Seguridad y Auditoría Informática

Auditoría Informática

Ing. Alfredo Pardo

Año 2021

Tabla de Contenidos

Auditoría Informática

Concepto de Auditoría

Es la actividad que consiste en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido dispuestas.

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican:

1. **Contenido**: Una **opinión**
2. **Condición**: **profesional**
3. **Justificación**: Sustentada en determinados **procedimientos**
4. **Objeto**: Una determinada información obtenida desde un cierto soporte
5. **Finalidad**: Determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su **fiabilidad**

Es una función que se efectúa **a posteriori**, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

Clases de Auditoría

El objeto y la finalidad distinguen de qué clase o tipo de auditoría se trata. El objeto sometido a estudio, sea cual sea su soporte, por una parte, y la finalidad con que se realiza el estudio, definen el tipo de auditoría de que se trata. Ejemplos:

Clase	Contenido	Objeto	Finalidad
Financiera	Opinión	Cuentas Anuales	Presentan realidad
Informática	Opinión	Sistemas de aplicación, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente y según normas establecidas
Gestión	Opinión	Dirección	Eficacia, eficiencia, rendimiento económico
Cumplimiento	Opinión	Normas establecidas	Las operaciones están alineadas a estas normas

Procedimientos

La opinión profesional se fundamenta y justifica por medio de procedimientos específicos tendientes a proporcionar una seguridad razonable de lo que se afirma. Cada una de las clases o tipos de auditoría posee sus propios procedimientos para alcanzar el fin previsto. El alcance de la auditoría viene dado por los procedimientos. La amplitud y profundidad de los procedimientos que se apliquen nos definen su alcance.

En las auditorías altamente reglamentadas como la financiera es obligatorio “aplicar las Normas Técnicas y decidir los procedimientos de auditoría”. “Cualquier limitación que impida la aplicación de lo dispuesto en las Normas Técnicas debe ser considerada en el Informe de auditoría como una reserva al alcance”.

Se pretende garantizar que se toman en consideración todos los aspectos, áreas, elementos, operaciones, circunstancias, etc. que sean significativas.

Para ello, se establecen normas y procedimientos que se resumen en que:

- El trabajo se planificará apropiadamente y se supervisará adecuadamente.
- Se estudiará y evaluará el sistema de control interno.
- Se obtendrá evidencia suficiente y adecuada.

Ante la llamada revolución cuantitativa en el que las operaciones se multiplicaron enormemente, el método tradicional resultó laborioso, tedioso, largo, ineficaz y económicamente inviable. No era posible verificar la totalidad de las operaciones y, por lo tanto, había que reducir el campo de acción del auditor a parte de la numerosa información. Esto trajo implícito un riesgo evidente, al no verificarse la totalidad de los movimientos y que escapara de la atención del auditor alguna irregularidad.

El auditor tiene la misión de mantener el riesgo de que esto ocurra dentro de límites tolerables. Esto podría representarse de forma aritmética como:

R(c) * R(d) = S(e)

R(c) = Riesgo en el proceso o riesgo de control

R(d) = Riesgo de detección

S(e) = Constante o parámetro admisible en que se desea mantener el riesgo de auditoría

Es inmediato el hecho de que el riesgo de control y el riesgo de detección dentro de la ecuación planteada son inversamente proporcionales. Si añadimos que el riesgo de control es ajeno al auditor, pues depende de las normas establecidas por la entidad en su sistema, es evidente que para definir el riesgo de detección que está dispuesto a admitir, debe evaluarse primero el riesgo de control existente.

El riesgo final del auditor es una combinación de dos riesgos separados:

- El primero de éstos está constituido por aquellos errores de importancia que ocurran en el proceso.
- El segundo riesgo es de que cualquier error de importancia que pueda existir sea o no detectado por el examen del auditor.

El auditor confía en:

- El control interno establecido por la entidad auditada para reducir el primer riesgo.
- En sus pruebas de detalle y en sus otros procedimientos para disminuir el segundo.

Variación del Objeto

La gestión de las entidades ha experimentado un cambio sustancial y hoy se utiliza la TI (Tecnología de la Información) en prácticamente todas las áreas de la empresa. Se ha introducido un nuevo elemento cualitativo en el objeto de la auditoría, el uso de la informática como factor consustancial a la gestión, con la introducción de la Tecnología de la Información (TI) en los sistemas, muy probablemente basada en las ventajas que aporta la informatización con respecto al trabajo manual, entre las que se podrían distinguir:

	Manual	**Automatizado**
Costo de Explotación	Alto	Bajo
Costo de Operación	Alto	Bajo
Rendimiento Continuo	Disminuye	Aumenta
Consistencia	Poca	Excelente
Capacidad de Cálculo	Buena	Pobre
Reacción ante lo Inesperado	Buena	Pobre
Sentido Común	Excelente	Pobre
Lenguaje	Bueno	Pobre

El auditor debe trabajar ante y con elementos de Tecnología de la Información. Dado que según sus propias Normas Técnicas de auditoría que regulan su actuación el auditor debe tener en cuenta todos los elementos de la entidad incluso los informáticos, el cumplir con esta función no es una decisión del auditor sino una obligación definida por la Norma. Si este requisito no puede cumplirse, el auditor se verá obligado a introducir una limitación al alcance de su trabajo.

La TI proporciona medios para ejecutar los procedimientos de forma eficiente y directa. Las CAATS (Técnicas de Auditoría asistidas por computadora) ponen a disposición del auditor una amplia variedad de herramientas que no sólo viabilizan los nuevos procedimientos sino que mejoran sensiblemente su aplicación y amplían la gama disponible.

La introducción de la TI afecta a los auditores de una forma dual:

- Cambia el soporte del objeto de su actividad.
- Posibilita la utilización de medios informatizados (CAATs) para la realización de sus procedimientos.

Concepto de Consultoría

La consultoría consiste en “dar asesoramiento o consejo sobre lo que se debe hacer o cómo llevar adecuadamente una determinada actividad para obtener los fines deseados”.

Los elementos de la consultoría podrían resumirse en:

1. **Contenido**: Dar asesoramiento o consejo
2. **Condición**: De carácter especializado
3. **Justificación**: En base a un examen o análisis
4. **Objeto**: La actividad o cuestión sometida a consideración
5. **Finalidad**: Establecer la manera de llevarla a cabo adecuadamente

Es una función a priori con el fin de determinar cómo llevar a cabo una función o actividad de forma que obtenga los resultados pretendidos. La auditoría verifica a posteriori si estas condiciones, una vez realizada esta función o actividad, se cumplen y los resultados pretendidos se obtienen realmente.

Podríamos relacionar los siguientes tipos o clases de consultoría:

Clase	Contenido	Objeto	Finalidad
Financiera	Asesoramiento	Planes de Cuentas, Procedimientos administrativos	Diseño e Implementación
Informática	Asesoramiento	Aplicaciones, Planes de Contingencia	Desarrollo, Diseño e Implementación

Especialmente el primer elemento distingue claramente la auditoría de la consultoría. Dependiendo de que su contenido sea opinar sobre resultados vs. dar asesoramiento o consejo en relación con una actividad a desarrollar, se tratará de auditoría o consultoría.

Las definiciones de auditoría informática tienden a englobar el concepto de consultoría. Dentro del abanico de definiciones, podemos citar:

1. La auditoría informática, que es una parte integrante de la auditoría, se estudia por separado para tratar problemas específicos y para aprovechar los recursos de personal. La auditoría informática debe realizarse dentro del marco de la auditoría general. El cometido de la auditoría informática se puede dividir en:
    a. Un estudio del sistema y un análisis de los controles organizativos y operativos del departamento de informática.
    b. Una investigación y análisis de los sistemas de aplicación que se estén desarrollando o que ya estén implementados.
    c. La realización de auditorías de datos reales y de resultados de los sistemas que se estén utilizando.
    d. La realización de auditorías de eficiencia y eficacia.
2. La revisión de la propia informática y de su entorno. Las actividades a que da lugar esta definición pueden ser:
    a. Análisis de riesgos.
    b. Planes de contingencia.
    c. Desarrollo de aplicaciones.
    d. Asesoramiento en paquetes de seguridad.
    e. Revisión de controles y cumplimiento de los mismos, así como las normas legales aplicables.
    f. Evaluación de la gestión de los recursos informáticos.
3. Un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.

La Informática como Herramienta de Auditoría

Grado de Informatización

En cuanto al objeto de la auditoría puede considerarse desde el uso de un Equipo con un par de aplicaciones básicas hasta un sistema complejo.

Entre los procedimientos (técnicas) que las normas de ejecución de la auditoría establecen se destacan la inspección, observación, averiguación, confirmación, cálculo y análisis. De estas seis, al menos cuatro se ejecutan de forma más eficiente con medios informáticos:

- **Inspección**: como la comparación de datos en dos archivos o cuentas distintas, conciliaciones.
- **Cálculo**: de amortizaciones, provisiones, ratios, etc.
- **Análisis**: regresiones o datos que cumplan determinadas condiciones.
- **Confirmación**: cálculo estadístico, selección y emisión de muestras, cumplimiento, etc.

Mejora de las Técnicas Habituales

El auditor puede valerse sustancialmente de las diversas herramientas informáticas que tiene a su disposición y que podríamos catalogar de la siguiente forma:

Tipo	Planificación de la Auditoría	Ejecución de la Auditoría
General	● Procesadores de Texto ● Flowcharting ● Utilidades	● Procesadores de Texto ● Hojas de Cálculo
Acceso Directo		● ACL (Audit Command Language)
Específico	Generadores de Papeles de Trabajo	● Simulación paralela ● Revisión analítica
Especializados	Integradores	● Sistemas Expertos ● Test Check (Muestra Aleatoria)

De manera breve, podemos reseñar los objetivos que se cubren con la utilización de las diversas herramientas enumeradas:

- **Tratamiento de textos**: utilizado generalmente en la práctica como una máquina de escribir super-automatizada para circulares, memorandos, memoria, etc. Con una mayor especialización, permite automatizar operaciones, generar documentos, relacionar diversos documentos, etc.
- **Hojas de Cálculo**: utilizada para efectuar cálculos, automatizar resultados de diferentes documentos numéricos y en algunos casos obtención de ratios, etc., así como generar actualizaciones automáticas, importar archivos de otras aplicaciones, y producir gráficos disponiendo de una amplia gama de fórmulas financieras, económicas, etc.
- **Generador de Papeles de Trabajo**: fundados esencialmente en el tratamiento de textos de donde se obtienen planillas, formatos, etc.; permite edición y actualización. Clasifica los documentos por áreas, sectores, personal involucrado, etc.
- **Flowcharting**: produce diagramas representativos de funciones realizadas o a realizar, flujo de documentos, etc.

- **Utilidades**: existe una amplia gama que cubre desde comunicaciones, visualizadores de archivos, búsquedas o incluso rectificadores de archivos.
- **Administradores**: efectúan el seguimiento administrativo de las auditorías. Horas empleadas, áreas, control presupuestario, etc.
- **Acceso Directo**: las aplicaciones de acceso directo adoptan como archivos propios los realizados por otras aplicaciones

Los archivos de datos son exactamente los existentes en el auditado, es decir los archivos físicos de la firma auditada, de la forma y con la codificación con que hayan sido grabados. Estos datos no cambian. ACL crea para su tratamiento el "documento" que contiene la información necesaria en cuanto a definiciones del formato del archivo de datos, batches, índices, vistas y espacio de trabajo.

La definición del formato contiene la estructura y contenido del archivo de datos. Incluye información como nombre de los campos, codificación de los datos, márgenes donde comienzan y dónde terminan. Con esta información ACL es capaz de leer e interpretar el archivo de datos original a auditar. ACL puede manipular los datos del archivo prácticamente de cualquier forma o manera: Ordenar, Establecer fechas, Extraer según condiciones, Estadísticas, Muestras, Clasificar, Contar, Agregar, Totalizar, Estratificar, Comparar.

Sistemas Expertos

Las aplicaciones más avanzadas en cualquier campo son las conocidas como sistemas expertos relativos también a la llamada inteligencia artificial. Se trata de usar la computadora para que proporcione resultados o conclusiones producto del procesamiento de datos específicos en base a conocimientos preexistentes en el mismo.

En el campo de la auditoría su utilización más evidente es en el análisis y evaluación del control interno.

Los fundamentos de un sistema experto consisten en crear cuestionarios cuya respuesta sea "sí" o "no" para evitar matices opinables, divididos por área de actividad y que se parta de la base de que una totalidad de respuestas positivas implica un sistema excelente. Menos de un determinado nivel implicaría un control débil o muy débil.

Debe incorporar las pruebas de cumplimiento correspondientes cuya cantidad se designe por medios estadísticos y que sirvan sus respuestas como retroalimentación para una clasificación definitiva del sistema.

Ésta clasificación a su vez proporciona un tamaño de muestra para las pruebas sustantivas a realizar así como una definición de las mismas.

Destacan entre sus ventajas, siempre bajo la supervisión del auditor: la objetividad del sistema, la utilización de fórmulas estadísticas, la cuantificación y especificación de pruebas de cumplimiento y sustantivas adecuadas, la actualización de la base de conocimiento con los nuevos sistemas analizados y el soporte legal que implica en caso de litigio.

Test Check

Esta práctica, cada vez en menor uso, consiste en introducir en la aplicación que el auditado utilice un conjunto de valores cuyo resultado se conoce. Estos valores se comparan con los que eventualmente proporcione la aplicación.

Integradores

Son aquellas aplicaciones que interrelacionan todas las demás para crear un entorno único que utiliza la totalidad de la información obtenida a través de las diferentes herramientas creando un “sistema de auditoría”.

Varias de las aplicaciones mencionadas proporcionan medios de programación o, sin ser tan ambiciosos, la posibilidad de crear “batches” de funcionamiento automático. Estos batches o conjuntos de instrucciones pueden operar conjuntamente brindando la posibilidad de realizar operaciones complejas de forma directa y cómoda.

Si tomamos en consideración el proceso completo de auditoría financiera -desde las normas y procedimientos establecidos para antes del propio inicio de la auditoría como la propuesta, contrato, cálculo de costos hasta el informe y recomendaciones finales pasando naturalmente por los procedimientos de ejecución de la auditoría, incluyendo el sistema experto, el acceso directo a archivos informáticos, las pruebas analíticas y adicionales o puntuales que el auditor debe llevar a cabo, y las integramos en un sistema que automatice tanto las actualizaciones pertinentes en base a los cambios introducidos como la emisión y ordenación de papeles de trabajo justificativos de los procedimientos aplicados-, tendremos un sistema o metodología de integración que sitúa en un sólo entorno las diversas fases, documentos, resultados, actualizaciones, etc. de una auditoría. A todo este proceso es a lo que denominaríamos un integrador.

Evolución

En la hipótesis de evolución de los sistemas de auditoría automatizados, se han distinguido diferentes etapas o niveles:

- **Nivel 1**: Reducción de Costos
- **Nivel 2**: Aumento de la Calidad
- **Nivel 3**: Nuevos productos dependientes de la TI
- **Nivel 4**: Gestión Estratégica basada en la TI
- **Nivel 5**: Nuevos Conceptos y Paradigmas basados en la TI

Control Interno y Auditoría Informática

La mayoría de las organizaciones han lanzado varias iniciativas para reforzar el control interno, tales como:

- La reestructuración de los procesos empresariales (BPR - Business Process Re-engineering).
- La gestión de la calidad total (TQM - Total Quality Management).
- El redimensionamiento por reducción y/o por aumento del tamaño hasta el nivel correcto.
- La contratación externa (outsourcing).
- La descentralización.

Las tendencias externas que influyen sobre las empresas son, entre otras, las siguientes:

- La globalización.
- La diversificación de actividades.
- La eliminación de ramas de negocio no rentables o antiguas.
- La introducción de nuevos productos como respuesta a la competencia.
- Las fusiones y la formación de alianzas estratégicas.

Los directivos deben tomar conciencia de que para evitar fallos de control significativos deben reevaluar y reestructurar sus sistemas de controles internos. Deben actuar de manera proactiva para garantizar que los controles internos de la empresa están adecuadamente diseñados para hacer frente a los retos del futuro y asegurar la integridad en el momento actual.

Los auditores informáticos aportan conocimientos especializados, así como su familiaridad con la tecnología informática. Se siguen tratando las mismas cuestiones de control en la

auditoría, pero los especialistas en auditoría informática de sistemas basados en computadores prestan una ayuda valiosa a la Organización y a los otros auditores en todo lo relativo a los controles sobre dichos sistemas.

En muchas organizaciones, el auditor ha dejado de centrarse en la evaluación y la comprobación de los resultados de procesos, desplazando su atención a la evaluación de riesgos y la comprobación de controles. Muchos de los controles se incorporan en programas informáticos o se realizan por parte de la función informática de la organización, representado por el Control Interno Informático.

Las Funciones de Control Interno y Auditoría Informáticos

Control Interno Informático

El Control Interno Informático se ocupa diariamente de que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales.

Control Interno Informático suele ser un órgano staff de la Dirección del Departamento de Informática y está dotado de las personas y medios materiales proporcionados a los cometidos que se le encomienden.

Como principales objetivos, podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas.
- Definir, establecer y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático. Cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implementación de las métricas adecuadas.

Realiza en los diferentes sistemas (centrales, departamentales, redes locales, PC’s, etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes actividades operativas sobre:

- El cumplimiento de procedimientos, normas y controles dictados. Merece resaltarse el seguimiento sobre el control de cambios y versiones del software.
- Controles sobre la producción diaria.

- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del software y del servicio informático.
- Controles en las redes de comunicaciones.
- Controles sobre el software de base.
- Controles en los sistemas microinformáticos.
- La seguridad informática (su responsabilidad puede estar asignada a control interno o bien puede asignársele la responsabilidad de control dual de la misma cuando está encargada a otro órgano):
    - Usuarios, responsables y perfiles de uso de archivos y bases de datos.
    - Normas de seguridad.
    - Control de información clasificada.
    - Control dual de la seguridad informática.
    - Licencias y relaciones contractuales con terceros.
    - Asesorar y transmitir cultura sobre el riesgo informático.

Auditoría Informática

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado protege los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo, la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso de software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas asistidas por computadora.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implementados y sobre la fiabilidad de la información suministrada.

Se pueden establecer tres grupos de funciones a realizar por un auditor informático:

- Participar en las revisiones durante y después del diseño, realización, implementación y explotación de aplicaciones informáticas, así como en las fases análogas de realización de cambios importantes.
- Revisar y juzgar los controles implementados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

Control Interno y Auditoría Informática: Campos Análogos

Aunque ambas figuras tienen objetivos comunes, existen diferencias que conviene matizar:

	Control Interno Informático	**Auditoría Informática**
Similitudes	● Personal Interno ● Conocimientos Especializados en Tecnología de la Información ● Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección General para los sistemas de información	
Diferencias	● Análisis de los controles en el día a día ● Informa a la Dirección del Departamento de Informática ● Sólo personal interno ● El alcance de sus funciones es únicamente sobre el Departamento de Informática	● Análisis de un momento informático determinado ● Informa a la Dirección General de la Organización ● Personal interno y/o externo ● Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización

Sistemas de Control Interno Informático

Definición y Tipos de Controles Internos

Se puede definir el control interno como “cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos”.

Los controles cuando se diseñen, desarrollen e implementen deben ser al menos completos, simples, fiables, revisables, adecuados y rentables.

Para asegurar la integridad, disponibilidad y eficacia de los sistemas se requieren complejos mecanismos de control, la mayoría de los cuales son automáticos. Los objetivos de los controles informáticos se han clasificado en las siguientes categorías:

- **Controles preventivos**: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- **Controles detectivos**: cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.
- **Controles correctivos**: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un archivo dañado a partir de las copias de seguridad.

Implementación de un Sistema de Controles Internos Informáticos

Los controles pueden implementarse a varios niveles diferentes. La evaluación de los controles de la Tecnología de la Información exige analizar diversos elementos interdependientes. Por ello es importante llegar a conocer bien la configuración del sistema, con el objeto de identificar los elementos, productos y herramientas que existen para saber dónde pueden implementarse los controles, así como para identificar posibles riesgos.

Para llegar a conocer la configuración del sistema es necesario documentar los detalles de la red, así como los distintos niveles de control y elementos relacionados:

- **Entorno de red**: esquema de la red, descripción de la configuración de hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los computadores de entornos de base que soportan aplicaciones críticas y consideraciones relativas a la seguridad de la red.

- **Configuración de los Equipos**: configuración del soporte físico, entorno del sistema operativo, software con particiones, entornos (prueba y real), bibliotecas de programas y conjuntos de datos.
- Entorno de aplicaciones: procesos de transacciones, sistemas de gestión de bases de datos y entornos de procesos distribuidos.
- **Productos y Herramientas**: software para el desarrollo de programas, software de gestión de bibliotecas y para operaciones automáticas.
- **Seguridad de los Equipos**: Identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, etc.

Para establecer un sistema de controles internos informáticos habrá que definir:

- **Gestión de sistemas de información**: políticas, pautas y normas técnicas que sirvan de base para el diseño y la implementación de los sistemas de información y de los controles correspondientes.
- **Administración de sistemas**: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.
- **Seguridad**: incluye las tres clases de controles fundamentales implementados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.
- **Gestión del cambio**: separación de las pruebas y la producción a nivel de software y controles de procedimientos para la migración de programas software aprobados y probados.

La implementación de una política y cultura sobre la seguridad requiere que sea realizada por fases y esté respaldada por la Dirección. Cada función juega un papel importante en las distintas etapas:

- **Dirección de Negocio o Dirección de Sistemas de Información (S.I.)**: Debe definir la política y/o directrices para los sistemas de información en base a las exigencias del negocio, que podrían ser internas o externas.
- **Dirección de Informática**: Debe definir las normas de funcionamiento del entorno informático y de cada una de las funciones de Informática mediante la creación y publicación de procedimientos, estándares, metodología y normas, aplicables a todas las áreas de Informática, así como a los usuarios, que establezcan el marco de funcionamiento.
- **Control Interno Informático**: Debe definir los diferentes controles periódicos a realizar en cada una de las funciones informáticas, de acuerdo al nivel de riesgo de cada una de ellas, y ser diseñados conforme a los objetivos de negocio y dentro del marco legal aplicable. Éstos se plasmarán en los oportunos procedimientos de control interno y podrán ser preventivos o de detección. Realizará periódicamente la revisión de los controles establecidos de Control Interno Informático informando de las desviaciones a la Dirección de Informática y sugiriendo cuantos cambios serán

convenientes en los controles, así como transmitirá constantemente a toda la organización de informática la cultura y políticas del riesgo informático.

- **Auditor Interno/externo informático**: Debe revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa, de acuerdo al nivel de riesgo, conforme a los objetivos definidos por la Dirección del Negocio y la Dirección de Informática. Informará a la alta dirección de los hechos observados y al detectarse deficiencias o ausencias de controles recomendarán acciones que minimicen los riesgos que pueden originarse.

A continuación se indican algunos controles internos para sistemas de información, agrupados por secciones funcionales, y que serían los que Control Interno Informático y Auditoría Informática deberían verificar para determinar su cumplimiento y validez:

1. **Controles generales organizativos**
    a. **Políticas**: deberán servir de base para la planificación, control y evaluación por la Dirección de las actividades del Departamento de Informática
    b. **Planificación**
        i. Plan Estratégico de Información, realizado por los órganos de la Alta Dirección de la Empresa donde se definen los procesos corporativos y se considera el uso de las diversas tecnologías de información así como las amenazas y oportunidades de su uso o de su ausencia.
        ii. Plan Informático, realizado por el Departamento de Informática, determina los caminos precisos para cubrir las necesidades de la Empresa plasmandose en proyectos informáticos.
        iii. Plan General de Seguridad (física y lógica), que garantice la confidencialidad, integridad y disponibilidad de la información.
        iv. Plan de emergencia ante desastres, que garantice la disponibilidad de los sistemas ante eventos.
    c. **Estándares**: que regulen la adquisición de recursos, el diseño, desarrollo y modificación y explotación de sistemas.
    d. **Procedimientos**: que describan la forma y las responsabilidades de ejecución para regular las relaciones entre el Departamento de Informática y los departamentos usuarios.
    e. Organizar el Departamento de Informática en un nivel suficientemente superior de estructura organizativa como para asegurar su independencia de los departamentos usuarios.
    f. Descripción de las funciones y responsabilidades dentro del Departamento con una clara separación de las mismas.
    g. **Políticas de personal**: selección, plan de formación, plan de vacaciones y evaluación y promoción.
    h. Asegurar que la Dirección revisa todos los informes de control y resuelve las excepciones que ocurran.

i. Asegurar que existe una política de clasificación de la información para saber dentro de la Organización qué personas están autorizadas y a qué información.
j. Designar oficialmente la figura de Control Interno Informático y de Auditoría Informática (dependiendo del tamaño del Departamento de Informática).

2. **Controles de desarrollo, adquisición y mantenimiento de sistemas de información**: para que permitan alcanzar la eficacia del sistema, economía y eficiencia, integridad de los datos, protección de los recursos y cumplimiento con las leyes y regulaciones.
    a. **Metodología del ciclo de vida del desarrollo de sistemas**: su empleo podrá garantizar a la alta Dirección que se alcanzarán los objetivos definidos para el sistema. Éstos son algunos controles que deben existir en la metodología:
        i. La alta Dirección debe publicar una normativa sobre el uso de metodología de ciclo de vida del desarrollo de sistemas y revisar ésta periódicamente.
        ii. La metodología debe establecer los papeles y responsabilidades de las distintas áreas del Departamento de Informática y de los usuarios, así como la composición y responsabilidades del equipo del proyecto.
        iii. Las especificaciones del nuevo sistema deben ser definidas por los usuarios y quedar escritas y aprobadas antes de que comience el proceso de desarrollo.
        iv. Debe establecerse un estudio tecnológico de viabilidad en el cual se formulen formas alternativas de alcanzar los objetivos del proyecto acompañadas de un análisis costo-beneficio -de cada alternativa-.
        v. Cuando se seleccione una alternativa debe realizarse el plan director del proyecto. En dicho plan deberá existir una metodología de control de costos.
        vi. Procedimientos para la definición y documentación de especificaciones de: diseño, de entrada, de salida, de archivos, de procesos, de programas, de controles de seguridad, de pistas de auditoría, etc.
        vii. Plan de validación, verificación y pruebas.
        viii. Estándares de prueba de programas, de prueba de sistemas.
        ix. Plan de Conversión: prueba de aceptación final.
        x. Los procedimientos de adquisición de software deberán seguir las políticas de adquisición de la Organización y dichos productos debieran ser probados y revisados antes de pagar por ellos y ponerlos en uso.
        xi. La contratación de programas de servicios de programación a medida debe estar justificada mediante una petición escrita de un director de proyecto.

xii. Deberán prepararse manuales de operación y mantenimiento como parte de todo proyecto de desarrollo o modificación de sistemas de información, así como manuales de usuario.

b. **Explotación y mantenimiento**: el establecimiento de controles asegurará que los datos se tratan de forma congruente y exacta y que el contenido de sistemas sólo será modificado mediante autorización adecuada. Éstos son algunos de los controles que se deben implementar:
   i. Procedimientos de control de explotación.
   ii. Sistema de contabilidad para asignar a usuarios los costos asociados con la explotación de un sistema de información.
   iii. Procedimientos para realizar un seguimiento y control de los cambios de un sistema de información.

c. **Controles de explotación de sistemas de información**
   i. **Planificación y Gestión de recursos**: definir el presupuesto operativo del Departamento, Plan de adquisición de equipos y gestión de la capacidad de los equipos.
   ii. **Controles para usar, de manera efectiva los recursos en computadores**:
      1. Calendario de carga de trabajo.
      2. Programación de personal.
      3. Mantenimiento preventivo del material.
      4. Gestión de problemas y cambios.
      5. Procedimientos de facturación a usuarios.
      6. Sistema de gestión de la biblioteca de soportes.
   iii. **Procedimientos de selección del software del sistema, de instalación, de mantenimiento, de seguridad y control de cambios**.
   iv. **Seguridad física y lógica**:
      1. Definir un grupo de seguridad de la información, siendo una de sus funciones la administración y gestión del software de seguridad, revisar periódicamente los informes de violaciones y actividad de seguridad para identificar y resolver incidentes.
      2. Controles físicos para asegurar que el acceso a las instalaciones del Departamento de Informática queda restringido a las personas autorizadas.
      3. Las personas externas a la Organización deberán ser acompañadas por un miembro de la plantilla cuando tengan que entrar en las instalaciones.
      4. Instalación de medidas de protección contra el fuego.
      5. Formación y concientización en procedimientos de seguridad y evaluación del edificio.

6. Control de acceso restringido a los computadores mediante la asignación de un identificador de usuario con palabra clave personal e intransferible.
7. Normas que regulen el acceso a los recursos informáticos.
8. Existencia de un plan de contingencias para el respaldo de recursos de computador críticos y para la recuperación de los servicios del Departamento Informático después de una interrupción imprevista de los mismos.

d. **Controles en aplicaciones**: cada aplicación debe llevar controles incorporados para garantizar la entrada, actualización, validez y mantenimiento completos y exactos de los datos. Las cuestiones más importantes en el control de los datos son:
   i. **Control de entrada de datos**: procedimientos de conversión y de entrada, validación y corrección de datos.
   ii. **Controles de tratamiento de datos**: para asegurar que no se den de alta, modifican o borran datos no autorizados para garantizar la integridad de los mismos mediante procesos no autorizados.
   iii. **Controles de salidas de datos**: sobre la consistencia de salidas, procedimientos de distribución de salidas, de gestión de errores en las salidas, etc.

e. **Controles específicos de ciertas tecnologías**
   i. **Controles en Sistemas de Gestión de Bases de Datos**: El software de gestión de bases de datos para prever el acceso a, la estructuración de, y el control sobre los datos compartidos, deberá instalarse y mantenerse de modo tal que asegure la integridad del software, las bases de datos y las instrucciones de control que definen el entorno.
      1. Que están definidas las responsabilidades sobre la planificación, organización, dotación y control de los activos de datos, es decir, un administrador de datos.
      2. Que existen procedimientos para la descripción y los cambios de datos así como para el mantenimiento del diccionario de datos.
      3. Controles sobre el acceso a datos y concurrencia.
      4. Controles para minimizar fallos, recuperar el entorno de las bases de datos hasta el punto de la caída y minimizar el tiempo necesario para la recuperación.
      5. Controles para asegurar la integridad de los datos, programas de utilidad para comprobar los enlaces físicos -punteros- asociados a los datos, registros de control para mantener los balances transitorios de transacciones para su posterior contraste con totales generados por el usuario o por otros sistemas.

ii. **Controles en informática distribuida y redes**:

1. Planes adecuados de implementación, conversión y pruebas de aceptación para la red.
2. Existencia de un grupo de control de red.
3. Controles para asegurar la compatibilidad de conjunto de datos entre aplicaciones cuando la red es distribuida.
4. Procedimientos que definan las medidas y controles de seguridad a ser usados en la red de informática en conexión con la distribución del contenido de bases de datos entre los departamentos que usan la red.
5. Que se identifican todos los conjuntos de datos sensibles de la red y que se han determinado las especificaciones para su seguridad.
6. Existencia de inventario de todos los activos de la red.
7. Procedimientos de respaldo del hardware y del software de la red.
8. Existencia de mantenimiento preventivo de todos los activos.
9. Que existen controles que verifican que todos los mensajes de salida se validan de forma rutinaria para asegurar que contienen direcciones de destino válidas.
10. Controles de seguridad lógica: control de acceso a la red, establecimiento de perfiles de usuario.
11. Procedimientos de cifrado de información sensible que se transmite a través de la red.
12. Procedimientos automáticos para resolver cierres del sistema.
13. Monitorización para medir la eficiencia de la red.
14. Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación local dentro de la organización.
15. Detectar la correcta o mala recepción de mensajes.
16. Identificar los mensajes por una clave individual de usuario, por terminal, y por el número de secuencia del mensaje.
17. Revisar los contratos de mantenimiento y el tiempo medio de servicio acordados con el proveedor con objeto de obtener una cifra de control constante.
18. Determinar si el equipo multiplexor/concentrador/procesador frontal remoto tiene lógica redundante y poder de respaldo con realimentación automática para el caso que falle.
19. Asegurarse que haya procedimientos de recuperación y reinicio.
20. Asegurarse de que existan pistas de auditoría que puedan usarse en la reconstrucción de los archivos de datos y de las

transacciones de los diversos terminales. Debe existir la capacidad de rastrear los datos entre la terminal y el usuario.

21. Considerar circuitos de conmutación que usen rutas alternativas para diferentes paquetes de información provenientes del mismo mensaje; esto ofrece una forma de seguridad en caso de que alguien intercepte los mensajes.

iii. Controles sobre computadores personales y redes de área local

1. Políticas de adquisición y utilización.
2. Normativas y procedimientos de desarrollo y adquisición de software de aplicaciones.
3. Procedimientos de control del software contratado bajo licencia.
4. Controles de acceso a redes, mediante palabra clave, a través de computadores personales.
5. Revisiones periódicas del uso de los computadores personales.
6. Políticas que contemplen la selección, adquisición e instalación de redes de área local.
7. Procedimientos de seguridad física y lógica.
8. Departamento que realice la gestión y soporte técnico de la red. Controles para evitar modificar la configuración de una red. Recoger información detallada sobre los componentes existentes: Arquitectura (CPUs, Discos, Memoria, Streamers, Terminales, etc.), Conectividad (LAN, minicomputadoras a host, etc.), software (sistema operativo, utilidades, lenguajes, aplicaciones, etc.), Servicios soportados.
9. Inventario actualizado de todas las aplicaciones de la Entidad.
10. Política referente a la organización y utilización de los discos duros de los equipos, así como para la nomenclatura de los archivos que contienen, y verificar que contiene al menos: obligatoriedad de etiquetar el disco duro con el número de serie del equipo, creación de un subdirectorio por usuario en el que se almacenarán todos sus archivos privados, así como creación de un subdirectorio público que contendrá todas las aplicaciones de uso común para los distintos usuarios.
11. Implementar herramientas de gestión de la red con el fin de valorar su rendimiento, planificación y control.
12. Procedimientos de control sobre las transferencias de archivos que se realizan y de controles de acceso para los equipos con posibilidades de comunicación. Políticas que obliguen a la desconexión de los equipos de las líneas de comunicación cuando no están haciendo uso de ellas.

13. Adoptar los procedimientos de control y gestión adecuados para la integridad, privacidad, confidencialidad y seguridad de la información contenida en redes de área local.
14. Cuando exista conexión PC-Host, comprobar que opera bajo los controles necesarios para evitar la carga/extracción de datos de forma no autorizada.
15. Contratos de mantenimiento (tanto preventivo como correctivo o detectivo).
16. Cuando en las acciones de mantenimiento se requiera la acción de terceros o la salida de los equipos de los límites de la oficina, se deberán establecer procedimientos para evitar la divulgación de información confidencial o sensible.
17. Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo.
18. Los computadores deberán estar conectados a equipos de continuidad (UPS's, grupo electrógeno, etc.)
19. Protección contra incendios, inundaciones o electricidad estática.
20. Control de acceso físico a los recursos microinformáticos: Llaves de PC's, Áreas restringidas, Ubicación de impresoras (propias y de red). Prevención de robos de dispositivos, Autorización para desplazamientos de equipos, Acceso físico fuera de horario normal.
21. Control de acceso físico a los datos y aplicaciones: almacenamiento de disquetes con copias de backup u otra información o aplicación, procedimientos de destrucción de datos e informes confidenciales, identificación de disquetes/cintas, inventario completo de disquetes almacenados, almacenamiento de documentación.
22. En las computadoras que se procesen aplicaciones o datos sensibles instalar protectores de oscilación de línea eléctrica y sistemas de alimentación ininterrumpida.
23. Implementar en la red local productos de seguridad así como herramientas y utilidades de seguridad.
24. Adecuada identificación de usuarios en cuanto a las siguientes operaciones: altas, bajas y modificaciones, cambios de password, explotación del log del sistema.
25. Controlar las conexiones remotas entrantes y salientes.
26. Procedimientos para la instalación o modificación de software y establecer que la dirección es consciente del riesgo de virus

informáticos y otros software maliciosos, así como de fraude por modificaciones no autorizadas de software y daños.

27. Controles para evitar la introducción de un sistema operativo a través de dispositivos externos que pudiera vulnerar el sistema de seguridad establecido.