

AUDITORÍA Y CONTROL DE SISTEMAS

AUDITORÍAS DE LAS OPERACIONES DE TI, REDES E INFRAESTRUCTURA FÍSICA

AGENDA

- ❑ Conceptos generales
- ❑ Auditoría de las Operaciones Informáticas
- ❑ Auditoría de Redes
- ❑ Auditoría de la Infraestructura Física de Sistemas
- ❑ Referencias



CONCEPTOS GENERALES

Definiciones

- Operaciones de TI
- Todas las actividades (diarias ejecutadas) dentro la infraestructura de TI de una organización [ISACA, 2018b]
- Condiciones:
 - ✓ Volumen de transacciones.
 - ✓ Nivel de uso que se tenga de los recursos de TI.
 - ✓ Niveles de calidad que persiga la empresa.



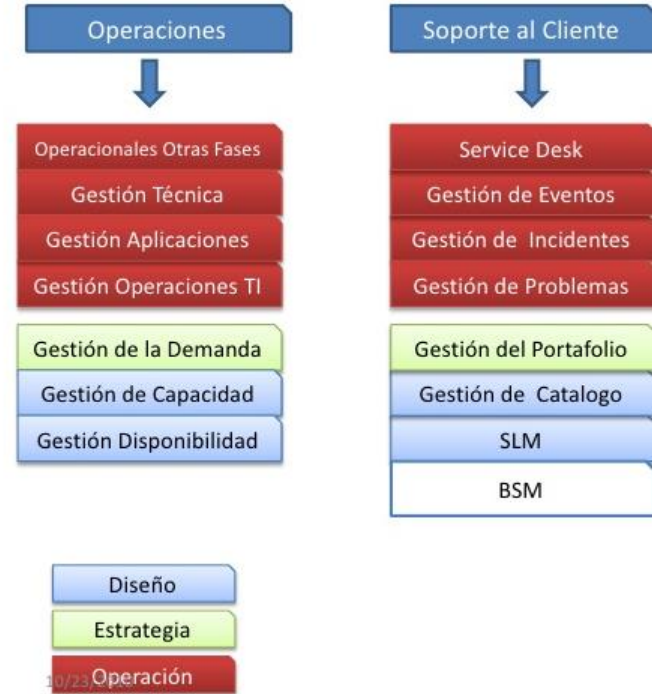
Definiciones

- **Gestión de las operaciones de TI:**[Axelos, 2019]
 - ✓ Consiste en la administración y monitoreo de todas las operaciones de TI de la organización, incluyendo:
 - Asignación de recursos necesarios para realizar dichas operaciones.
 - El establecimiento de estándares y procedimientos para todas las operaciones conforme las estrategias y políticas de negocio.
 - El monitoreo de los procedimientos y los activos de TI para su mejora continua.
 - Resolución de incidentes, problemas y eventos que afecten el desenvolvimiento de sistemas y demás TIC.



Definiciones

- La gestión de las operaciones podría incluir:
 - ✓ Planificación de operaciones automatizadas
 - ✓ Soporte a la infraestructura de TI
 - ✓ Soporte técnico del centro de servicio a usuario
 - ✓ Gestión de problemas e incidentes
 - ✓ Aseguramiento de la calidad de los activos de TI
 - ✓ Monitoreo de la disponibilidad y la capacidad
 - ✓ Control de cambios y gestión de versiones de los activos de TI
 - ✓ Gestión de la seguridad de información
 - ✓ Gestión de la continuidad de negocios



Definiciones

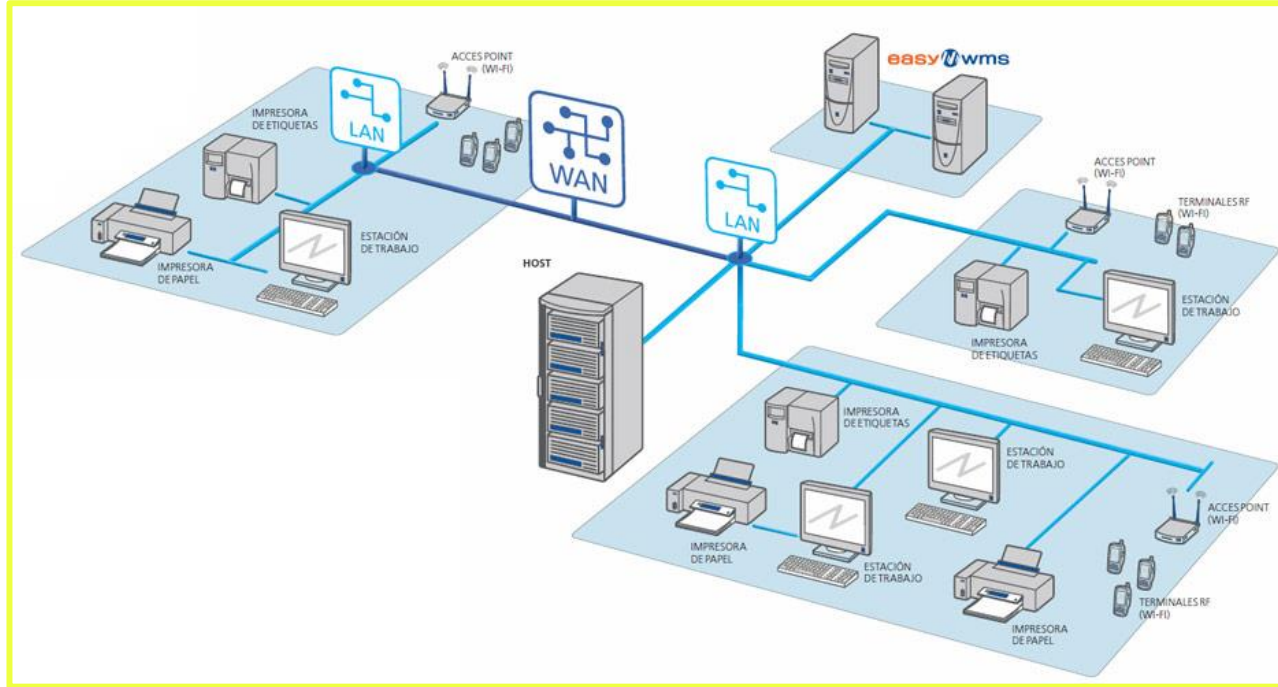
- **Redes de computadoras:**
- Interconexión física y lógica de una serie de recursos compartidos (aplicaciones y hardware) alojados en diferentes computadoras, al interior de una misma organización.
- **Características:**
 - ✓ Interoperabilidad: conexión de sistemas de múltiples naturalezas y de tecnologías distintas.
 - ✓ Disponibilidad: servicio continuo de acceso a los sistemas depositados en la red.
 - ✓ Flexibilidad: facilidad de expansión y de escalabilidad hacia versiones posteriores tanto de los sistemas de aplicación como del software de base (sistema operativo) instalados a lo largo en la infraestructura de la red.
 - ✓ Mantenimiento: facilidad de brindar soporte centralizado a la red.
- **Tipos:** PAN, LAN, MAN, WAN, SAN

Definiciones

- **Infraestructura de hardware**
- Con infraestructura hardware se hace referencia **a todos los equipos físicos** necesarios para soportar las diferentes soluciones tecnológicas de una organización.
- Elementos:
 - ✓ Servidores, los elementos de red, equipos para usuarios finales, entre otros.
 - ✓ **Los servidores** son los ordenadores de gran potencia, capacidad y prestaciones que, gracias a un software, permiten a un gran número de usuarios clientes conectarse concurrentemente y acceder a la información alojada en él.
 - En el servidor se realizan las siguientes funcionalidades: aceptar las peticiones que realizan los clientes, procesar la lógica de la aplicación, realizar formateo de datos para transmitirlos a los clientes, entre otros.

Definiciones

- Infraestructura de hardware



EJECUCIÓN DE AUDITORÍAS DE LAS OPERACIONES DE TI

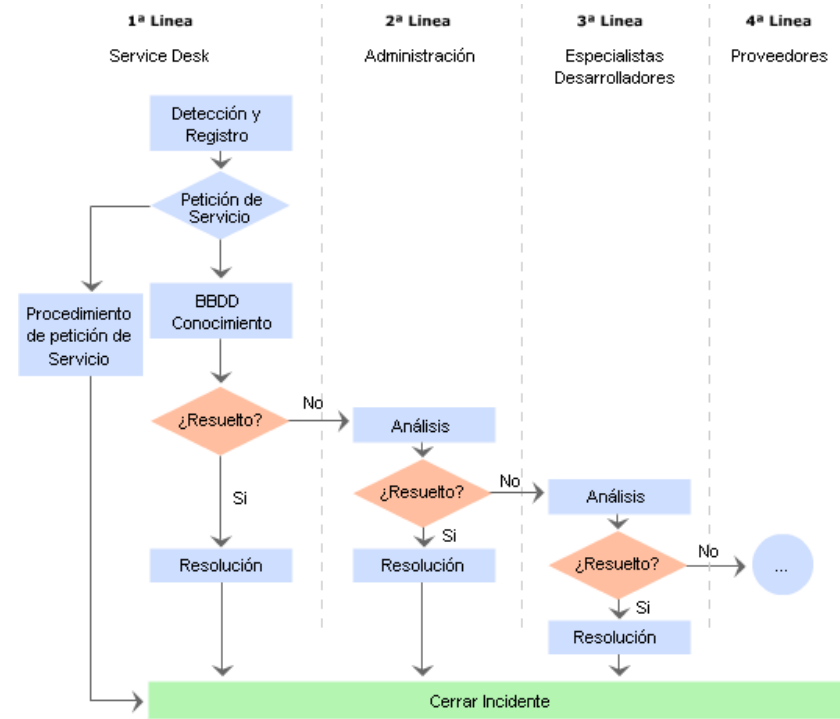
Alcance

- Se necesita definir qué tipos de operaciones van a ser evaluadas:
 - ✓ Operaciones técnicas (backups, restore, parches, actualizaciones de software)
 - ✓ Operaciones de la mesa de ayuda (o la propia idoneidad de la mesa de ayuda)
 - ✓ Gestión de eventos
 - ✓ Gestión de incidentes
 - ✓ Gestión de problemas
 - ✓ Gestión de los servicios de TI



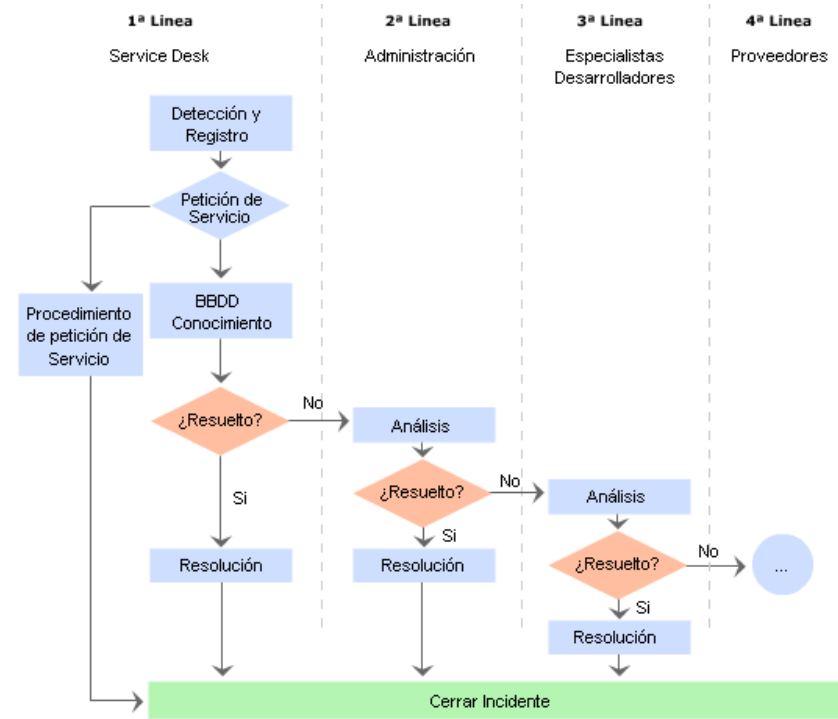
Criterios para auditorías de Operaciones de TI

- Información de los fabricantes de las tecnologías que dan soporte a las operaciones (White papers)
- Procedimientos de Operaciones de TI (Tratamiento de problemas, Gestión de incidentes entre otros)
- Métricas de Operaciones de TI (Rangos de aceptación)



Objetivos específicos para auditorías de Operaciones de TI

- Evaluar **eficiencia y eficacia de una o varias operaciones**
 - ✓ Puede incluir revisar el software y hardware relacionado a la operación
 - ✓ Basado en estadísticas de tiempo, costos
- Revisión de los **procesos de registro de problemas e incidentes**.
- Revisión de los registros de **desempeño para la resolución de problemas y los recursos involucrados**
- Revisión de **Tratamiento de problemas** recurrentes.



Fuentes de evidencia

- El equipo auditor encontrará evidencias revisando:
 - ❖ Procedimientos de operaciones específicas
 - ❖ Registros de incidentes, problemas, eventos
 - ❖ Otra documentación relacionada con la mesa de ayuda.
 - ❖ Auditorías previas.



EJECUCIÓN DE AUDITORÍAS DE REDES

Alcance

Alcance	Criterio
Topología y diseño	Observación, revisión de la documentación
Componentes importantes	Observación, revisión de los manuales respectivos
Usos de la red	Métodos de transmisión, Análisis de tráfico y de aplicaciones
Proceso de administración	Revisión de políticas y procedimientos - documentos, entrevistas con el administrador de red
Funciones y responsabilidades del administrador de red	
Esquema de usuarios	

Criterios para auditorías de Redes de computadoras

Aspecto	Control a evaluar	Criterio
Físicos	Componentes de hardware	Ubicación en instalaciones seguras
	Componentes de software	Aplicaciones y datos son fáciles de acceder, modificar y dañar
	Repositorios de datos	

Fuentes de evidencia

- El equipo auditor encontrará evidencias revisando:
 - ❖ Router, switch, hubs
 - ❖ Cableado estructurado y conexiones
 - ❖ Manuales de operación red
 - ❖ Estructura de usuarios: alta, baja, cambios.
 - ❖ Procedimientos de operaciones específicas
 - ❖ Entrevistas con los proveedores de componentes de redes



EJECUCIÓN DE AUDITORÍAS DE LA INFRAESTRUCTURA FÍSICA

Alcance

- Aspectos a incluir
 - ✓ Planes y procesos de adquisición de hardware.
 - ✓ Gestión de capacidad y desempeño de hardware, los cuales guardan relación con los reportes de incidentes (resueltos o no).
 - ✓ Programa de mantenimiento preventivo.
 - ✓ Gestión de la disponibilidad de hardware
 - ✓ Prestación del servicio de mantenimiento y soporte cuando es brindado por terceros.
 - ✓ Administración de los cambios dentro de la infraestructura de hardware.



Criterios

- ✓ Procedimientos de gestión de capacidad y desempeño de hardware.
- ✓ Programa de mantenimiento preventivo.
- ✓ Gestión de la disponibilidad de hardware e informes (ratios)
- ✓ Aspectos contractuales para la prestación del servicio de mantenimiento y soporte cuando es brindado por terceros.
- ✓ Proceso de administración de los cambios dentro de la infraestructura de hardware.
- ✓ Data Center: Estándar TIA 942



Objetivos específicos para auditorías de infraestructura

- El auditor deberá revisar:
 - ✓ Funcionamiento de cada hardware en particular, interactuando con el proveedor del mismo.
 - ✓ La existencia y aplicación de un programa de mantenimiento de hardware (preventivo y correctivo) tanto de forma directa como a través de un tercero (costos, fechas y SLA).
 - ✓ El local que acoge a la infraestructura y sus condiciones físicas y ambientales.



Fuentes de evidencia

- El equipo auditor encontrará evidencias revisando:
- Físicamente el hardware que está involucrado en el objetivo y el alcance
- La información relacionada con la infraestructura a revisar
- La información de los contratos de los proveedores de infraestructura (incluye mantenimiento)
- Registros de eventos, incidentes y problemas relacionados con la infraestructura de hardware



Referencias bibliográficas

- [Axelos, 2019] ITIL® Foundation, ITIL 4 edition. Axelos Publishing, Inglaterra (2019)
- [ISACA, 2018a] ISACA International. Certified Information Systems Auditor (CISA) Exam Preparation Guide. ISACA Publishing, USA (2018).
- [ISACA, 2018b] ISACA International. COBIT 2019. ISACA Publishing, USA (2018).
- [Ramirez, Alvarez, 2003] G. Ramirez, E. Álvarez. Auditoría a la Gestión de las Tecnologías y Sistemas de Información. Industrial Data, Vol(6)1:99-102.
- [Tupia, 2011] Manuel Tupia. Principios de auditoría de sistemas y tecnologías de información. Tupia Consultores Y Auditores S.A.C., Perú (2011)

¿Consultas?



AUDITORÍAS DE LAS OPERACIONES DE TI, REDES E INFRAESTRUCTURA FÍSICA