AUDITORÍA DE OPERACIONES Y MANTENIMIENTO DE SISTEMAS

La cambiante infraestructura tecnológica y la manera de operarla ha conducido a formas evolutivas de realizar auditorías de Hardware, Sistemas Operativos, Bases de Datos, Redes y Operaciones de Sistemas.

**Revisiones de hardware**: Cuando se realiza una auditoria de infraestructura, las revisiones de hardware deben incluir:

* Plan de adquisición de hardware
  + ¿Está alineado con los requerimientos del negocio?
  + ¿Esta sincronizado con los planes de TI?
  + ¿Cuenta con criterios de adquisición establecidos?
* Adquisición de hardware
  + ¿Está la adquisición en línea con los planes de adquisición documentados?
  + ¿Se han establecido procedimientos y formularios para el proceso?
  + ¿Se ha presentado un análisis de costo beneficios?
  + ¿Las compras, son canalizadas a través del departamento de compras?
* Gestión de capacidad y monitoreo
  + ¿Se realiza una verificación constante del desempeño y la capacidad del hardware?
  + ¿El criterio de monitoreo está basado en estadísticas y reportes de uso del hardware?
* Programa de mantenimiento preventivo
  + ¿Se supervisa la frecuencia del mantenimiento ofrecido en comparación con el indicado por el fabricante?
  + ¿El mantenimiento es realizado fuera de los tiempos pico de carga de trabajo?
  + ¿Se realiza el mantenimiento preventivo en momento cuando el sistema no este ejecutando aplicaciones críticas?
* Disponibilidad de hardware e informes de utilización
  + Es el programa flexible para poder aceptar el mantenimiento preventivo requerido sin percances.
* Registro de problemas
  + Revisa el personal de administración de sistemas los problemas de funcionamiento del hardware.

**Revisiones del sistema operativo:** Cuando se realiza una auditoria del desarrollo, adquisición o mantenimiento del sistema operativo, se debería considerar lo siguiente:

* Procedimientos de selección de software
  + ¿Cumple con los planes de TI a corto y largo plazo?
  + ¿Cumple con los requerimientos de TI?
  + ¿Incluye requerimientos de control?
* Estudio de Factibilidad
  + Existe un análisis de costo beneficio que considere: Costos financieros asociados con el producto, costo de mantenimiento, requerimiento de hardware, requerimiento de capacitación y soporte técnico, impacto sobre la seguridad de los datos y estabilidad del proveedor.
* Seguridad del sistema
  + ¿Se ha establecido procedimientos para restringir la posibilidad de evadir los controles de acceso lógico?
  + ¿Se han establecido procedimientos para administrar los parches de software y mantener actualizado el software?
  + ¿Existe una adecuada seguridad física para restringir el acceso al servidor del sistema?
  + ¿Fueron cambiadas las contraseñas por defecto, suministradas por el proveedor?
* Implementación del sistema, para esto debe existir:
  + Procedimientos de cambios
  + Procedimientos de autorización
  + Funciones de seguridad de acceso
  + Requerimientos de documentación
  + Documentación de pruebas del sistema
  + Pistas de auditoria

**Revisiones de la Base de Datos**: Cuando se realiza una auditoria de las bases de datos, el auditor de sistema debe revisar el diseño, el acceso, la administración, las interfaces, la portabilidad y los controles de sistemas que posee la base de datos, revisando lo siguiente:

* Esquema lógico
  + ¿Existen todas las entidades que contiene el diagrama entidad-relación?
  + ¿Están todas las relaciones representadas como claves externas?
  + ¿Se especifican las limitaciones con claridad?
* Esquema Físico
  + ¿La asignación de espacio de almacenamiento se ha realizado de acuerdo a los requerimientos?
  + ¿Están presentes los índices por claves primarias?
  + ¿Está la base de datos regulada por estándares?
* Controles de seguridad
  + ¿Están todos los derechos de usuarios y grupos justificados de acuerdo a sus funciones?
  + ¿Cuáles son los disparadores que posee configurada la base de datos?
  + ¿Existen normas de integridad de referencia?
  + ¿Las contraseñas expiran?
  + ¿Cuáles son los usuarios con privilegios de Sysadmin? ¿Son apropiados?
  + ¿Están activas las pistas de auditoria?
  + ¿Las pistas de auditorías o logs son revisadas?
  + ¿Fueron cambiadas las contraseñas por defecto?
* Respaldo y recuperación:
  + ¿Existen procedimientos de respaldo y recuperación?
  + ¿Los procedimientos de respaldo son ejecutados tal como fue establecido?
  + ¿Existen controles para garantizar la disponibilidad de la base de datos?

**Revisión de infraestructura de red:** El auditor de sistemas debe revisar los controles sobre la infraestructura de red para asegurar que está protegida y que el desempeño es adecuado.

Para realizar una revisión de manera efectiva, el auditor de sistemas debe identificar lo siguiente:

* La topología y el diseño de la red
* Los componentes de red importantes tales como servidores, enrutadores, switches, módems, dispositivos inalámbricos, etc.
* La utilización de la red
* El personal de administración y operación de la red.
* Los grupos de usuarios de la red
* Los medios de transmisión de red

En adición a esto, se debe revisar lo siguiente:

* Controles ambientales donde están instalados los equipos de redes
  + ¿Existen controles de humedad y temperatura?
  + ¿Posee protección contra electricidad estática?
  + ¿Poseen protectores de pico de corriente?
  + ¿Se ha instalado un sistema de supresión de incendio?
  + ¿Está la red equipada con equipos de energía ininterrumpida, UPS?
  + ¿Se mantiene el lugar libre de polvo, humo y otros materiales como alimentos?
* Controles de seguridad lógica
  + ¿Se les solicita a los usuarios cambiar sus contraseñas periódicamente?
  + ¿Son las contraseñas encriptadas?
  + ¿Las contraseñas están enmascaradas cuando son ingresadas?
  + ¿El acceso de los usuarios a la red es otorgado en base a una autorización por escrito?
  + ¿Los accesos son otorgados basados en funciones?
  + ¿Está prohibido en acceso remoto al administrados del sistema?
  + ¿Son todos los intentos fallidos de inicio de sesión registrados?
  + ¿Se utiliza encriptación para proteger los datos sensibles que se trasmiten a través de la red?
* Solicitudes de cambios
  + Son las solicitudes de cambios realizadas por escrito y autorizadas por el personal competente.
  + Se documentan las solicitudes de modificación y eliminación de acceso a la red
* Monitoreo de seguridad
  + Son revisados los registros de seguridad de los equipos críticos de red como firewalls y servidores.
  + Existen alertas que notifiquen sobre la ocurrencia de algún evento que requiera atención.