de la organización.

## Hechos posteriores

En ocasiones, se producen eventos con posterioridad al tiempo o período de tiempo en que se lleva a cabo la auditoría, pero antes de la fecha de presentación del informe del auditor, que tienen un efecto material sobre el área de actividad auditada y que por lo tanto, requieren un ajuste en los resultados del informe a ser presentado. Estos sucesos se denominan *hechos posteriores*. Si bien no se encuentra bajo la responsabilidad del auditor

informático detectar estos eventos, es recomendable que le preste la debida atención si es consciente de alguno. Es importante que el auditor consulte con la dirección sobre su conocimiento de algún hecho posterior que podría tener un impacto importante sobre las afirmaciones del informe.

**Figura 1: Informes de auditoría. Hechos posteriores**



Fuente: elaboración propia.

## Conclusiones e informe

El auditor informático debe examinar y evaluar las conclusiones particulares obtenidas de las evidencias recolectadas, como base para formar una opinión sobre los elementos incluidos en el alcance de la auditoría.

Si bien existen lineamientos surgidos del estándar de ISACA G2401 (para reportes de auditoría), todo informe debería incluir los siguientes puntos:

- **Identificación del informe:** El título del informe deberá identificarse con objeto de distinguirlo de otros informes.
- **Identificación del Cliente:** Deberán identificarse a los destinatarios y a las personas que efectúen el encargo.
- **Identificación de la entidad auditada:** Identificación de la entidad objeto de la auditoría informática.
- **Objetivos de la Auditoría Informática:** Declaración de los objetivos de la auditoría para identificar su propósito, señalando los objetivos incumplidos.
- **Normativa aplicada y excepciones:** Identificación de las normas legales y profesionales utilizadas, así como las excepciones significativas de uso y el posible impacto en los resultados de la auditoría.
- **Alcance de la Auditoría:** Concretar la naturaleza y extensión del trabajo realizado: área organizativa, período de auditoría, sistemas de

información... señalando limitaciones al alcance y restricciones del auditado.

- **Conclusiones – Informe corto de opinión:** el resumen de los resultados, que son la esencia del dictamen, la opinión y, si amerita, los párrafos de salvedades y énfasis.
- **Resultado - Informe largo y otros informes:** informe detallado de los resultados.
- **Informes previos:** se utilizan en el caso de detección de irregularidades significativas, previas al informe final, que requieran actuación inmediata según la normativa legal y profesional.
- **Fecha del Informe:** es importante para poder identificar hechos posteriores al fin del período de la auditoría.
- **Identificación y firma del auditor:** aspecto formal esencial, tanto si es individual como si forma parte de una sociedad de auditoría.
- **Distribución del Informe:** en el contrato o en la carta propuesta del auditor informático, deberá definirse quién o quiénes podrán hacer uso del informe, así como los usos concretos que tendrá. (ISACA, 2014, p. 6, <https://goo.gl/nEg3y1>).

## Actividades de seguimiento

La auditoría no concluye cuando se presenta el informe, sino que existe un período de tiempo llamado *actividades de seguimiento*, para verificar la implementación de las recomendación del informe. Dependiendo de la importancia e impacto del hallazgo encontrado, las actividades de seguimiento tendrán un tiempo de ejecución variable. Se deben priorizar las actividades de acuerdo con el tipo y magnitud del riesgo y con los costos asociados a él.

En el estatuto de la auditoría, se tiene que indicar quién realizará el seguimiento y el monitoreo de la implementación de las acciones correctivas. En el caso de la auditoría externa, esto dependerá del alcance y los términos del contrato con el auditor externo. Alternativamente, la dirección puede asumir el riesgo de no efectuar los cambios sugeridos en el informe de auditoría.

Después de llevadas a cabo las acciones correctivas, el auditor puede efectuar pruebas y evaluaciones para corroborar la eficiencia de los cambios realizados y si se ajustan a las recomendaciones y sugerencias presentadas en el informe. Luego, debe presentar otro informe de las actividades de seguimiento, donde se incluyen sus observaciones del estado de estas.



## Referencias

**Blanco, E. L. J.** (2005). *Auditoría y sistemas informáticos*. La Habana, CU: Editorial Félix Varela.

**ISACA, (2014), Guía de Auditoría y Aseguramiento publicada por ISACA N° 2401 – “Reportes de Auditoría”.** En [http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2401\\_gui\\_Spa\\_0415.pdf](http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2401_gui_Spa_0415.pdf). Recuperado de enlace)

# Regulaciones y la auditoría de TI

---



Auditoría de  
Sistemas

UNIVERSIDAD

**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**

# » Regulaciones y la auditoría de sistemas

La comunicación A 4609 del BCRA (y sus modificatorias) define los requisitos mínimos de gestión y control para las entidades financieras de Argentina, sobre los riesgos de la tecnología informática y de los sistemas de información.

La tecnología informática y los sistemas de información han cambiado muchos aspectos de la vida de las personas en estos últimos años. La informática se encuentra arraigada en nuestras comunicaciones, en nuestra recreación y, principalmente, en nuestros trabajos. Es por esto que la *tecnología de información* (TI) debe ser legislada y regulada con normas y leyes, y los profesionales TI tienen que esforzarse por conocerlas y respetarlas.

Cualquiera sea el tamaño, mercado o segmento de una empresa, hay amplia coincidencia en reconocer a TI como uno de los recursos críticos a gestionar para maximizar valor y optimizar los riesgos, más aún en el sistema financiero en el cual se negocia con información.

Las entidades bancarias poseen procesos de negocio altamente automatizados. Han potenciado una complejidad creciente y dinámica, no solo en términos de la industria informática, sino también en el plano regulatorio, donde los entes de control los han obligado a seguir normativas cuyos ciclos de vida soporten la adopción de nuevas y exigentes tecnologías.

## Evolución de las regulaciones internacionales sobre TI en el sistema financiero

Para describir los principales antecedentes normativos del sistema financiero relacionados con riesgos tecnológicos, es necesario remontarse al año 1988, con la publicación del acuerdo Basilea I por parte del comité conformado por los bancos centrales de las principales países del mundo, Alemania, Estados Unidos, Francia, Japón, etcétera.

Dicho acuerdo, que finalmente terminó siendo adoptado por los sistemas financieros de más de 130 países, establecía una serie de recomendaciones para definir un capital mínimo (capital regulatorio) con el que debía contar una entidad bancaria, en función de los riesgos que afrontaba.

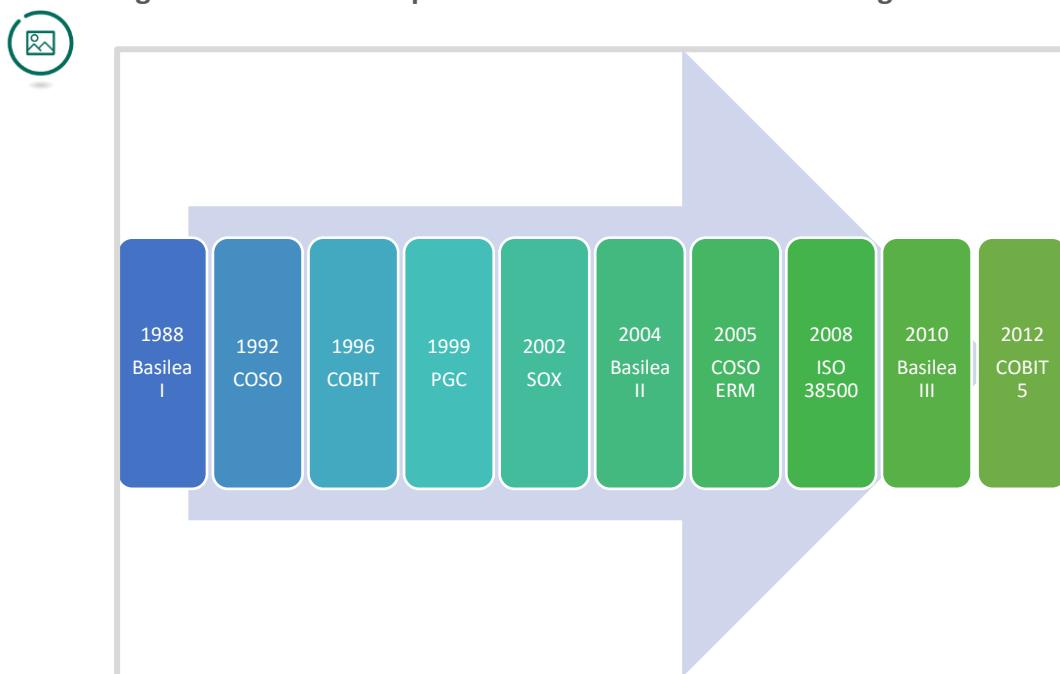
En el año 1992, surgió un marco orientado a toda la actividad, para mejorar el diseño, evaluación y monitoreo del control interno de las organizaciones, denominado COSO por las siglas en inglés de la comisión que lo creó (*Committee of Sponsoring Organizations of the Treadway*), cuya aplicación brindaría un grado de seguridad razonable en cuanto a la consecución de los objetivos de eficacia y eficiencia de las operaciones, confiabilidad de la

información financiera y el cumplimiento de las leyes, reglamentos y normas aplicables.

Años más tarde, concretamente en 1996, sucedió un hecho relevante para las tecnologías de información en las organizaciones. Surge la primera edición de COBIT (*Control Objectives for Information and related Technology*), creado por ISACA (*Information System Auditor and Control Association*), una metodología orientada a brindar un marco de control interno específico para procesos y aplicaciones de tecnología de información.

En 1999, surgen los principios de gobierno corporativo de la Organización para la Cooperación y el Desarrollo Económico (OCDE). Estos se convirtieron en una referencia internacional como guía para la creación de políticas y regulaciones orientadas a mejorar el marco legal, la transparencia en la gestión de las organizaciones y proteger los intereses de los accionistas y de la compañía.

**Figura 1: Evolución de publicaciones relacionadas con riesgos de TI**



Fuente: elaboración propia.

En 2002, luego de los escándalos de corrupción originados por grandes corporaciones como Enron y Worldcom, entre otras, se sanciona en Estados Unidos una ley, creada por el senador del partido demócrata Paul Sarbanes y el congresista del partido republicano Michael G. Oxley. Mundialmente conocida con el nombre abreviado de SOx, tuvo como objetivo establecer el

control para la protección del inversor, de las empresas que cotizan en bolsa, y evitar que el valor de las acciones sea alterado en forma fraudulenta.

En 2004, se realiza una actualización de los principios de Basilea para la industria financiera, denominada Basilea II, que incorpora el concepto de los riesgos operativos, los cuales se agregan a los riesgos financieros como elementos que podrían afectar a las entidades y que habrían de requerir necesidades de exigencias mínimas de capital, para protegerse ante sus efectos negativos. Estos principios fueron nuevamente actualizados en el año 2010, con la publicación del documento Basilea III, más orientado a proteger a los bancos ante crisis de liquidez.

## **Antecedentes locales sobre normativas de TI en el sistema financiero argentino**

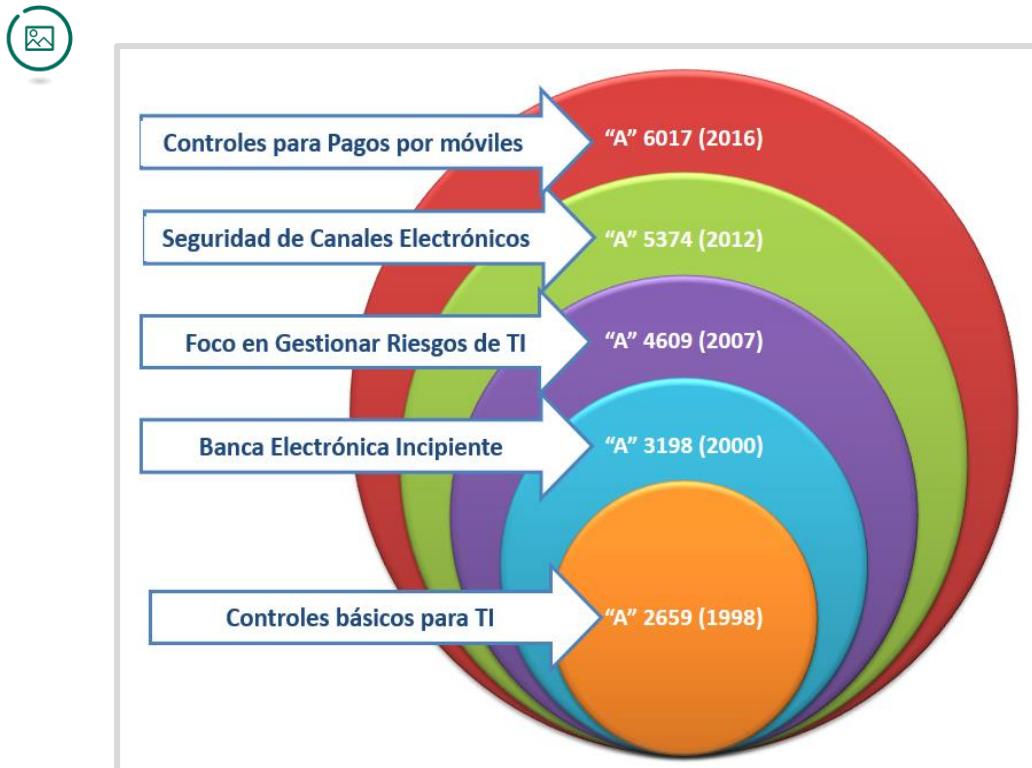
A continuación, se detallan distintas normativas emitidas por el Banco Central de la República Argentina:

- Comunicación A 2659 (enero de 1998): incluyó las primeras exigencias sobre los sistemas informáticos de las entidades financieras. Estaba dividida en once secciones y solo tuvo 2 años de vigencia, ya que contemplaba exigencias de seguridad débiles (por ejemplo, claves de solo cuatro dígitos).
- Comunicación A 3198 (diciembre de 2000): incorporó controles para banca electrónica. Se encontraba más orientada al cumplimiento que a la gestión del riesgo tecnológico. Se basaba en controles generales, y era poco flexible a los cambios tecnológicos. Se mantuvo vigente durante 7 años.
- Comunicación A 4609 (junio de 2007): Esta normativa aparece en el mercado a partir de la necesidad de contar con lineamientos para la gestión y el control de los activos informáticos, proporcionando sanas prácticas con el fin de obtener un equilibrio entre la eficiencia entre la gestión de la información y la gestión de los riesgos.
- Comunicación A 5374 (diciembre de 2012): está orientada a la seguridad en los canales electrónicos, con requisitos técnicos específicos para cajeros automáticos, banca por internet, banca móvil, banca telefónica, terminales de autoservicio y puntos de venta (POS) para tarjetas de crédito y débito.
- Comunicación A 6017 (julio de 2016): incorpora aspectos de seguridad y controles relacionados con pagos por móviles (billetera virtual).

Las tres últimas comunicaciones mencionadas se encuentran actualmente vigentes y compiladas en un texto ordenado, publicado por el BCRA en su sitio web (<http://www.bcra.gov.ar/Pdfs/Texord/t-rmsist.pdf>), bajo el nombre de *Requisitos mínimos de gestión, implementación y control de*

*los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.*

**Figura 2: Regulaciones sobre riesgos de TI en el sistema financiero local**



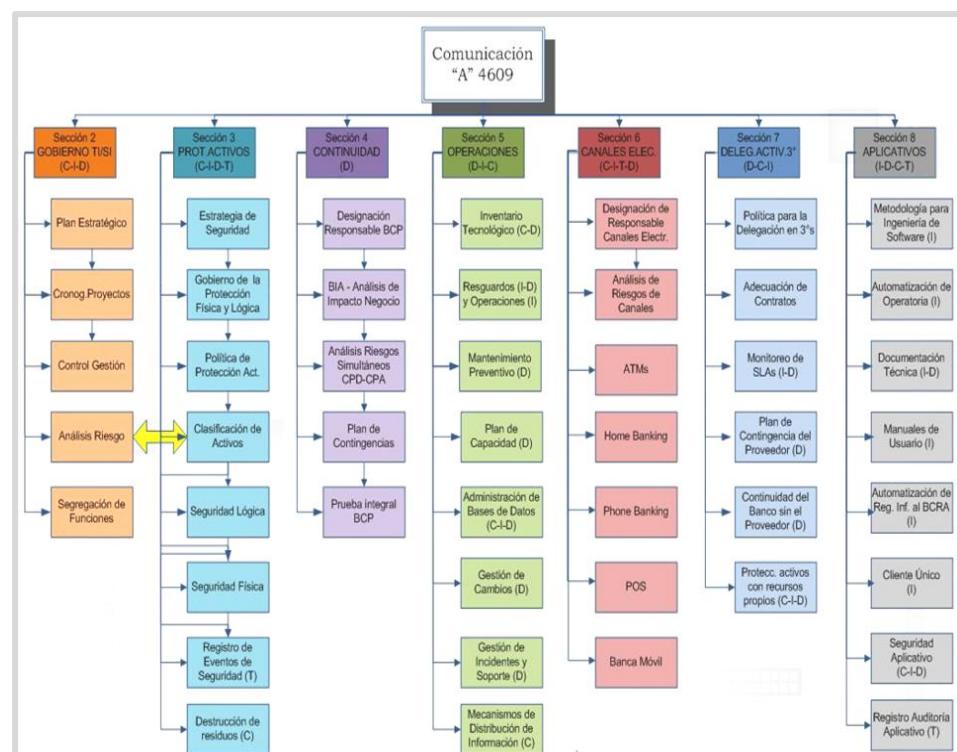
Fuente: elaboración propia.

En función de la normativa mencionada vigente, de cumplimiento obligatorio para las entidades financieras del país, existen diversas exigencias de controles mínimos agrupados en las siguientes secciones:

- Aspectos Generales
- Organización funcional y gestión de tecnología informática y sistemas
- Protección de Activos de Información
- Continuidad del procesamiento electrónico de datos
- Operaciones y procesamiento de datos
- Banca electrónica por diversos medios
- Delegación de actividades propias de la entidad en terceros
- Sistemas aplicativos de información (BCRA, 2007, <https://goo.gl/dHXJH8>).

El auditor de sistemas de las entidades financieras debe incorporar, en su proceso de auditoría, la revisión de los controles exigidos por la normativa vigente para garantizar el cumplimiento regulatorio.

Figura 3: Principales exigencias de la comunicación A 4609 del BCRA



Fuente: elaboración propia.

Es fundamental que el auditor de sistemas de las entidades financieras no solo verifique el cumplimientos de las exigencias normativas, sino que también sepa identificar y comunicar claramente los riesgos que implican cada uno de los hallazgos y debilidades de control que se detecten durante el proceso de auditoría.



## Referencias

**Blanco Encinosa, L. J.** (2008). Auditorías a Sistemas Informatizados en explotación. *Auditoría y Sistemas Informáticos* (pp. 29-34). La Habana, Cuba: Editorial Félix Varela.

**BCRA.** (2007). Requisitos mínimos para la Gestión de la Tecnología Informática. <http://www.bcra.gov.ar/pdfs/comytexord/A4609.pdf> Recuperado de enlace.

# Protección de datos personales



Auditoría de  
Sistemas

UNIVERSIDAD  
**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**



# Protección de datos personales

La protección de datos personales se encuentra garantizada en nuestro país, a través de la acción de *habeas data*, incorporada en la Constitución Nacional (1994). Luego, se sancionó la Ley 25.326 el 4 de octubre del año 2000.

El derecho informático se encarga de regular a la comunidad informática y evita que esta quede sin control alguno. A partir del derecho informático, surgen conceptos que tratará esta sección, como la protección de datos personales, la protección jurídica del *software*, los delitos informáticos y el comercio electrónico, entre otras.

## Protección de datos de carácter personal

La Ley 25.326 (Ley de protección de datos personales y *habeas data*) fue sancionada en Argentina el 4 de octubre del año 2000. El artículo 1<sup>1</sup>define el objetivo de la ley:

La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas. (Congreso Argentino, 2000, <https://goo.gl/fs4tgs>).

El artículo 2<sup>2</sup> establece las definiciones de los términos informáticos. Las más importantes son:

Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento

1 Art. 1 Ley N° 25.326 - Ley de protección de datos personales y *habeas data* – DNPDP Dirección Nacional de Protección de Datos Personales

2 Art. 2 Ley N° 25.326 - Ley de protección de datos personales y *habeas data* – DNPDP Dirección Nacional de Protección de Datos Personales

o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable. (Congreso Argentino, 2000, <https://goo.gl/fs4tgs>).

El derecho a la privacidad, o derecho a los datos personales, se ve directamente afectado por la aplicación de la TI (Tecnología Informática) a la información de las personas. Si bien el procesamiento de información personal se ha estado realizando en las organizaciones de manera manual, mucho antes de la implementación de la TI, el tratamiento automatizado que provee la TI ha producido un incremento en la preocupación por el tema de la privacidad.

## **Dirección Nacional de Datos Personales**

La Dirección Nacional de Protección de Datos Personales (PDP) es el órgano de control creado en el ámbito nacional, para la efectiva protección de los datos personales. Tiene a su cargo el Registro Nacional de Bases de Datos, medio que la ley confiere para conocer y controlar a quienes tratan datos personales.

Asesora y asiste a los titulares de datos personales, recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos. (PDP, 2016, <https://goo.gl/ng0Miw>)

## Concepto de datos personales

La información es de carácter personal cuando es sobre una persona. Con la llegada de la TI, es necesario un replanteo sobre el derecho a la intimidad, debido a la gran cantidad de información que es almacenada y procesada en los bancos de datos de las distintas entidades, públicas y privadas.

En este punto, vale la pena hacer una aclaración sobre los términos *datos* e *información*. Los archivos o bancos de datos son los lugares donde se almacenan físicamente los datos de las personas. Estos datos por sí solos no aportan valor, sino que es necesario efectuar un procesamiento sobre ellos para obtener un resultado útil, que se denomina información. El procesamiento de la información puede comprender operaciones de adición, combinación, exclusión o comparación de datos.

Los datos denominados personales son aquellos que pueden ser identificados con una persona en particular y que permiten conocer de características de esta persona. Dentro de los datos personales, se encuentran los datos sensibles, que se refieren a aspectos privados de las personas que puedan dar lugar a la discriminación. Algunos ejemplos de datos sensibles son la religión, la pertenencia racial, ideología política, fisonomía moral e ideológica, entre otros.

La protección de datos personales hace hincapié en la protección del derecho a la intimidad personal, en otras palabras, "aquella parte de la legislación que protege el derecho fundamental de libertad, en particular del derecho individual a la intimidad, respecto del procesamiento manual o automático de datos" (Molina Quiroga, 2003, <https://goo.gl/IP5VFV>).

El Capítulo II de la Ley 25.326 se titula *Principios generales relativos a la protección de datos*. En el artículo 4<sup>3</sup>, se exponen principios de calidad de los datos:

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

---

<sup>3</sup> Art. 4 Ley N° 25.326 - Ley de protección de datos personales y habeas data – DNPDP Dirección Nacional de Protección de Datos Personales

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.
3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.
5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.
6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.  
(Congreso Argentino, 2000, <https://goo.gl/fs4tgs>).

El cumplimiento de estos principios de calidad es responsabilidad de cada encargado de los sistemas de información que almacenen o procesen información de las personas. Además, los artículos 13, 14 y 15<sup>4</sup> especifican el derecho que tienen las personas a acceder y consultar la información referida a ellos, “incluidos en los bancos de datos públicos, o privados” (Congreso Argentino, 2000, <https://goo.gl/fs4tgs>). En este sentido, “la información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen” (Congreso Argentino, 2000, <https://goo.gl/fs4tgs>).

En el artículo 16, se declara el derecho a que los datos personales incorrectos “sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad” (Congreso Argentino, 2000, <https://goo.gl/fs4tgs>), así como la notificación a terceros que hayan sido afectados por la información errónea. La excepción a este derecho, de pedir que la información personal sea actualizada o borrada, la constituyen los bancos de datos como AFIP o Veraz.

Todas las empresas u organizaciones que posean bases de datos con información de las personas tienen que registrarlos ante la Dirección Nacional de Protección de Datos Personales (DNPDP), dependiente del Ministerio de

---

<sup>4</sup> Art. 13, 14 y 15 Ley N° 25.326 - Ley de protección de datos personales y habeas data – DNPDP Dirección Nacional de Protección de Datos Personales

Justicia. Por el solo hecho de no tener registrado el banco de datos en la DNPDP, se comete infracción a la Ley 25.326.

En la actualidad, todavía existe una brecha muy importante entre lo que establece la ley y la realidad que se práctica en el país. Esto debe ser resuelto con reglamentaciones e interpretaciones judiciales que tengan en cuenta la protección integral de la información.

## **Habeas data**

El *habeas data* es un derecho que poseen las personas a efectuar un amparo “para conocer los datos referidos a ellos, almacenados en bancos de datos públicos o privados. Este derecho también permite exigir la supresión, rectificación, actualización y confidencialidad de los mismos si fueran falsos o discriminatorios” (Congreso Argentino, 2000, <https://goo.gl/fs4tgs>). El término *habeas data* se interpreta como *traigan los datos*, y es similar al término *habeas corpus*, que significa *traigan el cuerpo*. Por lo que el propósito de este derecho es que las personas puedan verificar la exactitud de sus datos personales.

El artículo 33<sup>5</sup> de la Ley 25.326, de protección de datos personales establece:

- 1) La acción de protección de los datos personales o de hábeas data procederá:
  - a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;
  - b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización. (Congreso Argentino, 2000, <https://goo.gl/fs4tgs>).

Y en el artículo 38<sup>6</sup>, encontramos lo siguiente:

- 1) La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo.
- 2) En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen.
- 3) El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información

---

5 Art. 33 Ley N° 25.326 - Ley de protección de datos personales y habeas data – DNPDP Dirección Nacional de Protección de Datos Personales

6 Art. 38 Ley N° 25.326 - Ley de protección de datos personales y habeas data – DNPDP Dirección Nacional de Protección de Datos Personales

referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley.

4) El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial.

5) El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate. (Congreso Argentino, 2000, <https://goo.gl/fs4tgs>).

## Conclusiones sobre la protección de datos personales

Como consecuencia de la Ley 25.326, es posible declarar que el uso de información de las personas con un propósito distinto al ingresado al banco de datos, y en especial la falta de veracidad, constituye una violación a la protección de datos personales. Ejemplo de esto son correos electrónicos con propagandas, las promociones telefónicas o la difusión de datos entre entidades privadas cuando las direcciones de *e-mail*, el número de teléfono u otros datos extraídos de las bases no tuvieron el consentimiento del titular.



## Referencias

**Blanco Encinosa, L. J.** (2008). Auditorías a Sistemas Informatizados en explotación. *Auditoría y Sistemas Informáticos* (pp. 29-34). La Habana, Cuba: Editorial Félix Varela.

**Ley N° 25.326 (2000). Protección de datos personales. Congreso Nacional.**  
Recuperada de: [http://www.jus.gob.ar/media/33481/ley\\_25326.pdf](http://www.jus.gob.ar/media/33481/ley_25326.pdf)

**PDP.** (2016). Registros de la Dirección Nacional de Protección de Datos Personales.  
Recuperado de enlace: <http://www.jus.gob.ar/datos-personales/registros.aspx>

**Molina Quiroga, E.** (2003). Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material. Recuperado de enlace: <http://www.saij.gob.ar/eduardo-molina-quiroga-proteccion-datos-personales-como-derecho-autonomo-principios-rectores-informes-solvencia-crediticia-uso-arbitrario-dano-moral-material-dacc030027-2003/123456789-0abc-defg7200-30ccanirtcod>

# Controles y riesgos tecnológicos

---



Auditoría de  
Sistemas

UNIVERSIDAD

**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**



# Controles y riesgos tecnológicos

Riesgo proviene del italiano *risico* o *riscchio* que, a su vez, tiene origen en el árabe clásico *rizq* (“lo que depara la providencia”). El término hace referencia a la proximidad o contingencia de un posible daño. (Auditool, 2012, p.1)

La función de los controles informáticos es la de prevenir y evitar la ocurrencia de los riesgos en los sistemas de información.

Por ejemplo, los riesgos tecnológicos relacionados con el sistema financiero parecen ser el blanco principal de los criminales en la actualidad y con vistas de crecimiento en el futuro. Esto está muy relacionado con el hecho de que la economía tiende a convertirse en una actividad puramente virtual, con actividades totalmente ejecutadas por los sistemas de información.

Todo el riesgo para el Negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de TI dentro de una empresa, se lo considera Riesgo Tecnológico. (ISACA, 2013, p. 17)

A su vez, como dicho riesgo tecnológico podría impactar en las operaciones de la empresa, también es considerado como algo que debe quedar abarcado como parte de la gestión del riesgo operativo, que es el riesgo de sufrir pérdidas debido a la no adecuación o a fallos en los procesos, personal y sistemas internos, o bien por causa de eventos externos.

Figura 1: Tipos de eventos de riesgo operativo



## Tipos de eventos de riesgo operativo

- Fraude interno.
- Fraude externo.
- Relaciones laborales.
- Fallos en TI.
- Daños (activos materiales).
- Clientes y productos.
- Procesos.

Fuente: elaboración propia.

Las organizaciones deben integrar la gestión del riesgo tecnológico en una forma efectiva y concreta dentro de la gestión del riesgo empresarial (ERM) si quieren reducir sus futuras pérdidas y mejorar el rendimiento del negocio. Una inadecuada gestión de los riesgos de TI (tecnología informativa) pueden reducir el valor del negocio, creando pérdidas financieras, dañar la reputación corporativa y desperdiciar nuevas oportunidades.

## Procesos de gestión de riesgos tecnológicos

Actualmente, parece imposible imaginar una compañía que ejecute sus actividades prescindiendo de la tecnología informática (TI). Sin importar la industria ni el tamaño de la organización, son evidentes los múltiples beneficios que el apropiado uso de las TI puede aportar a la rentabilidad de un negocio, en términos de automatización, eficiencia, amplio alcance geográfico, uso remoto, reducción de costos, velocidad, etcétera.

No obstante, la adquisición e implementación de sistemas e infraestructura tecnológica debe ser acompañada de un proceso continuo de análisis y gestión de los riesgos informáticos, ya que, en caso de no ser adecuadamente mitigados, podrían significar un severo impacto para el negocio. La gestión de los riesgos inherentes a la tecnología informática, debería realizarse en forma consistente, bajo un marco metodológico de trabajo (*framework*) que responda a las mejores prácticas y estándares internacionales reconocidos en la materia (Risk IT, COBIT, MAGERIT, AS/NZ4360, ISO 31000, ISO 27005, etc.), y totalmente integrado a la gestión del riesgo corporativo (enfoque ERM, *Enterprise Risk Management*), para que esté alineado con el nivel de tolerancia que la alta gerencia ha establecido para la organización, en sus distintos aspectos de riesgos (operacional, liquidez, crédito, mercado, legal, reputacional, etc.).

**Figura 2: Tipos de riesgos en las organizaciones**



Fuente: ISACA, 2012, <https://goo.gl/krTJTF>

En ese sentido, cabe destacar la norma ISO 31000, especialmente elaborada para la gestión de riesgos, que incluye los siguientes principios:

- La Gestión de Riesgos debe crear y proteger el valor.
- Debe ser una parte integral de los procesos.
- Debe ser parte de la toma de decisiones.
- Abordará explícitamente la incertidumbre.

- Debe ser sistémica, estructurada y oportuna.
- Se basará en la mejor información disponible.
- Debe estar hecha a medida.
- Considerará factores personales y culturales.
- Debe ser transparente e inclusiva.
- Será dinámica, iterativa y sensible al cambio.
- Facilitará la mejora continua de la organización. (ISO31000, 2009, <https://goo.gl/OaPSZa>)

Dicha norma incluye un marco de trabajo como el que se expone en el gráfico a continuación, con los pasos necesarios para implementar la gestión de riesgos en una organización.

**Figura 3: Marco de trabajo de la norma ISO 31000 para gestión de riesgo**



Fuente: Adaptado de ISO31000, 2009, <https://goo.gl/OaPSZa>

Posteriormente, se debería verificar un proceso continuo de análisis y gestión de riesgos, compuesto por las siguientes etapas:

Figura 4: Proceso de gestión de riesgo según la norma ISO 31000



Fuente: Adaptado de ISO31000, 2009, <https://goo.gl/OaPSZa>

## Tipos de riesgos tecnológicos

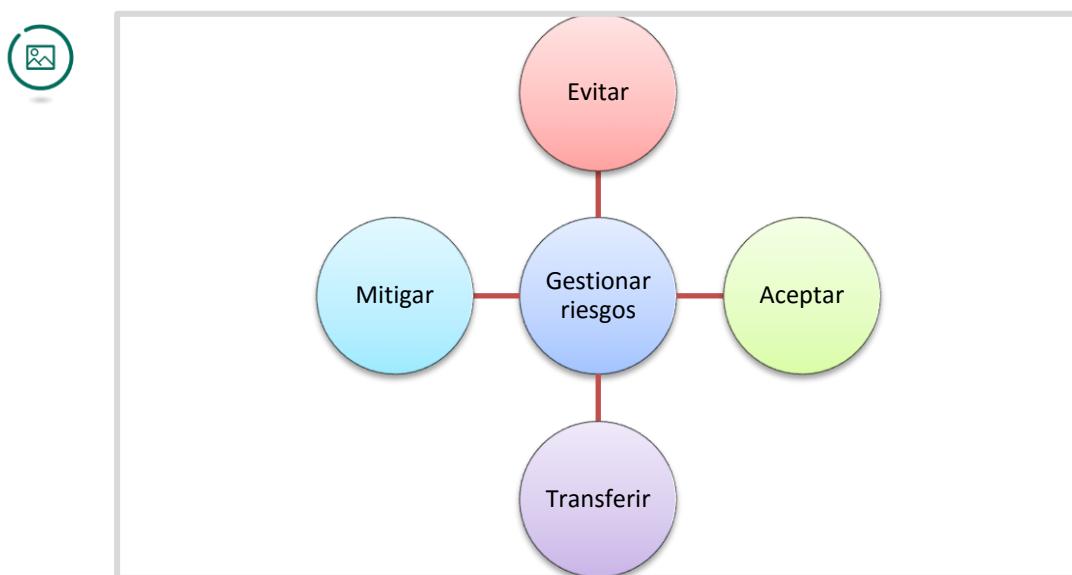
Dentro de los riesgos tecnológicos habitualmente identificados, podemos señalar aquellos que, si se materializan, podrían generar un evento de:

- Revelación o divulgación.
  - Por ejemplo, fuga de información sensible
- Interrupción.
  - Por ejemplo, interrupción de procesamiento
- Modificación.
  - Alteración de la configuración de dispositivos.
- Robo.
  - Por ejemplo, robo de equipamiento crítico.
- Destrucción o eliminación.
  - Por ejemplo, destrucción de centro de procesamiento de datos por desastres naturales.
- Diseño inadecuado.
  - Por ejemplo, soluciones tecnológicas cuyo diseño no satisface las necesidades del negocio
- Ejecución no efectiva.
  - Por ejemplo, procesos ejecutados con desempeño insuficiente.
- Uso inapropiado.
  - Por ejemplo, utilización de recursos informáticos de la compañía para fines no previstos.
- Incumplimientos regulatorios.
  - Por ejemplo, sanciones por reclamos de clientes.

Estos eventos podrían ser originados por actores internos, externos o por causas de la naturaleza, ya sea en forma maliciosa, accidental o mediante fallas.

En consecuencia, el auditor debería revisar el nivel de riesgos existente para cada uno de los posibles eventos de riesgo identificados y verificar que la organización elabore los planes de acción con las respuestas necesarias, coordinadas entre los distintos sectores involucrados, para que los riesgos informáticos no superen los niveles aceptables para la alta gerencia. Debe analizar costos y beneficios de implementar controles mitigantes o transferir parte del riesgo a terceros, por ejemplo, mediante pólizas de seguros.

**Figura 5: Tratamiento de los riesgos tecnológicos**



Fuente: elaboración propia.

Por último, debe verificarse que exista comunicación de los resultados finales a la alta gerencia, a través de reportes que muestren en forma clara los riesgos residuales a los que se encuentran expuestos los componentes de las distintas soluciones informáticas que soportan procesos críticos para el negocio, con el fin de que puedan ser integrados dentro de la gestión de los riesgos corporativos de la organización.

## Referencias

**Blanco Encinosa, L. J.** (2008). *Auditoría y Sistemas Informáticos* (pp.53-70). La Habana, Cuba: Editorial Félix Varela.

**ISO 31000. (2009)** Norma para la Gestión de los Riesgos  
<http://www.iso.org/iso/home/standards/iso31000.htm>

**ISACA. (2007). Risk IT. Figura 3. Jerarquía de Riesgos.** Recuperado de:  
<http://docplayer.es/docs-images/23/1782354/images/11-0.png>

**Auditool. (2012)** ¿Qué es el riesgo, riesgo inherente y riesgo residual?  
<https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual>

# Intercambio electrónico de datos



Auditoría de  
Sistemas

UNIVERSIDAD  
**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**

# » Intercambio electrónico de datos

Como ejemplo de un Intercambio Electrónico de Datos muy utilizado, está la red internacional SWIFT que funciona a través de un sistema para las transferencias electrónicas de fondos.

Una de las claves para competir en el entorno actual, caracterizado por una fuerte competencia en todos los sectores, reside en el establecimiento de sistemas efectivos de mejora continua de la productividad –sin reducción de la calidad– que apliquen una utilización óptima de la información.

En ese sentido, el intercambio electrónico de datos permite mantener flujos de comunicación en tiempo real, que refuerzen los acuerdos cooperativos que forman parte de la estrategia global de la empresa.

El Intercambio Electrónico de Datos (EDI) elimina la intervención manual en la transmisión de documentos normalizados. Actualmente, el uso del EDI es imprescindible, sobre todo si se quiere trabajar en determinados sectores, que lo exigen debido a los múltiples beneficios que ofrece a las empresas.

Para su éxito se necesita una implementación cuidadosamente planificada. También son factores clave en la difusión de este sistema, entre otros, solucionar el problema de los estándares EDI, que los socios comerciales que lo usan tengan confianza entre sí y que ejerzan su poder de negociación de forma persuasiva. (Claver Cortés, 1998, <https://goo.gl/iTXIBi>).

## Definiciones iniciales del EDI

En otras palabras, el EDI es el intercambio electrónico de documentos comerciales y administrativos entre sistemas de información de distintas empresas. Para que esto sea posible, ambos sistemas deben comunicarse en un lenguaje común, que se logra a través de normalización de los formatos de los datos.

Esto ocurre, generalmente, entre organizaciones que poseen una alta relación comercial como, por ejemplo, la relación clientes-proveedor, las entidades financieras con el Estado o similares. Estas empresas que utilizan EDI se denominan *socios comerciales*. La información comercial que generalmente se transmite son datos de transacciones, aunque también se suele intercambiar información referente a cotizaciones de precios y consultas sobre el estado de las órdenes de compra.

El intercambio electrónico de datos representa una ventaja competitiva para muchas empresas, que logran optimizar sus recursos con su implementación. Algunos beneficios que el EDI proporciona son:

- La información que se intercambia logra mayor calidad al ser más exacta y poseer menos errores que la que se obtiene con el procesamiento manual.
- El trabajo es más organizado y se desarrolla en menor tiempo, dado que la información se transmite electrónicamente, con un mejor *cash-flow*, dado por la transmisión y gestión automática del dinero, independientemente de los horarios de las jornadas laborales.
- Mejoran las relaciones comerciales al disminuir los tiempos de utilización de los recursos y al aumentar la satisfacción de los clientes, por ofrecer una mejor disponibilidad de la información.
- Reducción de los costos al aumentar la productividad de las actividades de recolectar, enviar y recibir información. Se reduce también la documentación escrita y los costos de su envío.

Las interacciones entre las organizaciones participantes del EDI se llevan a cabo a través de aplicaciones informáticas que cumplen el rol de ser interfaces entre los sistemas para el intercambio de los datos locales. El EDI debe formalizar la estructura que tendrán los datos, para puedan ser comprendidos por las aplicaciones participantes de la transmisión, así como el significado comercial que tendrán.

Las ONU desarrolló estándares para que las transacciones electrónicas de la plataforma funcional del EDI se efectúen de manera uniforme. Los estándares más utilizados son el ANSI X-12 para los Estados Unidos y el EDIFACT para Europa, que es el único estándar normalizado para el intercambio electrónico de datos.

Muchas organizaciones adoptaron el EDI, debido a las numerosas negociaciones y a los altos esfuerzos de cooperación que desarrollan con sus socios comerciales. Estas relaciones interorganizacionales son un requisito para la implantación exitosa de un EDI, así como también, las alianzas estratégicas, las sociedades comerciales, los *joint venture*, los consorcios de investigación y desarrollo, etcétera.

**Figura 1: Factores claves para el desarrollo de una EDI**



Fuente: elaboración propia.

### **El factor *confianza* en un EDI**

Muchos estudios sobre el EDI tradicional fundamentan su éxito en la economía de los costos de las transacciones. Esta teoría afirma que los socios de negocios, a menudo, no confían entre sí, debido a que poseen un mayor interés en sí mismos que en el éxito de la alianza. Para reducir el costo que esto ocasiona y mejorar el grado de confianza, los socios de negocios necesitan emplear ciertos mecanismos, como son la búsqueda previa de información, los contactos, las negociaciones y los contratos, así como la aplicación *a posteriori* del seguimiento, control y aseguramiento.

El costo de las transacciones entre ellos resulta en costos asociados a estos mecanismos. Cinco atributos generales pueden influir en el costo de transacción: especificidad de los activos, incertidumbre del entorno transaccional, frecuencia de las transacciones, grado de confianza y actitud ante el riesgo de los socios de negocios.

El EDI intenta bajar los costos de transacción, mediante la mejora de estos cinco atributos. Como cualquier IOS, la confianza es un factor importante para el éxito de la EDI. Las organizaciones que aplican la confianza están más dispuestas a invertir en un EDI y a compartir información con sus socios comerciales. Por otra parte, la confianza puede detener la aparición del comportamiento oportunista. La oportunidad de compartir información con los socios de negocios mejorará después de la reducción de este tipo de comportamiento.

### **El factor *poder* en un EDI**

La teoría de la dependencia de los recursos de Pfeffer y Salanzik es también aplicable a la explicación de la implementación de un EDI. Esta teoría afirma que la dependencia interorganizacional es creada cuando un socio de negocio no controla completamente todas las condiciones necesarias para el logro de una acción o para obtener el resultado deseado de la acción.

Desde este punto de vista teórico, un socio de negocios necesita reducir el grado de interdependencia, es decir, reducir al mínimo la incertidumbre de la dependencia de los socios comerciales de los recursos importantes. De acuerdo con esta teoría, la estructura de poder entre los socios de negocios se encuentra muy correlacionada con el grado de interdependencia y su balance, que se determina por quién tiene el control de los recursos claves.

El proceso de implementación de un EDI requiere la institucionalización de:

- los estándares de calidad acordados;
- las prácticas comerciales,
- la información a ser compartida;
- las inversiones en equipamiento y recursos humanos;

Estos requisitos pueden afectar sustancialmente la asignación de recursos claves, que son lo que determinan la relación de interdependencia.

El poder convincente y el poder imperativo que posea una organización también pueden influir en otra entidad, para que implemente un EDI. El poder convincente se utiliza con mecanismos de incentivos, como recompensas financieras, para animar a una organización a implementar un EDI, principalmente, al demostrar los beneficios económicos que logran con un EDI.

Cuando una organización tiene un poder de negociación más importante que sus pequeños y diversificados socios comerciales, el poder imperativo resulta más efectivo que el poder convincente, para forzar a los socios a adoptar un EDI. Este es el caso de las firmas comerciales dominantes, cuyas decisiones ejercen una gran presión en las compañías que trabajan con ellas.

## El factor visión en un EDI

El objetivo a corto plazo de la cooperación interorganizacional es obtener beneficios económicos. El objetivo a largo plazo es buscar y maximizar una relación duradera interorganizacional con los socios comerciales, a través de una serie de actividades de cooperación. Ambas partes de la alianza necesitan crear una visión común y definir claramente sus respectivas funciones y expectativas. Una comunicación constante sobre los objetivos comunes puede facilitar el desarrollo exitoso de la relación de cooperación. Por lo tanto, es importante crear una visión compartida, antes que la asociación se inicie. La visión lograda afectará el costo y los beneficios percibidos por la ejecución del EDI, mejorando así la disposición a implementar otros proyectos del EDI.

Contar con objetivos comunes mejorará también la voluntad de los socios comerciales de compartir el conocimiento, la integración de negocios y las inversiones en *joint venture*, además de fomentar el compromiso y la

confianza en la asociación. Por lo que, establecer una visión común antes de crear la alianza formal influye considerablemente en el grado de participación de las organizaciones en el EDI.

## Transferencia electrónica de fondos (TEF)

En su concepto más amplio, la TEF puede comprender cualquier tipo de envío de dinero a través de medios electrónicos. Esto no solamente se restringe a internet, sino que incluye a cualquier tecnología de comunicación que pueda efectuar una transmisión de fondos de manera automática, inmediata y simultánea, por pedido del titular de una cuenta en una entidad financiera. Algunos ejemplos de esto son: las transferencias entre bancos y entidades financieras o de estas con otras organizaciones, pagos con tarjeta de crédito, cajeros automáticos, terminales de puntos de ventas, dispositivos móviles y pagos por internet desde los hogares.

En Argentina, la transferencia electrónica de fondos de encuentra regulada por el Banco Central (BCRA), dentro de sus normativas del sistema *nacional de pagos-transferencias*, junto con las diversas regulaciones, mencionadas en distintas lecturas de este módulo.

## Seguridad de la documentación electrónica

Existen dos aspectos a considerar en la seguridad de la documentación electrónica: la autenticidad del documento y la seguridad del soporte que almacena al documento.

Para la autenticación de los documentos electrónicos, habitualmente se utilizan tres grandes métodos:

- **El código de ingreso**, que consiste en un número o una clave numérica que se otorga a una persona para su uso exclusivo y personal;
- **La criptografía**, que consiste en el arte o la ciencia de escribir un texto de tal forma, que sea entendido solamente por quienes conocen los medios de descifrado. Por lo general, consisten en una clave confidencial unida a un proceso lógico de transformación o algoritmo, que tornan los datos y programas incomprensibles para quienes no conozcan dichas claves;
- El reconocimiento de características físicas, utilizando las llamadas **"técnicas biométricas"**, que consisten en que el ordenador identifique la voz, característica del iris, impresión digital del operador, etc.

Estas técnicas pueden utilizarse en forma individual o combinada, para dar mayor seguridad a la autenticación de un procedimiento electrónico. En tal sentido, tomemos un ejemplo cotidiano: las tarjetas magnéticas utilizadas para ingresar en los cajeros automáticos de cualquier Banco del

país y realizar operaciones de extracción o depósito de dinero. Estas tarjetas poseen una banda magnéticamente grabada que permite la identificación de la misma. Pero además de ello, se exige también la identificación del operador de la tarjeta mediante un código o número de identificación personal (P.I.N.).

En cuanto a la seguridad del soporte, los medios informativos requieren de técnicas de control totalmente distintas a las conocidas y utilizadas hasta ahora en los documentos escritos. En un rápido esbozo, podrían resumirse en:

- Un adecuado control técnico de los equipos y programas a utilizar.
- La estandarización de los sistemas informativos emisores, entendida como la instrumentación de un sistema uniforme de emisión de los documentos. Esto implicará la adopción de un único software convencional para los ordenadores que puedan emitir documentos electrónicos.
- El empleo de mecanismos de protección de los archivos y programas que impidan su reinscripción, otorgándole al documento la característica de inalterable. (Martínez, 2002, <https://goo.gl/Zc8zkx>)



## Referencias

**Blanco Encinosa, L. J.** (2005). *Auditoría y Sistemas Informáticos* (pp. 180-190). La Habana, Cuba: Editorial Félix Varela.

**Claver Cortés.** (1998). *El intercambio electrónico de datos: pautas para su implantación y factores críticos.* Recuperado de: <http://rua.ua.es/dspace/handle/10045/17339>

**Martínez, María Raquel.** (2002). *El documento electrónico.* Recuperado de: <http://biblioteca.clacso.edu.ar/ar/libros/argentina/cijs/SEC1014.HTML>

# Auditoría de las bases de datos

---



Auditoría de  
Sistemas

UNIVERSIDAD  
**SIGLO 21** | MIEMBRO DE LA RED  
**ILUMNO**

# » Auditoría de las bases de datos

La importancia de las bases de datos radica en que gestionan el activo más importante de las organizaciones: la información. Por esto, es crucial implementar las medidas correctas de protección para las bases de datos, donde se controlarán a los usuarios que ingresan al sistema y el nivel de exposición que puedan tener los datos, en función de los niveles de autorización definidos.

El propósito de la auditoría de las bases de datos es verificar el cumplimiento a los procedimientos de seguridad para la información almacenada. Además, esta auditoría permite descubrir puntos débiles y brindar sugerencias acerca de cómo mejorarlos.

Al software que se encarga de gestionar y controlar la forma en que se organiza, almacena, recupera la información de una base de datos, se lo denomina Sistema de Gestión de Bases de Datos (SGBD). Asimismo, dicho sistema es que gestionar la seguridad y la integridad de la información , acepta solicitudes de las aplicacionesy envía instrucciones al sistema operativo para transferir los datos apropiados a las aplicaciones que realizaron las solicitudes.

Es posible definir a la auditoría de bases de datos como: “el proceso de medir, asegurar, demostrar, monitorear y registrar los accesos a la información contenida en las bases de datos, incluyendo la capacidad de determinar quién, cuándo, desde qué tipo de dispositivo/aplicación y desde dónde se accedieron a los datos” (Rodríguez, 2010, <https://goo.gl/dQ566o>).

La auditoría de las bases de datos es de importancia fundamental como punto de partida para analizar los programas y las aplicaciones de la organización que utilizan los datos contenidos en estas. Esta auditoría es de gran relevancia debido a que, en la actualidad, toda la información corporativa reside en bases de datos, por lo que los auditores deben poder verificar los controles existentes, a fin de mantener la integridad de la información recolectada y almacenada.

Al analizar los controles y los procedimientos sobre el manejo de las bases de datos, se deben considerar los riesgos asociados con la pérdida o revelación de los datos confidenciales, en especial, los relacionados con los clientes de la organización. Los auditores deben validar la existencia y eficiencia del sistema de monitoreo sobre los datos, para saber perfectamente quién accedió a la información, cuándo lo hizo y qué cambios realizó.

## Metodología para auditar bases de datos

Dado que la auditoría de bases de datos se ubica dentro de la auditoría de sistemas de información, esta debe ejecutarse basándose en una metodología de auditoría. Las metodologías se fundamentan en estándares internacionales y en las buenas prácticas de la industria con respecto a la seguridad de los datos.

Los puntos claves a verificar que tiene que abarcar una metodología incluyen la definición de las estructuras físicas y lógicas de las bases de datos, el control de carga y de desempeño de las bases, la integridad y la protección de la información, los procedimientos de programación y mantenimiento para aplicativos de las bases, los mecanismos de respaldo y recuperación de datos y la segregación de las funciones de los responsables de las bases de datos.

Los pasos que debe seguir una metodología de auditoría comprenden, entre otras cosas, poder identificar todas las bases de datos de la organización, para luego clasificar los niveles de riesgo de los datos, con el objetivo de analizar los permisos de acceso y los controles existentes de acceso a las bases de datos. Además, los auditores analizan los modelos de auditoría de bases de datos, si los hubiera. Si no existen, los deben establecer para la organización, así como las pruebas a realizar para cada base de datos, aplicación y usuario.

Cada organización puede definir su propia metodología para auditar las bases de datos, sin embargo, estas generalmente se agrupan en dos tipos: metodologías tradicionales y metodologías de evaluación de riesgos.

### **Metodología tradicional para auditar bases de datos**

La metodología tradicional consiste en la revisión de todo el entorno de las bases de datos, utilizando una lista de comprobación o *checklist*. Estas listas deben comprender todos los aspectos a tener en cuenta y, generalmente, se utilizan al auditar los productos de bases de datos.

El auditor simplemente recorre los puntos de la lista y marca el resultado de su revisión. Resulta vital para el éxito de este método que la lista abarque todos los puntos más importantes que deben ser auditados, dado que los puntos que no se especifiquen en la lista no serán considerados en la auditoría.

### **Metodología de evaluación de riesgos para auditar bases de datos**

Se identifican los riesgos relacionados con la base de datos, realizando las distintas etapas del proceso de gestión de riesgos (ver lectura del módulo 3 sobre controles y riesgos tecnológicos).

Los riesgos más importantes que pueden presentarse en las bases de datos son:

- Incremento de la dependencia del servicio informático debido a la concentración de datos.
- Mayores posibilidades de acceso en la figura del administrador de la base de datos.
- Incompatibilidades entre sistemas de seguridad de acceso propios del Sistema de Gestión de Bases de Datos (SGBD) y el general de la instalación.
- Mayor impacto de errores en datos o programas que en los sistemas tradicionales.
- Ruptura de enlaces o cadenas por fallos del software o de los programas de aplicación.
- Mayor impacto de accesos no autorizados al diccionario de la base de datos que a un fichero tradicional.
- Mayor dependencia del nivel de conocimientos técnicos del personal que realice tareas relacionadas con el software de base de datos (administrador, programadores, etc.). (ULADEC, 2006, <https://goo.gl/CZGmYG>)

Una vez identificados estos riesgos, es posible crear objetivos, técnicas y pruebas para su control. Un mismo objetivo puede tener varias técnicas asociadas para su cumplimiento. Las técnicas pueden ser de carácter preventivo, detectivo o correctivo.

Por ejemplo, un objetivo podría ser conservar la confidencialidad de la información en la base. Con este objetivo en mente, las técnicas a definir serían del tipo establecer los perfiles de usuarios con sus respectivos permisos y restricciones de acceso.

Después de haber definido las técnicas, llega el turno de diseñar las pruebas para verificar la eficiencia de las técnicas de control. Estas pruebas pueden ser de dos tipos.

**Figura 1: Tipos de pruebas de auditoría a aplicar sobre las bases de datos**



Fuente: elaboración propia.

1. **Pruebas de cumplimiento:** tratan de obtener evidencia en relación con la integridad, exactitud y validez de si se están cumpliendo y aplicando correctamente los procedimientos de control interno existentes. Una prueba de cumplimiento es el examen de la evidencia disponible de que una o más técnicas de control interno están en operación o actuando durante el período auditado. Estas pruebas tratan de obtener evidencia de que los procedimientos de control interno, en los que el auditor basa su confianza en el sistema, se aplican de acuerdo a la manera establecida. (Gómez López, 2010, <https://goo.gl/AwO3hg>)

Asimismo, son útiles para determinar si hubo algún incumplimiento respecto a una adecuada segregación de funciones.

La naturaleza de los procedimientos de control interno y la evidencia disponible sobre su cumplimiento determinan, necesariamente, la naturaleza de las pruebas de cumplimiento e influyen sobre el momento de ejecución y extensión de tales pruebas.

Las pruebas de cumplimiento están íntimamente interrelacionadas con las pruebas sustantivas y, en la práctica, los procedimientos de auditoría suministran al mismotiempo evidencia de cumplimiento de los procedimientos de control interno contable, así como la evidencia requerida de las pruebas sustantivas. (Mira Navarro, 2006, <https://goo.gl/lXnKAr>).

Un ejemplo de prueba de cumplimiento es el listar los privilegios y perfiles existentes en el SGBD para verificar si la realidad corresponde con lo establecido por los controles.

2. **Pruebas sustantivas:** Este tipo de pruebas se encuentran orientadas a verificar si la información auditada, cuenta con integridad, exactitud y validez.

“También se refieren a la comprobación de la información para saber si esta ha sido corrompida, comparándola con otra fuente o revisando los documentos de entrada de datos y las transacciones que se han ejecutado” (ULADECH, 2006, <https://goo.gl/CZGmYG>).

3. “Los procedimientos sustantivos intentan dar validez y fiabilidad a toda la información que generan los sistemas de información auditados” (Gómez López, 2010, <https://goo.gl/AwO3hg>).

Con las pruebas de cumplimiento y las pruebas sustantivas, el auditor informático tiene que estar en condiciones de preparar un informe a la

dirección de la organización, acerca del grado de cumplimiento de los procedimientos de control y la fiabilidad de la información procesada por las bases de datos.

## Auditoría y control interno en un entorno de base de datos

Cuando la base de datos se encuentre en producción, los auditores tienen que abarcar en sus análisis al entorno informático donde se encuentra la base. Se vuelve fundamental considerar el control, la integridad y la seguridad de los datos compartidos por múltiples usuarios y abarcar a todos los componentes del entorno de bases de datos.

A continuación, se detallan algunos de los procedimientos y las políticas que deberían establecerse en todos los entornos de bases de datos:

- Organización de la base de datos y diccionario de datos.
- Procedimientos de mantenimiento y seguridad de bases de datos.
- Determinación y mantenimiento de la propiedad de las bases de datos.
- **Procedimientos de control de cambios sobre el diseño y contenido de la base de datos.**
- Reportes administrativos y seguimientos de auditoría que definen actividades de bases de datos.
- Políticas y procedimientos relacionados con la librería de medios y con el almacenamiento de datos fuera del *site*, incluyendo:
  - administración de la librería de medios y del sistema de administración de la librería;
  - requerir la identificación externa de todos los medios;
  - requerir el inventario actual de todos los contenidos y procesos para actividades de control.
- Procesos de administración para proteger los recursos de datos.
- Procedimientos de conciliación entre registros reales y de datos.
- Reciclaje de datos y rotación de medios de datos.
- Funciones del personal dentro y fuera del *site* en los planes de manejo de desastres y recuperación del negocio.



## Referencias

**Blanco Encinosa, L. J.** (2005). *Auditoría y Sistemas Informáticos* (pp. 173-190). La Habana, Cuba: Editorial Félix Varela.

**Rodríguez, R.** (2010), *Auditoría de Bases de Datos*. Recuperado de:  
<http://auditoria3.obolog.es/auditoria-base-datos-876651>

**ULADECH.** (2006). *Auditoría de Bases de Datos*. Recuperado de enlace:  
[http://files.uladech.edu.pe/docente/02659781/CAT/S02/06\\_auditoria\\_de\\_base\\_de\\_datos.pdf](http://files.uladech.edu.pe/docente/02659781/CAT/S02/06_auditoria_de_base_de_datos.pdf)

**Gómez López, R.** (2010). *Generalidades en Auditoría*. Recuperado de:  
<http://www.eumed.net/cursecon/libreria/rgl-genaud/1k.htm>

**Mira Navarro, J.C.** (2006), *Apuntes de Auditoría*. Recuperado de enlace:  
<https://goo.gl/lXnKAr>

# Auditoría de la seguridad



Auditoría de  
Sistemas

UNIVERSIDAD  
**SIGLO 21** | MIEMBRO DE LA RED  
**ILUMNO**



# Auditoría de la seguridad

La norma internacional ISO 27001 establece los pasos necesarios y lineamientos de alto nivel para implementar un sistema integral de gestión de la seguridad de la información (SGSI).

Al considerar que la información es el principal activo para muchas organizaciones, resulta evidente la necesidad de protección para los sistemas que la gestionan. La función de la seguridad es asegurarse de que los sistemas de información sean accedidos y modificados solo por el personal autorizado, quienes solo deben actuar dentro de los límites de su rol.

La seguridad de los sistemas de información tiene los siguientes objetivos:

- **proTEGER LA INTEGRIDAD, EXACTITUD Y CONFIDENCIALIDAD DE LA INFORMACIÓN;**
- **LA PROTECCIÓN DE LOS ACTIVOS ANTE AMENAZAS DE VANDALISMO;**
- **LA PROTECCIÓN DE LOS ACTIVOS ANTE DESASTRES NATURALES;**
- **CONTAR CON PLANES DE CONTINGENCIA PARA LA RECUPERACIÓN DE LOS SISTEMAS.**

La auditoría de la seguridad de los sistemas de información abarca no solo la seguridad informática, que puede llegar a relacionarse únicamente con los equipos y los entornos técnicos, sino también la información en otros soportes y los ambientes donde se desarrollan las operaciones de la organización. La auditoría se enfoca en verificar que los modelos de seguridad estén en consonancia con las nuevas arquitecturas, plataformas y medios de comunicaciones y transmisión de datos.

## Áreas a abarcar en una auditoría de la seguridad

Las siguientes son las áreas de las organizaciones que pueden ser objeto de la auditoría de seguridad. Cabe la aclaración de que estas áreas se encuentran relacionadas entre sí, en muchos casos, con funciones solapadas, y también forman parte de otras auditorías de sistemas que puedan efectuarse:

- controles directivos de la seguridad que incluyan políticas, planes, funciones, estándares, guías, objetivos de control, presupuestos, comité de seguridad y métodos de evaluación de riesgos;
- cumplimiento de las normas, regulaciones y pedidos gubernamentales;
- amenazas físicas como las inundaciones, incendios, terremotos, etcétera;
- mecanismos de control de accesos físicos y lógicos;
- controles para cumplir con las leyes de datos personales.
- redes de comunicaciones y transmisión de datos, antivirus, *firewall*, etcétera;
- el entorno de producción de los sistemas;
- la gestión de los proyectos de desarrollo de *software*;

- la continuidad de las operaciones.

## Auditoría de la seguridad física

Por un lado, se deben analizar las protecciones físicas para la información, los programas, las instalaciones, el equipamiento y las redes. Por otra parte, se deben considerar las medidas de protección para el personal, como son las medidas de evacuación, las alarmas y las salidas de emergencia. La auditoría de seguridad física se enfoca en ver que se cumplan estas medidas para las áreas donde se gestiona y almacena la información de la organización. Los aspectos que los auditores deben considerar en las auditorías de la seguridad física comprenden:

- Locación del centro de procesamiento de datos, de los servidores locales, y en general de cualquier elemento a proteger, como puedan ser los propios terminales, especialmente en zonas de paso, de acceso público, o próximos a ventanas en plantas bajas. Protección de computadoras portátiles, incluso fuera de las oficinas como los aeropuertos, automóviles y restaurantes.
- Estructura, diseño, construcción y distribución de los edificios y plantas.
- Riesgos a los que están expuestos, tanto por agentes externos, casuales o no, como por accesos físicos no controlados.
- Riesgos de incendio, riesgos por agua como los accidentes atmosféricos o averías en los conductos, problemas en el suministro eléctrico, tanto por caídas como por vandalismo.
- Controles, tanto preventivos como de detección, relacionados con los puntos anteriores, así como de acceso basándose en la clasificación de áreas según usuarios, incluso según el día de la semana y el horario.
- Además del acceso, en determinados edificios o áreas debe efectuarse controles para evitar sustituciones o sustracción de equipos, componentes, soportes, documentación u otros activos. Este control deberá incluir tanto a personas externas e internas de la entidad. (Del Peso Navarro, 2008, <https://goo.gl/GWs7n2>)

## Auditoría de la seguridad lógica

El primer punto a verificar en una auditoría son los niveles de acceso a los datos que tienen los empleados. Cada uno debe poder acceder solamente a los programas, aplicativos, bases de datos o transacciones permitidos para su función, de acuerdo con una tabla de accesos establecida para todos los roles de la organización. Esta tabla también debe aclarar los tipos de permisos, como lectura, escritura, ejecución o algún permiso especial.

Al verificar la seguridad lógica de los sistemas es importante estudiar la forma en la que los usuarios de los sistemas se autentican para el ingreso y los procedimientos con los que cuenta la organización para conceder los permisos de ingreso y los perfiles de usuarios. También se deben auditar los procesos de baja de usuarios a los sistemas cuando estos dejen la organización o cambien de funciones dentro de ella.

El método más común para identificarse en los sistemas es la contraseña. Algunos aspectos a evaluar sobre el uso de las contraseñas son:

- La forma de asignar la contraseña inicial y las sucesivas. Algunas organizaciones permiten que los usuarios las elijan, mientras que otras las imponen o proporcionan algún método de asignación.
- La longitud y la composición de los caracteres, por ejemplo, incluir mayúsculas y minúsculas y caracteres especiales.
- Vigencia, dependiendo de la aplicación o criticidad de la información.
- No permitir repetir cierto número de contraseñas anteriores.
- La cantidad de intentos inválidos que se permitirán.
- Métodos para cifrar las contraseñas.
- La responsabilidad individual de los usuarios debe estar establecida por normativa respecto al uso o a la no-cesión de las contraseñas.
- Sistemas de bloqueo de usuario y contraseñas al no ingresar por determinado tiempo.

## Auditoría de la seguridad en el desarrollo de aplicaciones y de producción

Cuando se evalúan los procesos de desarrollo, se debe validar que todos los proyectos hayan obtenido todas las aprobaciones requeridas por procedimientos internos de la organización. Esto puede incluir la revisión por algún comité de cambios o autorizaciones de los clientes.

Otros aspectos que se deben verificar comprenden a los permisos que los desarrolladores tienen sobre los programas, los datos y los entornos de trabajo. Un desarrollador no debe poseer permisos para los ambientes de producción y, en muchos casos, tampoco para los ambientes de test del sistema, principalmente, donde haya una organización formal de testeo.

La implementación de nuevos programas o librerías a producción debe ser debidamente controlada. Pueden incluso participar el comité de control de cambios y los auditores externos, para verificar que cada programa introducido en el ambiente de producción haya obtenido todas las aprobaciones necesarias. En algunos lugares, se contrata a un tercero para que cumpla esta función, para una mayor independencia.

Asimismo, se debe controlar la independencia entre los distintos ambientes de los sistemas, como desarrollo, test de integridad, test de sistema, test de aceptación del usuario y producción, contando con niveles de accesos para cada caso, de acuerdo al puesto del empleado.

## Auditoría de seguridad en producción de datos

En las organizaciones de carácter internacional, existe la función de seguridad de los datos, encargada principalmente de la protección de los datos y la información. Los enfoques que puede tomar la protección de los datos alcanzan a la confidencialidad, la disponibilidad y la integridad. Algunos datos poseen mayor criticidad en uno de los aspectos. Por ejemplo, en los datos regidos por la ley de datos personales, se debe cuidar, en especial, la confidencialidad de la información. En otros casos, la falta de disponibilidad de la información puede generar una pérdida importante, cosa que también podría suceder con la falta de integridad.

La auditoría de seguridad de los datos puede revisar controles existentes en diferentes puntos del ciclo de vida de los datos, que pueden incluir:

- La proveniencia de los datos: para revisar la verificación de errores en la captura de los datos, que puede ser interno o de otra organización, por ingreso manual o por migraciones de sistemas anteriores.
- Procesamiento de los datos: revisar los controles de validación, integridad, almacenamiento, respaldo y recuperación.
- Salidas de los procesos: verificar los controles de errores, conciliación de balances e intentos de fraude en los envíos de información a terceros y en la generación de reportes e informes.
- Tratamiento de la información confidencial cuando ya no sea necesaria.

## Técnicas, métodos y herramientas

En todos los procesos de auditoría, se fijan objetivos, entorno y alcance que tendrán los trabajos. A partir de allí, se planifican las tareas, considerando las fuentes de datos para la auditoría. Estas fuentes pueden ser:

- Políticas, estándares, normas y procedimientos. Planes de seguridad.
- Contratos, pólizas de seguros. Organigrama y descripción de funciones.
- Documentación de aplicaciones. Inventarios: soportes, aplicaciones.
- Descripción de dispositivos relacionados con la seguridad.
- Manuales técnicos de sistemas operativos o de herramientas.
- Topología de redes. Planos de instalaciones.
- Registros: problemas, cambios, visitas, accesos lógicos producidos.

- Entrevistas a diferentes niveles. La observación de las tareas.
- Archivos. Programas. Actas de reuniones relacionadas.
- Documentación de planes de continuidad y sus pruebas.
- Informes de suministradores o consultores. (Del Peso Navarro, 2008, <https://goo.gl/GWs7n2>)

Una vez que se tienen definidas las fuentes de información que se utilizarán, se seleccionan las técnicas, los métodos y las herramientas más adecuadas para el caso particular de la seguridad de la organización auditada. Los métodos y técnicas pueden incluir los cuestionarios, las entrevistas, la observación, el muestreo, las pruebas y la simulación en paralelo con datos reales. Entre las herramientas, es posible nombrar a los programas, las aplicaciones de *software* para auditorías y las CAAT (*Computer Aided Auditing Techniques*). (Del Peso Navarro, 2003).

## Conclusiones de la auditoría de seguridad

Cada vez más, los responsables de los sistemas de información están mostrando su interés en la auditoría y en la seguridad, su filosofía, sus técnicas y métodos, a fin de conocer cuáles son los riesgos que pueden presentarse en su entorno y qué controles deben implementar. En esta época, es fácil reconocer la importancia de invertir en la seguridad para salvaguardar los activos de la organización. Al ver que la auditoría intenta encontrar y corregir vulnerabilidades en los mecanismos de seguridad, resulta lógica su ejecución como parte de las auditorías de los sistemas de información.

Las empresas deben basarse en los estándares y en las mejores prácticas de la industria para obtener los mayores beneficios de sus esfuerzos. Entre estos, podemos nombrar a COBIT (ISACA), que posee como uno de sus objetivos de control garantizar *la seguridad de los sistemas*, y también al estándar ISO 27001, que se conforma como un código internacional de buenas prácticas de seguridad de la información.



## Referencias

**Blanco Encinosa, L. J.** (2005). *Auditoría y Sistemas Informáticos* (pp. 125-152). La Habana, Cuba: Editorial Félix Varela.

**Del Peso Navarro, E.** (2008). *Nuevo reglamento de protección de datos de carácter personal*. Recuperado de: <https://goo.gl/GWs7n2>

**Del Peso Navarro, E.** (2003). *La Seguridad de los datos de carácter personal*. Recuperado de: <https://goo.gl/gESi0o>

# Auditoría de redes y telecomunicaciones

---



Auditoría de  
Sistemas

UNIVERSIDAD

**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**

# » Auditoría de las redes y telecomunicaciones

El modelo OSI es una descripción abstracta para el diseño de comunicaciones por capas y para un protocolo de redes de computadoras. Fue creado por la ISO en 1984. En su forma más básica, divide a la arquitectura de la red en siete capas.

Cuando se efectúa una auditoría de redes, el primer punto que se debe analizar es la función de la administración de las redes y comunicaciones, con el objetivo de determinar si estas funciones están claramente definidas y si comprenden a:

- la gestión de la red, el equipamiento y la normativa de conectividad;
- monitoreo de comunicaciones, el registro y la resolución de problemas;
- la revisión de los costos, la asignación de proveedores de acceso a internet y la selección del equipamiento de red;
- la participación activa en la estrategia de procesos de datos en el establecimiento de estándares para el desarrollo de aplicaciones y en la evaluación de las necesidades de comunicaciones.

Los auditores deben verificar la existencia de lo siguiente, en el área de comunicaciones:

- una gerencia de comunicaciones con autoridad para establecer procedimientos y normativas;
- procedimientos y registros de inventarios y gestión de cambios;
- monitoreo del uso de la red de comunicaciones, gestión de incidencias, resolución de problemas y ajustes del rendimiento;
- control de los costos en las comunicaciones y facturación a los departamentos respectivos;
- participación activa de la gerencia en el diseño de nuevas aplicaciones para mantener las políticas y las normativas.

El siguiente es un ejemplo de una lista de control que podrían usar los auditores de redes, comprobando que:

1. El área responsable de redes y telecomunicaciones en el organigrama tenga autoridad suficiente para dirigir y controlar la función.
2. Haya coordinación organizativa entre la comunicación de datos y la de voz, en caso de estar separadas estas funciones.
3. Existan descripciones del puesto de trabajo, competencias, requerimientos y responsabilidades para el personal involucrado en las comunicaciones.
4. Existan normas en comunicaciones al menos para las siguientes áreas:
  - a. Tipos de equipamiento, como los adaptadores LAN, que pueden ser instalados en la red.
  - b. Procedimientos de autorización para conectar nuevo equipamiento en la red.

- c. Planes y procedimientos de autorización para la introducción de líneas y equipos fuera de las horas normales de operación.
  - d. Procedimientos para el uso de cualquier conexión digital con el exterior, como línea de red telefónica conmutada o Internet.
  - e. Procedimientos de autorización para el uso de exploradores físicos y lógicos (sniffers).
  - f. Control de los equipos
5. Los contratos con proveedores de comunicaciones tienen definidas responsabilidades y obligaciones.
  6. Existen planes de comunicación a largo plazo, incluyendo estrategia de voz y datos.
  7. Existen, si fueren necesarios, planes para comunicaciones a alta velocidad, como fibra óptica, ATM, etc.
  8. Se planifican redes de cableado integral para cualquier nuevo edificio o dependencia que vaya a utilizar la empresa.
  9. El plan general de recuperación de desastres considera el respaldo y recuperación de los sistemas de comunicaciones.
  10. Las listas de inventario cubren todo el equipamiento de comunicaciones de datos, incluyendo módems, controladores, terminales, líneas y equipos relacionados.
  11. Se mantienen los diagramas de red que documentan las conexiones físicas y lógicas entre las comunicaciones y otros equipos de proceso de datos.
  12. Se refleja correctamente, en el registro de inventario y en los diagramas de red, una muestra seleccionada de equipos de comunicaciones, de dentro y de fuera de la sala de computadoras.
  13. Los procedimientos de cambio para equipos de comunicaciones, así como para añadir nuevos terminales o cambios en direcciones, son adecuados y consistentes con otros procedimientos de cambio en las operaciones de proceso de datos.
  14. Existe un procedimiento formal de prueba que cubre la introducción de cualquier nuevo equipo o cambios en la red de comunicaciones.
  15. Para una selección de diversas altas o cambios en la red, de un período reciente, los procedimientos formales de control han sido cumplidos.
  16. Están establecidos ratios de rendimiento que cubren áreas como la de tiempos de respuesta en las terminales y tasas de errores.
  17. Se vigila la actividad dentro de los sistemas online y se realizan los ajustes apropiados para mejorar el rendimiento.
  18. Existen procedimientos adecuados de identificación, documentación y toma de acciones correctivas ante cualquier fallo de comunicaciones.
  19. La facturación de los proveedores de comunicaciones y otros vendedores es revisada regularmente y los cargos con discrepancias se conforman adecuadamente.
  20. Existe un sistema comprensible de contabilidad y cargo en costos de comunicaciones, incluyendo líneas, equipos, y terminales.

21. Los gestores de comunicaciones están informados y participan en la planificación pre-implementación de los nuevos sistemas de información que puedan tener impacto en las comunicaciones.
22. Las consideraciones de planificación de capacidad en comunicaciones son tomadas en cuenta en el diseño e implementación de nuevas aplicaciones. (Del Peso, 2000, <https://goo.gl/syB3LP>)

## Auditoría de redes físicas

La auditoría física de las redes de comunicaciones se enfoca en conocer si la infraestructura e instalaciones físicas se encuentran adecuadamente protegidas respecto a las vulnerabilidades que podrían afectar físicamente a la seguridad de las redes.

Debe registrarse cualquier acceso físico proveniente del exterior de la red interna, para poder instalar los medios necesarios que eviten que vuelvan a ocurrir. Esto se basa en el supuesto de que la red estará a salvo mientras no ocurran accesos físicos desde el exterior. Otro punto que los auditores deben considerar son los planes de contingencia ante desastres, en donde se indique cómo se han de recuperar las comunicaciones, ya sea en forma parcial o total.

Como objetivos de control, los auditores deben verificar la existencia de:

- áreas controladas para los equipos de comunicaciones, previniendo los accesos inadecuados;
- implementación y protección del cableado de datos y las líneas de comunicaciones para evitar accesos físicos;
- controles en los equipos de comunicaciones utilizados para monitorear el tráfico de la red;
- atención específica en la recuperación de los sistemas de comunicación de datos como parte del plan de recuperación de desastre de los sistemas de información.

La lista de controles que los auditores deben verificar en las auditorías físicas de las redes abarca lo siguiente:

1. El equipo de comunicaciones se mantiene en habitaciones cerradas con acceso limitado a personas autorizadas.
2. La seguridad física de los equipos de comunicaciones, tales como que controladores de comunicaciones sean los adecuados para las computadoras de la empresa.
3. Sólo personas con responsabilidad y conocimientos están incluidas en la lista de personas permanentemente autorizadas para entrar en las salas de equipos de comunicaciones.
4. Se toman medidas para separar las actividades de electricistas y personal de tendido y mantenimiento de tendido de líneas telefónicas, así como

sus autorizaciones de acceso, de aquellas del personal bajo control de la gerencia de comunicaciones.

5. En las zonas adyacentes a la salas de comunicaciones, todas las líneas de comunicaciones deben estar fuera de la vista.
6. Las líneas de comunicaciones, en las salas de comunicaciones, armarios distribuidores y terminaciones de los despachos, estarán etiquetados con un código gestionado por la gerencia de comunicaciones, y no por su descripción física o métodos sin coherencia.
7. Existen procedimientos para la protección de cables y bocas de conexión que dificulten en que sean interceptados o conectados por personas no autorizadas.
8. Se revisa periódicamente la red de comunicaciones, buscando intercepciones activas o pasivas.
9. Los equipos de prueba de comunicaciones usados para resolver los problemas de comunicación de datos deben tener propósitos y funciones definidos.
10. Existen controles adecuados sobre los equipos de prueba de comunicaciones usados para monitorizar líneas y fijar problemas incluyendo: Procedimientos restringiendo el uso de estos equipos a personal autorizado y facilidades de traza y registro del tráfico de datos que posean los equipos de monitorización.
11. Procedimientos de aprobación y registro ante las conexiones a líneas de comunicaciones en la detección y corrección de problemas.
12. En el plan general de recuperación de desastres para servicios de información se presta adecuada atención a la recuperación y vuelta al servicio de los sistemas de comunicación de datos.
13. Existen planes de contingencia para desastres que sólo afecten a las comunicaciones, como el fallo de una sala completa de redes.
14. Las alternativas de respaldo de comunicaciones, con las mismas salas o con salas de respaldo, consideran la seguridad física de estos lugares.
15. Las líneas telefónicas usadas para datos, cuyos números no deben ser públicos, tiene dispositivos/procedimientos de seguridad tales como retrollamada, códigos de conexión o interruptores para impedir accesos no autorizados a sistema informático. (Martínez Betancourt, 2015, <https://goo.gl/NdVVS7>)

## Auditoría de redes lógicas

La necesidad actual de las aplicaciones es poder conectar a los equipos con cualquier otro, sin importar el medio físico que los comunica ni los dispositivos instalados, a través de medios exclusivamente lógicos. El problema radica en que si un equipo se dispusiera a enviar tráfico de forma indiscriminada a la red, terminaría bloqueándola por completo. Es por ello que deben definirse medios para monitorear la red y revisar los errores que puedan presentarse o las situaciones anómalas.

Para poder proteger la información que viaja a través de las redes se utiliza la encriptación de los datos, que consiste en un proceso para volver ilegible la información considerada importante. Una vez que la información ha sido encriptada, solo puede ser leída al aplicar una clave. La encriptación se utiliza como una medida de seguridad para almacenar o transferir información delicada que no debería ser accesible por terceros, por ej.: contraseñas, números de tarjetas de créditos, documentación, etc. (Secodata, 2015, <https://goo.gl/8LoN6j>)

## Auditoría de seguridad en comunicación y redes

Esta auditoría verifica que las políticas de seguridad para las redes de datos y comunicaciones reconozcan que toda información transmitida es propiedad de la entidad y no debe utilizarse para fines no autorizados, principalmente, por motivos de seguridad y también de productividad.

Aquí es donde se verifican los mecanismos de cifrado para comunicaciones, para comprobar la eficiencia de los sistemas existentes y recomendar mejoras si fuere necesario. También, se revisan los sistemas de protección contra posibles accesos externos a las redes, tanto preventivos como de detección, incluyendo a los virus que pueden provenir por diferentes vías.

Al mismo tiempo, los usuarios deben tener restricciones de acceso por dominios de red y solo pueden instalar los aplicativos señalados para sus puestos, variando las configuraciones personales según las especificaciones técnicas aprobadas. La auditoría de seguridad de las redes es relevante cuando se trabaja con transferencias electrónicas de dinero, comercio electrónico, pago con tarjetas, etcétera, donde un ataque de vandalismo puede tener serias consecuencias económicas. Otros aspectos a revisar son:

- los tipos de redes;
- conexiones, información trasmisita y los mecanismos de cifrado;
- los tipos de transacciones;
- protecciones físicas y lógicas para terminales y puntos de acceso a la red;
- protecciones para las conversaciones de voz, cuando sean necesarias;
- los controles en la transferencia de archivos, en las puertas de enlace a otras redes, separación de dominios y *firewalls*;
- controles sobre las páginas web, el correo electrónico, el comercio electrónico y otras actividades que se desarrollen sobre Internet.

## Conclusiones sobre la auditoría de redes

Constantemente surgen nuevos fallos de seguridad, nuevos virus, nuevas herramientas que facilitan la intrusión a los sistemas, como así también nuevas y más efectivas tecnologías para prevenir estos problemas. Por todo esto, las actividades de auditorías de las redes deben ser activas, procurando un seguimiento continuo de lo que esté sucediendo con las nuevas tecnologías, cubriendo las nuevas brechas que vayan surgiendo que puedan amenazar nuestros sistemas de información.



## Referencias

**Blanco Encinosa, L. J.** (2005). *Auditoría y Sistemas Informáticos* (pp. 209-211). La Habana, Cuba: Editorial Félix Varela.

**Del Peso, E.** (2000). *Auditoria informática, un enfoque práctico*. Recuperado de enlace: <http://documents.mx/documents/auditoria-de-red-extraxto-de-libro.html>

**Martínez Betancourt, A.** (2015). *Auditoria de Sistemas de TI*. Recuperado de enlace: <http://es.slideshare.net/hannickamrtxbht/plantilla-unidad-ii>

**SECOMDATA.** (2015). *Definición de cifrado (encriptación)*. Recuperado de enlace: [www.secomdata.com/qu%C3%A9-es-el-cifrado-encriptaci%C3%B3n/](http://www.secomdata.com/qu%C3%A9-es-el-cifrado-encriptaci%C3%B3n/)

# Auditoría de las aplicaciones



Auditoría de  
Sistemas

UNIVERSIDAD

**SIGLO 21**

MIEMBRO DE LA RED  
**ILUMNO**



# Auditoría de las aplicaciones

Se usa el término *aplicaciones* para llamar a estos programas, debido a que cada uno posee una aplicación específica para el usuario.

Todas las organizaciones, sin importar su tamaño, ubicación geográfica o industria, utilizan distintos tipos de aplicaciones (programas de *software*) en sus equipos de computadoras, aprovechando estas herramientas para diversos tipos de trabajo que los usuarios de las organizaciones deben realizar.

Dentro de los ejemplos de aplicaciones, encontramos al procesador de texto, las planillas de cálculo, los navegadores web, los administradores de correo electrónico, los juegos, las bases de datos, multimedia, diseño gráfico, presentaciones, gestión de finanzas, compresión de archivos, entre muchos otros.

Las aplicaciones ayudan a automatizar actividades complicadas como la contabilidad, la redacción de textos o la gestión de un comercio. Algunas aplicaciones tienen un propósito específico para resolver una tarea en particular, mientras que otras tienen objetivos más generales y se suelen agrupar en paquetes integrados de *software*, como es el caso del MSOffice.

Las aplicaciones son diferentes a otros tipos de *software* como los siguientes:

- Los programas o *software* del sistema que permiten que las aplicaciones puedan correr en una computadora. Por ejemplo, ensambladores, compiladores, herramientas de administración de archivos y el sistema operativo mismo.
- Los lenguajes de programación, cuyo objetivo es crear programas informáticos.
- Las utilidades que se utilizan para tareas de mantenimiento o de uso general en las computadoras.

Las aplicaciones pueden responder a cuatro tipos de finalidades:

- registrar la información que la organización necesita procesar para su normal funcionamiento;
- procesar la información registrada con cálculos o edición de documentos para producir informes y reportes;
- responder consultas sobre la información almacenada y procesada;
- generar informes para múltiples propósitos, finalidades o criterios.

La auditoría de las aplicaciones se centra en las etapas, donde los sistemas de información se encuentran implementados en la organización y en el funcionamiento productivo. En este punto, ya se han superado las etapas de definición, análisis, diseño, desarrollo, implantación y testeo, tanto del

hardware como de los sistemas operativos, bases de datos y aplicaciones informáticas.

El propósito de auditar las aplicaciones instaladas es analizar el grado de cumplimiento de los objetivos para los que estas fueron creadas o adquiridas. En otras palabras, el diseño es verificar que las aplicaciones sean utilizadas como herramientas operativas y de gestión eficaces, que brinden una contribución eficiente a la organización.

## Problemática de la auditoría de las aplicaciones informáticas

El principal problema que existe con el uso de las aplicaciones es el factor humano que interviene. Hablando en lenguaje informático, es posible decir que las aplicaciones corren en la cima de la pila del *software* del sistema. Esto significa que actúan directamente con los usuarios finales, o sea, las personas. Aquí entra en juego el factor de error que las personas pueden introducir en la información que las aplicaciones procesan. Puede ser por descuidos involuntarios, cansancio, o también por malas intenciones e intentos de fraude.

Por otro lado, si los usuarios utilizan un rigor profesional en el manejo de las aplicaciones, es muy probable lograr el éxito en el desarrollo de las actividades de la organización, en lo que respecta a la gestión de la información.

En las etapas previas a la implementación, se deben analizar minuciosamente las amenazas y riesgos asociados con el uso de las aplicaciones. Para cada una de ellas, se debe establecer medidas de protección para controlar o disminuir los impactos de ocurrencia de los riesgos detectados. Estas medidas corresponden, fundamentalmente, al control interno de dos maneras:

1. Controles manuales: son los que deben efectuar el personal del área donde se encuentren los usuarios de las aplicaciones. Estos controles sirven para reparar y subsanar los errores que hayan podido producirse, principalmente, en la introducción manual de los datos.
2. Controles automáticos: estos son controles incorporados en los programas de aplicación para asegurar que la información se registre y mantenga de forma completa y exacta.

Estos controles también pueden ser clasificados por su finalidad en:

- Controles preventivos: buscan evitar la introducción de errores al exigir el ajuste de los datos ingresados a un formato y estructura de datos como las fechas, números de documentos, CUIL y otros similares.

- Controles detectivos: estos controles intentan descubrir errores después de que hayan sido introducidos al sistema.
- Controles correctivos: buscan corregir todos los errores encontrados por los controles detectivos.

Todos estos controles pueden utilizarse en las transacciones para ingresar datos, en los procesamientos de la información ya introducida en las aplicaciones o en la generación de reportes e informes de salida.

Los auditores internos deben ser invitados a participar activamente en el diseño y la implementación de los controles para las aplicaciones. Ellos tienen que aprobar las revisiones que se realicen y pueden suministrar recomendaciones de mejoras.

La problemática de la auditoría de una aplicación abarca una revisión de la eficacia del funcionamiento de los controles diseñados para cada uno de los pasos de dicha aplicación, frente a los riesgos que tratan de eliminar o minimizar, como medios para asegurar la fiabilidad (totalidad y exactitud), seguridad, disponibilidad y confidencialidad de la información gestionada por la aplicación.

## Herramientas de uso más común en la auditoría de aplicaciones

El principal inconveniente que encuentran los auditores informáticos es la exponencial evolución de la tecnología de los sistemas de información, que los obliga a recibir capacitación constante y especializada sobre las herramientas de auditoría y las nuevas aplicaciones del mercado. Esto se aplica tanto a los auditores internos de las empresas como a los auditores externos, contratados ocasionalmente.

A continuación, se expone una lista de las herramientas más comunes utilizadas en la auditoría de aplicaciones. Estas pueden usarse de manera combinada para aprovechar el tiempo de la auditoría.

- **Entrevistas:** son utilizadas ampliamente en todas las etapas de la auditoría. Ellas deben cumplir con los siguientes requisitos:
  - Las personas entrevistadas deben poder aportar al objetivo de la auditoría.
  - La entrevista debe ser preparada eficientemente para sacar el máximo provecho posible.
  - Tener una agenda de temas a tratar para evitar olvidarse de algún asunto importante.

- Debe ser coordinada con suficiente anticipación para que ambas partes puedan preparar toda la información y la documentación necesarias.
  - Los líderes de los entrevistados deben estar informados. Es recomendable que sean ellos los que informen a los empleados de las entrevistas, a fin de que les expresen la necesidad de participar.
  - El auditor debe tomar notas de toda la información obtenida durante la entrevista.
- 
- **Encuestas:** la mayoría de los requisitos ya nombrados para las entrevistas también se aplican a las encuestas. Estas sirven para determinar el alcance y los objetivos que tendrá la auditoría y para conocer los niveles de satisfacción de los usuarios de las aplicaciones. Una de las diferencias con las entrevistas es que, en las encuestas, se prepara un cuestionario que pueda contestarse con rapidez, al seleccionar entre la lista de respuestas dadas. Actualmente, muchas encuestas se realizan de manera digital: mediante internet, se recibe la invitación por un correo electrónico.
  - **Observación de los usuarios:** si bien pueden utilizarse otros medios para comprobar errores o faltas de los usuarios, los auditores con mayor experiencia pueden hacer uso de la observación para descubrir falta de eficiencia de los controles, en lo que respecta a las aplicaciones, que no pueda ser descubierta por otros medios. Las mejoras que pueden encontrarse con la observación abarcan desde carencias de los usuarios o vicios adquiridos por falta de formación, hasta mejoras de diseño para aumentar la agilidad y productividad en el uso de las aplicaciones.
  - **Pruebas de conformidad:** son actuaciones destinadas a comprobar si ciertos procedimientos, normas o controles internos se encuentran correctamente establecidos y si funcionan de conformidad con lo previsto y esperado.
  - **Pruebas substantivas o de validación:** se utilizan cuando no hay evidencias de que existan controles internos suficientes para garantizar el funcionamiento del sistema esperado. También pueden detectar la presencia o ausencia de errores o irregularidades en los procesos, las actividades, las transacciones o los controles internos. Los errores que estas pruebas pueden detectar incluyen a las transacciones omitidas, no registradas, duplicadas, inexistentes, no autorizadas o mal clasificadas.
  - **Uso del equipamiento:** el auditor debe hacer uso de las computadoras y de los programas de *software* de auditoría comerciales o de desarrollo

propio, no solo para potenciar su trabajo, sino también para examinar las aplicaciones de los sistemas de información auditados.

## **Etapas de la auditoría de aplicaciones**

### **Recolección de información y documentación de las aplicaciones**

El primer paso para efectuar una auditoría de aplicaciones es lograr un conocimiento básico de las aplicaciones que posee la organización y del entorno informático donde están instaladas. Esto se puede obtener a través de un estudio previo donde se puedan determinar los puntos débiles y funciones con posibles riesgos.

### **Determinación de los objetivos y alcance de la auditoría**

Una vez que el auditor ha recopilado información y documentación obtenidas con las entrevistas y las observaciones realizadas, se encuentra en posición de definir los objetivos de la auditoría de las aplicaciones. Basándose en los riesgos y puntos débiles encontrados, el auditor debe preparar el plan de trabajo a realizar, dedicando más recursos a las debilidades más importantes o a las que posean consecuencias mayores si llegan a materializarse.

Es conveniente que este plan de auditoría contemple los siguientes apartados: planificación de las tareas, herramientas y métodos, programa de trabajo detallado, test de confirmación, datos y resultados.

### **Planificación de la auditoría**

Como toda auditoría, la de las aplicaciones debe ser cuidadosamente planificada, tratando de determinar el momento más oportuno para su realización. Por ejemplo, no es conveniente efectuar la auditoría en el período de implementación, dado que es un momento crítico en el que los usuarios se están adaptando a las nuevas aplicaciones. Asimismo, en el período próximo a la implantación, se suelen detectar pequeñas fallas en las aplicaciones que pueden llegar a sesgar la auditoría.

## **Trabajo de campo, informe e implementación de mejoras**

Las etapas de realización de la auditoría de aplicaciones, redacción de los informes con las sugerencias de mejoras y su posterior implementación no son diferentes de los demás trabajos de auditoría.

## **Conclusiones sobre la auditoría de aplicaciones**

La importancia de esta auditoría radica en el avance tecnológico constante que exige un esfuerzo de capacitación por parte de los auditores, a fin de poder ayudar a que las organizaciones controlen un entorno cada vez más amenazado por nuevos riesgos, implicados en las mismas tecnologías.



## Referencias

**Blanco Encinosa, L. J.** (2005). *Auditoría y Sistemas Informáticos* (pp. 102-122). La Habana, Cuba: Editorial Félix Varela.