

# Métodos de evaluación de auditorías

Jaime Lorenzo Sánchez

7 de marzo de 2022

# Índice general

<b>1. Introducción</b>	<b>1</b>
1.1. Estándares de auditoría en sistemas . . . . .	1
1.1.1. Norma ISA 401 . . . . .	2
1.1.2. ISO 15504 . . . . .	2
<b>2. Ejemplos de evaluaciones según el tipo de auditoría informática</b>	<b>3</b>
2.1. Evaluación de la Función de Auditoría Interna . . . . .	3
2.1.1. Evaluaciones internas . . . . .	3
2.1.2. Evaluaciones externas . . . . .	4
2.1.3. Organización PwC Venezuela . . . . .	4
2.2. Evaluación de la Efectividad de la Auditoría Externa . . . . .	4
2.2.1. Fundamentos de supervisión del Comité de Auditoría . . . . .	5
2.2.2. Preguntas clave que el Comité de Auditoría debe considerar . . . . .	5
<b>3. Procedimientos de evaluación de la auditoría informática</b>	<b>10</b>
3.1. Estudio, evaluación y organización . . . . .	10
3.2. Estudio y evaluación de sistemas y procedimientos . . . . .	11
3.3. Estudio y evaluación del flujo-grama . . . . .	11
3.4. Estudio y evaluación de los sistemas de control interno . . . . .	12
3.5. Métodos de control administrativos . . . . .	14
3.6. Evaluación de riesgos . . . . .	15
3.7. Sistemas de información y comunicación . . . . .	15
3.8. Procedimiento de control . . . . .	16
3.9. Evaluación de la auditoría . . . . .	16

<b>4. Ejemplos de técnicas de evaluación</b>	<b>18</b>
4.1. Guía de auditoría . . . . .	18
4.2. Ponderación . . . . .	19
4.3. Matriz de evaluación . . . . .	19
4.4. Lista de verificación o chequeo . . . . .	20
4.5. Checklists . . . . .	20
<b>5. Bibliografía</b>	<b>22</b>

# Capítulo 1

## Introducción

Una de las fases principales de las auditorías informáticas es realizar la evaluación de la misma. Esta evaluación se puede realizar mediante numerosas técnicas, no habiendo una única evaluación para todas las auditorías informáticas; sino que cada auditoría informática tendrá una evaluación propia.

Al nivel empresarial, existe una relación entre evaluación y técnicas de auditoría informática. Esto se debe a que, aunque una auditoría informática tiene muchos métodos de evaluación, una auditoría informática puede ser utilizada como medio de evaluación de una empresa y/o compañía. Esto lo veremos más adelante con ejemplos.

A continuación, veremos algunos estándares utilizados para la evaluación de una auditoría informática, o al menos parte de las funcionalidades o propiedades de la misma, así como distintos ejemplos y procedimientos de evaluación de una auditoría informática.

### 1.1. Estándares de auditoría en sistemas

Un hecho importante en la evaluación de una auditoría informática es tener en cuenta la existencia de estándares internacionales.

En la evaluación de la auditoría informática se destacan los siguientes estándares:

### **1.1.1. Norma ISA 401**

La norma ISA 401 es una norma internacional de auditoría sobre Sistemas de Información por Computadora, que dice que en una organización que usa Tecnologías de Información se puede ver afectada en uno de los siguientes componentes del control interno:

- Ambiente de control: Es una pauta de funcionamiento de la entidad y base de los demás componentes.
- Evaluación de riesgos: La entidad se enfrenta a riesgos internos y externos que deben ser evaluados.
- Actividades de control: Son políticas y procedimientos para conseguir seguridad razonable sobre la eficacia del control de riesgos relacionados con la consecución de objetivos de la entidad.
- Información y comunicación: Enmarcan las actividades de control
- Supervisión: Todo proceso de control interno debe ser vigilado de forma continuada.

Además de la forma en que se inicializan, registran, procesan y reporta las transacciones.

### **1.1.2. ISO 15504**

Es un estándar que abarca el sistema de calidad de producto software, que permite la evaluación de procesos software en organizaciones que realicen alguna de las actividades del ciclo de vida del software.

## Capítulo 2

# Ejemplos de evaluaciones según el tipo de auditoría informática

Las auditorías informáticas pueden ser de distintos tipos y, por tanto, cada tipo de auditoría tiene un modo de evaluación distinto. A continuación, se muestran algunos ejemplos:

### 2.1. Evaluación de la Función de Auditoría Interna

En su sección 1300 las Normas para el Ejercicio Profesional de la Auditoría Interna emitidas por el instituto de Auditores Internos (THEIIA), establecen que el director de la auditoría debe desarrollar y mantener un programa de aseguramiento de la calidad y mejora que cubra todos los aspectos de la actividad de auditoría interna y revise continuamente su eficacia.

La actividad de auditoría interna debe adoptar un proceso para supervisar y evaluar la eficacia general del programa de calidad. Dicho proceso debe incluir tanto evaluaciones internas como evaluaciones externas:

#### 2.1.1. Evaluaciones internas

Dichas evaluaciones deben incluir revisiones continuas del desempeño de la actividad de auditoría interna, y revisiones periódicas mediante autoevaluación o mediante otras

personas dentro de la organización; con conocimiento de las prácticas de auditoría interna y de las Normas.

### **2.1.2. Evaluaciones externas**

Deben ser consistentes de al menos cada 5 años por revisores calificados e independientes; proveniente de fuera de la organización.

### **2.1.3. Organización PwC Venezuela**

Existen organizaciones que ayudan a realizar esta evaluación, como por ejemplo PwC Venezuela.

Esta organización realiza evaluaciones del departamento de auditoría interna tal y como lo requieren las Normas Internacionales de Auditoría Interna, comparando la ejecución de su función de auditoría interna contra lo que exigen dichas Normas, identificando las brechas, los incumplimientos y las oportunidades de mejora para la optimización de su departamento de auditoría interna.

## **2.2. Evaluación de la Efectividad de la Auditoría Externa**

La evaluación de la efectividad de la Auditoría Externa es área de atención creciente tanto a los entes reguladores como de los inversores. No sólo es importante para la función del Comité de Auditoría, sino que también puede tener impacto en las recomendaciones respecto de la selección o rotación de los auditores.



### **2.2.1. Fundamentos de supervisión del Comité de Auditoría**

El Comité de Auditoría tiene la responsabilidad de administrar las relaciones con el auditor y asegurarse de que el auditor se responsabilice ante este comité.

Por este motivo, la competencia y las aptitudes del auditor deberían ser analizadas. Algunas consideraciones en este sentido son:

- Entendimiento por parte del auditor de los riesgos que enfrenta la compañía y su respuesta a esto en el plan de auditoría.
- Desempeño y resultados a la luz del plan de auditoría
- Comentarios realizados por el auditor a las preguntas del Comité de Auditoría.

La evaluación debería considerar la independencia, objetividad y escepticismo profesional del auditor. En esta parte, se debería tener en cuenta:

- El nivel de cuestionamiento por parte del auditor y su comunicación al Comité de Auditoría.
- Las medidas de salvaguardas de la independencia implementadas por el auditor.
- La información provista al Comité de Auditoría en esta área.

La evaluación del auditor externo anualmente se considera como una práctica recomendada, porque no sólo ayuda a optimizar el desempeño del auditor, sino que promueve la buena comunicación entre el auditor y el Comité de Auditoría.

### **2.2.2. Preguntas clave que el Comité de Auditoría debe considerar**

El Comité de Auditoría debe considerar 5 preguntas clave:

- Enfoque de la evaluación
- Calidad del servicio
- Juicio y Estimaciones



- Independencia y escepticismo profesional
- Comunicación e Interacción

## Enfoque de la evaluación

- ¿Se han considerado los siguientes mecanismos para evaluar la efectividad de la auditoría?:
  - Revisión de las presentaciones y comunicaciones de auditoría.
  - Revisión de la identificación del riesgo y resultados a la luz del plan de auditoría/ documento de oferta.
  - Evaluación del escepticismo profesional durante toda la auditoría.
  - Revisión de la calidad del personal, recursos, ubicación geográfica, etc.
  - Revisión de los procedimientos internos de control de calidad e informes.
- Los resultados del proceso de evaluación ¿son analizados con el auditor externo? ¿se llega a un acuerdo sobre las áreas que requieren mejora?

## Calidad del servicio

- ¿El socio a cargo del trabajo analizó el plan de auditoría y cómo consideró las áreas de riesgo de auditoría específicas de la compañía/industria (inclusive el riesgo de fraude) con el Comité de Auditoría?
- En relación con las auditorías en múltiples locaciones, ¿el socio a cargo de la auditoría brindó información acerca de las competencias técnicas, experiencia y objetividad profesional de los equipos de auditoría?
- ¿Cumplió el auditor con el plan de auditoría acordado y los criterios de desempeño objetivos? ¿El auditor ajustó el plan para responder a los riesgos y circunstancias cambiantes?
- ¿El socio a cargo del trabajo le informó al Comité de Auditoría los resultados de las consultas a la oficina de práctica profesional de la firma?
- Si la auditoría de la compañía estuvo sujeta a inspección por parte de los organismos reguladores, ¿el auditor le informó al Comité de Auditoría los hallazgos de la inspección y el respectivo impacto sobre los resultados de la auditoría?
- ¿El costo de la auditoría es razonable y suficiente en relación con el tamaño, complejidad y riesgos de la compañía? ¿Se le comunicó al Comité de Auditoría toda modificación del costo (ej. cambios en el alcance del trabajo)?

## Juicios y estimaciones: proceso y supuestos

- ¿Contaba el equipo de auditoría con los conocimientos y competencias necesarios para cumplir los requerimientos de auditoría de la compañía? ¿Cómo respondió el auditor a los comentarios? ¿El Comité de Auditoría y la gerencia de la compañía tenían acceso al socio a cargo del trabajo?
- ¿Cuenta la firma de auditoría con la experiencia requerida en la industria, los conocimientos especializados sobre las políticas contables críticas de la compañía y el alcance geográfico requerido para continuar brindando servicio a la compañía?
- ¿Tiene el equipo de auditoría acceso suficiente al conocimiento especializado durante la auditoría?

## Independencia y escepticismo profesional

- ¿La firma de auditores externos informó al Comité de Auditoría todos los temas que pudieran razonablemente afectar la independencia de la firma? ¿La firma de auditores externos analizó las medidas de salvaguarda implementadas para detectar asuntos de independencia?
- ¿Existieron diferencias significativas de opinión entre la gerencia y el auditor? Si fuera el caso, ¿el auditor presentó un punto de vista claro sobre los temas contables cuando diferían de la perspectiva inicial de la gerencia?
- Si el auditor confía en las pruebas realizadas por la gerencia y la auditoría interna, ¿el Comité de Auditoría concuerda con el grado de confianza depositado?

## Comunicación e interacción

- ¿El socio a cargo del trabajo mantuvo un diálogo profesional y abierto con el presidente del Comité de Auditoría? ¿Los análisis fueron completos y claros?
- ¿El auditor analizó adecuadamente la calidad de la información contable de la compañía, incluso la razonabilidad de las estimaciones y juicios contables? ¿El auditor analizó cómo se compararon las políticas contables con las tendencias y prácticas de la industria?
- En las reuniones ejecutivas, ¿el auditor analizó los asuntos sensibles abiertamente y profesionalmente -inclusive sus opiniones e inquietudes acerca de los procesos de emisión de información, controles internos (ej. políticas de denuncias) y la calidad de la función financiera?
- ¿Se aseguró el auditor de que el Comité de Auditoría estuviera informado de los desarrollos actuales en los principios contables y normas de auditoría así como del posible impacto de ello en la auditoría?

## Capítulo 3

# Procedimientos de evaluación de la auditoría informática

### 3.1. Estudio, evaluación y organización

El auditor deberá contar con elementos de la entidad para estudiar la organización y el equipo de trabajo que la integra.

En primer lugar, deberá tener un organigrama detallado de la misma, el cual deberá estar actualizado.

La elaboración del organigrama deberá contener:

- Deberá establecer a toda la entidad o función sujeta a revisión.
- Deberá incluir los puestos principales de la entidad y toda la estructura si el objetivo es revisar una función.
- Deberá definir perfectamente los tipos de autoridad: lineal, funcional y staff

Esto se refiere a que toda entidad deberá contar con los manuales de sistemas y procedimientos de operación en los cuáles el auditor debe basarse para hacer su evaluación.

## **3.2. Estudio y evaluación de sistemas y procedimientos**

Un procedimiento en auditoría podrá ser llevado de la siguiente manera:

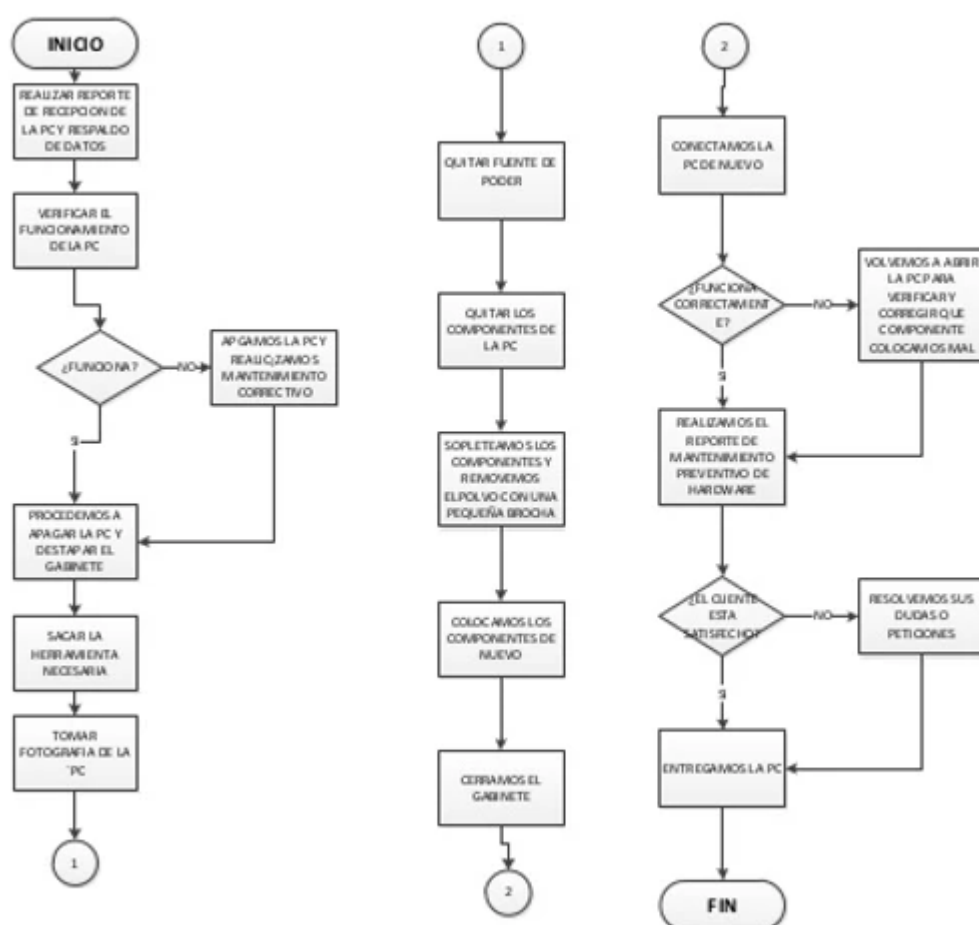
- Nombre
- Sistema al que pertenece.
- Dónde inicia
- Dónde acaba
- Objetivos que persigue
- Políticas administrativas y/o disposiciones que deberán de ser respetadas.

A su vez se deberá de describir en forma secuencial todas aquellas actividades que estén involucradas en el proceso.

## **3.3. Estudio y evaluación del flujo-grama**

Este estudio tendrá por objetivo representar gráficamente los procedimientos de operación de la entidad, viéndose complementados con aquellos comentarios que les sean asignados.

## MANTENIMIENTO PREVENTIVO DE HARDWARE



### 3.4. Estudio y evaluación de los sistemas de control interno

En el desempeño de esta función, aquellas que lo hacen de forma eficiente ejecutan su labor de control solicitando información relevante, pertinente y precisa al equipo directivo, a los auditores interno y externo, además de formulando preguntas directas y complejas.

La Comisión de Auditoría debe supervisar estos controles y revisar la efectividad del sistema en su conjunto. Un sistema de control interno efectivo aporta seguridad razonable acerca de que las políticas, procesos, tareas, comportamientos y demás aspectos de una organización —considerados en su conjunto— propician su funcionamiento efectivo y eficiente, contribuyen a garantizar la calidad de la información presentada a nivel interno y externo, y ayudan a garantizar el cumplimiento de la legislación aplicable.

El rendimiento del sistema de control interno debe evaluarse mediante actividades de monitorización continuas.

Los procedimientos para supervisar la adecuación y efectividad de los controles identificados deben estar integrados en las operaciones habituales de la organización. Aunque los procedimientos de monitorización forman parte del sistema de control general, estos son independientes en gran medida de los elementos que comprueban.

El consejo, con la ayuda de la Comisión de Auditoría, debería recibir y revisar regularmente los informes sobre el control interno y estar informado acerca de cómo se han llevado a cabo las comprobaciones en las que se basan los informes.

Los informes de la dirección deberían ofrecer una valoración equilibrada en relación con la efectividad del sistema de control interno de las áreas cubiertas. Cualquier deficiencia o fallo de control significativo identificado debe abordarse en los informes, incluido el efecto que han tenido, podrían haber tenido o podrían tener en la organización, así como las acciones que se están adoptando para corregirlos. Es fundamental mantener un diálogo directo, continuo y abierto entre la dirección y la Comisión de Auditoría sobre los riesgos y los controles de la organización.

A continuación, se indican algunos indicios de que el control interno no está funcionando según lo previsto y deberían actuar como señales de alerta:



**Los ejecutivos y los equipos de negocio no participan en los procesos de evaluación de riesgos y controles**

- Los debates formales sobre riesgos y controles suelen posponerse
- Los procesos de riesgos y controles no se enmarcan en la actividad habitual

**El desarrollo del sistema de control interno se percibe como el objetivo último**

- Escaso debate o aportaciones adicionales
- La información presentada se centra solo en el riesgo cubierto

**La supervisión y el cuestionamiento no son sólidos**

- Las evaluaciones de riesgo y control, y los informes/procesos apenas cambian
- No se cuestiona a los “business owners” y estos reciben escaso feedback

### 3.5. Métodos de control administrativos

Al realizar una evaluación de la administración de una auditoría informática, se realiza el siguiente estudio:

- Estudio de la no conformidad: Se comprueba si se ha producido el incumplimiento de algún requisito. Por ejemplo: si se encuentra evidencia de diferencias entre el Manual de Calidad, los procedimientos y/o los criterios de auditoría.
- Evaluación de la efectividad del control
- Evaluación del proceso: Se debe evaluar si es capaz y produce los resultados deseados
- Evaluación del ciclo de gestión de mejora continua

## 3.6. Evaluación de riesgos

Se debe realizar una evaluación de las posibles amenazas de la auditoría informática. Dichas amenazas pueden ser:

- Amenazas externas: Incendios, inundaciones, condiciones climatológicas, señales de radar, instalaciones eléctricas, etc
- Amenazas humanas: Robos, fraude, sabotaje, etc.

## 3.7. Sistemas de información y comunicación

Para lograr obtener resultados que beneficien a la organización, los sistemas de información y comunicación deben auditarse para asegurar su sintonía con los objetivos organizacionales. Por tanto, es necesario realizar una correcta evaluación de la estrategia organizacional de la auditoría informática.

Lo primero que hay que tener claro es qué es una estrategia. La estrategia consiste en realizar un profundo análisis tanto de la organización como del entorno.

Para realizar la evaluación de la estrategia organizacional de la auditoría informática se emplea el análisis DOFA O FODA. El análisis FODA consiste en realizar una evaluación de los factores fuertes y débiles que, en su conjunto, diagnostican la situación interna de una organización, así como su evaluación externa (oportunidades y amenazas).

Una vez identificados los aspectos fuertes y débiles de una organización se debe proceder a una evaluación de los mismos. Es importante destacar que algunos factores tienen mayor preponderancia que otros: mientras que los aspectos considerados fuertes de una organización son los activos competitivos, los aspectos considerados débiles de una organización son los pasivos competitivos. Lo trascendente es dar mayor preponderancia a los activos.

Para ello, se utiliza la denominada Matriz FODA:

	<b>FORTALEZAS (F)</b> Lista de Fortalezas	<b>DEBILIDADES (D)</b> Lista de debilidades
<b>OPORTUNIDADES (O)</b> Lista de oportunidades	<b>Estrategias F-O</b> Usar las fortalezas para aprovechar las oportunidades.	<b>Estrategias D-O</b> Superar las debilidades aprovechando las oportunidades.
<b>AMENAZAS (A)</b> Lista de amenazas	<b>Estrategias F-A</b> Usar las fortalezas para evitar las amenazas.	<b>Estrategias D-A</b> Reducir las debilidades y evitar las amenazas

### 3.8. Procedimiento de control

En la evaluación del procedimiento de control, se deben seguir los siguientes pasos:

1. Objetivos de la evaluación: Verificar la existencia de los controles requeridos, asimismo determinar la operatividad y suficiencia de los controles existentes.
2. Plan de pruebas de los controles: Incluye la selección del tipo de prueba a realizar, por lo tanto se debe solicitarse al área respectiva, todos los elementos necesarios de prueba
3. Pruebas de controles: Cada control existente debe ser sometido a prueba
4. Análisis de resultados de las pruebas: Por lo tanto, los resultados obtenidas de las pruebas de control serán analizados para la toma de decisiones.

### 3.9. Evaluación de la auditoría

Para realizar la evaluación de la auditoría, es necesario que además de realizar las evaluaciones indicadas anteriormente, se realiza un informe denominado informe de evaluación.

A continuación, se muestra un ejemplo de un informe de evaluación de una auditoría informática:

INFORME DE AUDITORIA								
Nombre de la Empresa:								
Area auditada:								
Fecha inicial de auditoria:		Fecha final de auditoria:			Auditor:			
Secuencia	Punto en observación	Recomendación	Responsable	Riesgo	Categorización (impacto)			
					Crítico	Mayor	Menor	Sin Impacto

# Capítulo 4

## Ejemplos de técnicas de evaluación

### 4.1. Guía de auditoría

Ch auditoria

informática

empresa=xxx

fecha:

aa:mm:dd hoja :

1 de yy

Ref	Actividad a ser evaluada	Procedimiento de auditoria	Herramienta a utilizar	Observacion
AS01	Evaluar los planes de contingencia del área de sistemas	Solicitar plan de contingencia y evaluar su estructura, asignación de funciones, funciones medidas preventivas y correctivas	Revisión documental	

## 4.2. Ponderación

Factores que serán evaluados	Peso por factor	0 a 100%	Poderados
Objetivos de la oficina de sistemas	10%		
Estructura de la rganizacion	10%		
Procesos y funciones	15%		
Sistemas de información			
Personal y usuarios			

## 4.3. Matriz de evaluación

Descripción de los conceptos evaluados	10Excelente	8Bueno	6Aceptable	4Regular	2Deficiente
Calidad del servicio entregado al usuario solicitante					
Grado de documentación de las aplicaciones					

Lista de verificación o chequeo

## 4.4. Lista de verificación o chequeo

---

Verificar el funcionamiento adecuado de la red, así como la inclusión de sus componentes, su aplicación y uso

---

Descripción	Cumple
La instalación de la red es flexible y adaptable a las necesidades de la empres	
La lista de componentes de la red contienen todo el hardware requerido para su funcionamiento	
Existen niveles de acceso y seguridad en la red	

---

## 4.5. Checklists

### Ejemplo de checklist de seguridad física

- ¿Se encuentra el sistema en una superficie sólida y estable lo más cerca del suelo posible?
- ¿Está el sistema a salvo de la luz solar excesiva, viento, polvo, agua o temperaturas extremas de frío / calor?
- ¿Está el sistema situado en un sitio donde pueda tener un seguimiento, aislado y con poco tráfico humano?
- ¿Está la sala / edificio en el que se encuentra el sistema securizado con una cerradura o sistema de alarma para que sólo personal autorizado acceda? ¿Están las puertas cerradas con llave y las alarmas activadas fuera de horario de oficina?
- ¿Está el terminal del sistema bloqueado para evitar que alguien por casualidad pase por el sistema y lo use (aunque sólo sea por unos segundos)? ¿Están todos los usuarios desconectados del terminal?
- ¿Están los interruptores del terminal bloqueados o protegidos?
- ¿Existen dispositivos de entrada al sistema no asegurados / deshabilitados: unidades de disco bloqueadas / deshabilitadas? ¿Están los puertos paralelo / serie / infrarrojo / USB / SCSI asegurados o deshabilitados? ¿Existen discos duros conectados físicamente al sistema sin bloquear?

### Ejemplo de checklist de seguridad de redes

- Red Física: ¿está la red segura sin peligro de conexión no autorizada? ¿Tiene sólo el personal autorizado acceso a la red física a la que está conectado el sistema? ¿Conoce y confía en todos los diversos puntos donde se gestiona la conexión de red física / administrados por otra persona o entidad?
- ¿Están los otros sistemas de la misma red física y electrónicamente securizados? Si el sistema es razonablemente seguro, pero otro sistema de la red no lo es, la vulnerabilidad de su sistema se aumenta en gran medida.
- Tráfico de red aprobado:
  - ¿Conoce los nombres de los proveedores, la funcionalidad y la naturaleza del software en su sistema que participa en cualquier actividad de la red? ¿Ha comprobado que no existan parches de seguridad del software y recibe regularmente las actualizaciones de seguridad / vulnerabilidades del software que utiliza en la red?
  - ¿Ha probado a fondo cualquier servicio que funcione en la red para asegurarse de que por defecto no proporcionan a algún usuario no autorizado información de seguridad que se podría utilizar para atacar el sistema?

## **Ejemplo de checklist de seguridad de datos**

- Conozca el esquema de propiedad de los archivos que el sistema implementa: ¿está basado en grupos, usuarios, roles o alguna combinación de estos? Conozca los diferentes niveles de protección que se pueden aplicar a los archivos y directorios y sea consciente de quien tiene acceso para realizar cambios en estas protecciones.
- Conozca la estructura general de los sistemas de archivo, cuánto se almacena dónde y quién accede normalmente a qué partes de ellos. Mantenga registros de actividad de disco (por ejemplo, cambios significativos en el espacio de disco utilizado) y de los problemas de disco.
- Asegúrese de que los usuarios sólo pueden tener acceso a las partes del sistema a las que deberían tenerlo; su esquema de protección debe incluir de forma clara y fácil una separación lógica y conceptual de los archivos de usuario y los datos de los archivos del sistema.



# Capítulo 5

## Bibliografía

**Informe Auditoria:** <https://es.slideshare.net/AmdCdmass/informe-final-de-auditoria-infor>

**Ejemplos checklist:** <https://www.impulsotecnologico.com/auditoria-informatica-checklist->

**Evaluacion procedimiento control:** <https://sistemasvirtual.com/proceso-de-la-auditoria-i>

**Análisis DOFA o FODA:** <https://chaui201921701312320.wordpress.com/2019/10/03/analisis-dofa-o-foda/>

**Estrategia organizacional:** <https://www.gestiopolis.com/la-estrategia-organizacional-y-e>

**Sistemas de información y comunicación:** <https://www.gestiopolis.com/auditoria-de-los-si>

**Evaluacion de riesgos:** <https://alylugv.wordpress.com/category/caso-de-una-mala-auditori>  
[evaluacion-de-riesgos/](https://alylugv.wordpress.com/category/caso-de-una-mala-auditori)

**¿Cómo realizar una auditoría?:** <https://www.efectodigital.online/single-post/2018/05/04/-c%C3%B3mo-realizar-una-auditor%C3%ADa-inform%C3%A1tica> -> Enlace obsoleto

**Evaluación de los sistemas de control interno:** <https://www.tendencias.kpmg.es/2019/01/comision-auditoria-evaluacion-sistemas-control-interno/>

**Estandares:** <https://auditingsistem.blogspot.com/2017/06/estandares-y-metodologias.html>

**Ejemplos-tecnicas-evaluacion:** <https://chaui201921701022353.wordpress.com/2020/02/28/ejemplos-de-tecnicas-de-evaluacion/>

**Qué es una auditoría informática:** <https://www.euroinnova.edu.es/blog/que-es-una-auditoria-informatica/>

**Evaluación de una auditoria interna:** <https://www.pwc.com/ve/es/servicios/auditoria/auditoria-interna/evaluacion-del-departamento-de-auditoria-interna.html>

**Evaluación auditoría externa:** <https://home.kpmg/content/dam/kpmg/ar/pdf/ICA/pub-local/evaluacion-efectividad-auditoria-externa.pdf>

**Auditoría Informática: ¿Qué es?, Tipos y más :** <https://mediavuelta digital.com/auditoria-informatica/#auditoria-operacional>

**Componentes del control interno:** <http://www.iimv.org/iimv-wp-1-0/resources/uploads/2014/12/mariajosegomez.pdf>

**Evaluacion Control administrativo:** <https://cursos.aiu.edu/Auditor%C3%ADa%20Administrati PDF/Tema%204.pdf>