UNIVERSIDAD DE COSTA RICA
SEDE GUANACASTE

AUDITORÍA DE SISTEMAS EN PRODUCCIÓN
AUDITORÍA AL PROCESO DE DESARROLLO DE SISTEMAS
CLASES DE ESTUDIOS DE AUDITORÍA

INFORMÁTICA EMPRESARIAL

Auditoría Informática
IF8200

PROFESOR

BAYRON ESPINOZA ORTIZ

GRUPO 1

II SEMESTRE, 2019

CONTENIDO

INTRODUCCIÓN

La auditoría de las tecnologías de información comprende muchos ámbitos dentro de los procesos de la organización. Así como las tecnologías apoyan los objetivos que la alta gerencia dispone, se debe realizar un proceso de verificación desde TI con el fin de evaluar si los procesos de informática están alineados con la organización.

Los sistemas implantados en la organización deben cumplir con el control interno dispuesto. Desde el servicio al cliente, hasta los procesos más complejos como la contabilidad y facturación.

No todas las empresas presentan las mismas características, aún aquellas que producen o venden los mismos servicios o productos. Así que se debe conocer bien los procesos de TI que la conforman.

AUDITORIA DE SISTEMAS EN PRODUCCIÓN

Sistema en producción se refiere a los programas informáticos o aplicativos que utiliza la organización para realizar sus tareas diarias.

Poseer los equipos tecnológicos de la organización es fundamental. La mayor parte de las empresas dependen de ciertos tipos de sistemas o programas para realizar las actividades cotidianas y cumplir con sus objetivos.

¿Para qué sirve?

Se basa en auditar todos los sistemas que la empresa posee. Esto significa realizar un control de todos los componentes de la empresa y ver cuál es la situación actual.

Con este proceso, se busca que los programas y equipos sean actualizados continuamente, además que sean seguros y resguarden la integridad de los datos. Entre sus objetivos:

- Análisis del software y hardware de la empresa.
- Conocer el rendimiento de la inversión tecnológica realizada.
- Realizar un inventario de los activos de software de la empresa.
- Relación entre el software y el hardware de la empresa para comprobar la legalidad de las licencias.

Es por esto que se debe realizar un análisis de todos los equipos de tecnologías de información de la organización, sea físico o virtual, antivirus,

y software utilizado para el buen funcionamiento de la empresa. Incluye el equipo o contratos que se mantengan con las empresas proveedoras del software.

¿Qué evaluar?

Seguridad lógica

La seguridad lógica comprende los controles que se implantan a nivel de software. La seguridad lógica aplica mecanismos y barreras que mantengan a salvo la información de la organización desde su propio medio. Algunos de los controles utilizados en la seguridad lógica son:

- Se limita el acceso a determinadas aplicaciones, programas o archivos mediante claves o a través de la criptografía.
- Se otorgan los privilegios mínimos a los usuarios del sistema informático. Es decir, sólo se conceden los privilegios que el personal necesita para desempeñar su actividad.
- Cerciorarse de los archivos, las aplicaciones y programas que se utilizan en la compañía se adaptan a las necesidades y se usan de manera adecuada por los empleados.
- Controlar que la información que entra o sale de la empresa es íntegra y sólo está disponible para los usuarios autorizados.

ACID (Autenticación, confidencialidad, integridad y disponibilidad)

- **Autenticación:** Garantiza que el usuario "es quien dice ser".
- **Confidencialidad:** la información sólo se revela a los usuarios autorizados para prevenir el acceso no autorizado, ya sea intencional o accidental.
- **Integridad:** La información debe ser siempre exacta y completa, y sólo puede ser modificada por personal autorizado.
- **Disponibilidad:** La información sólo ha de estar disponible cuando se necesite y de la forma que la requieran los usuarios autorizados.

Otros aspectos

Estas características son igualmente importantes.

- **No repudio:** Es una manera de asegurar que ninguna de las partes involucradas pueda negar su participación. Importante en comercio electrónico y banca.
- **Trazabilidad:** permite asociar acciones realizadas en un sistema cono el individuo o sistema que las llevó a cabo y en qué momento.

Amenazas lógicas

Para evitar posibles amenazas lógicas en nuestra organización, es importante que todos los empleados, especialmente los administradores de los equipos, tomen conciencia del cuidado que deben poner para que no se

materialicen posibles daños en la compañía. Además, es fundamental implementar mecanismos de prevención, detección y recuperación ante posibles amenazas lógicas como virus, gusanos, bombas lógicas y otros códigos maliciosos.

La Norma ISO/IEC 27002 recomienda protegerse de las amenazas lógicas, la empresa debe contar con dos o más programas (diferentes vendedores) encargados de detectar y reparar códigos maliciosos para mejorar las probabilidades de éxito ante ataque.

Controles de entrada de datos

En términos generales, cualquiera que sea el ambiente en que se procesan los datos, se hace necesario efectuar el control de ingreso para asegurar que cada transacción a ser procesada cumpla con los siguientes requisitos:

- Se debe recibir y registrar con exactitud e íntegramente.
- Se deben procesar solamente datos válidos y autorizados.
- Se deben ingresar los datos una vez por cada transacción.

Los controles en el ingreso de datos son ***preventivos***, pues tratan de evitar la producción de errores exigiendo el ajuste de los datos introducidos a patrones de formato y estructura (fecha valida, dato numérico, dato dentro de un rango especifico, introducción de dígitos de chequeo, etc.).

-

Buenas prácticas en el control de datos de entrada.

- Las pantallas de captura de datos deben ser diseñadas de manera similar consistente con los documentos fuente que son ingresados al sistema. El orden de los campos, en la pantalla y el documento, deben ser iguales para evitar errores de digitación.
- En el ingreso de los datos, la aplicación debe tener adecuados mensajes de ayuda, con el fin de facilitar los ingresos de estos y advertir sobre algún error cometido, indicando la clase de error.
- Restringir el acceso de los usuarios a las diferentes opciones de la aplicación, de tal forma que se definan los diferentes perfiles de acceso, de acuerdo con las funciones de cada cargo, logrando con esto, disminuir el riesgo de que personas no autorizadas puedan leer, modificar, adicionar, eliminar datos o transacciones.
- Verificar en cada pantalla de captura que los campos de los datos importantes sean de obligatoria digitación.
- En toda la aplicación, cada campo debe tener el formato de datos apropiado: numérico, alfabético o alfanumérico y la cantidad adecuada de caracteres.
- Para los campos numéricos y campos fecha, implantar controles de limite o racionabilidad, para asegurar que los datos estén dentro de un límite. Por ejemplo: la fecha de vencimiento de un crédito debe ser posterior a la fecha de apertura del mismo.

- En la captura o modificación de datos críticos debe dejarse una pista de auditoria (log) donde se identifique lo siguiente: nombre del usuario, fecha y hora, valor del campo y donde se realizó la transacción.
- Verificar que los log's de la aplicación sean revisados por los responsables para investigar accesos y manipulaciones no autorizadas.
- Al ir ingresando los datos, el sistema debe ir comparando con los registros de los archivos maestros para determinar la validez de los datos ingresados, en caso de presentarse una inconsistencia, el sistema debe avisar al usuario inmediatamente a fin de que la misma sea corregida.
- De acuerdo con cada aplicación, en las pantallas de captura de documentos fuente críticos y que tengan al menos una columna numérica, se debe incluir el ingreso de totales de control, con el fin de verificar la correcta digitación de cantidades. Los totales de control también se puede aplicar en el ingreso de los lotes de documentos, ingresando para cada lote, él número de documentos a ser procesados, con el fin de detectar documentos faltantes por ingresar o documentos ingresados más de una vez.
- La aplicación debe permitir imprimir listados de datos ingresados para que estos sean revisados por los usuarios, con el propósito de verificar la correcta inclusión de los datos.

- La aplicación no debe permitir que los datos de los archivos maestros después de haber tenido movimiento pueden ser borrados del sistema.
- Los números de documentos fuente o él número del lote, no deben permitir ser ingresados para el procesamiento más de una vez.
- Es importante tener en cuenta que los anteriores controles se aplican no solo cuando los datos se ingresan por primera vez, sino también, cuando ya estos existen en el sistema y lo que se quiere es modificarlos.
- En el ingreso de los datos, se puede presentar que estos sean rechazados por el sistema; lo que la aplicación debe facilitar es el control sobre dicha transacción rechazada, manteniendo en un archivo, las transacciones rechazadas para que estas sean analizadas y corregidas por los usuarios.

Procesamiento

Los controles de procesamiento garantizan que los datos se están transformando en información, en forma exacta y confiable.

Los programas de aplicación deben prever la posibilidad de detectar errores de procesamiento y, en ese caso, deben indicar el error a través de mensajes dirigidos en primera instancia al operador. Estos mensajes, o bien las instrucciones al operador contenidas en el manual de operaciones o en las ayudas (helps) visibles en pantalla, deben especificar un procedimiento de

corrección. Según el tipo de error, el procesamiento deberá ser interrumpido o por el contario continuar.

Algunos tipos de control que comprueban el procesamiento de la computadora:

- **Importe de totales predeterminados:** En el procesamiento se incluye una corrida, un importe total que deberá ser conciliado al final del procesamiento de todas las partidas procesadas. La conciliación se puede efectuar automáticamente por el mismo programa; esto aseguraría que el procesamiento ha sido correcto y completo, al menos en cuanto a la cantidad de ítems procesados.
- **Controles de razonabilidad y de límites de importes calculados por programa:** Los programas deben comprobar la razonabilidad de un cálculo aritmético efectuado durante el procesamiento, comparando el resultado obtenido en cada operación con límites fijos o flexibles predeterminados. En operaciones de facturación de productos relativamente homogéneos, el programa puede prever un cálculo adicional que permita comprobar si el precio resultante queda dentro de un marco de referencia razonable o estándar. Si el precio llegase a ser erróneo esté se deberá anunciar por medio de un mensaje de error.
- **Prueba de sumas horizontales**: Es un método de control cruzado que consiste en llegar a un importe neto final por dos caminos diferentes.

Si las cifras finales obtenidas a través de estos dos caminos no coinciden, se deberá indicar el error en el procesamiento.

Salidas

Los controles en la salida (consulta por pantalla o reportes) sirven para verificar la exactitud, funcionabilidad, además del adecuado uso y distribución de los reportes.

- → Con unos parámetros específicos, generar reportes por excepción, donde se identifiquen aspectos tales como: cantidades poco frecuentes o transacciones que no cumplen con las políticas definida por la compañía. Estos reportes deben ser analizados por el jefe de cada área usuaria y por auditoria.
- → Generar listado o consulta por pantalla de los datos producidos por el sistema para ser revisados y autorizados por los usuarios.
- → Los reportes que genera la aplicación deben indicar en la última página que ha finalizado. Para reportes confidenciales, se debe indicar la distribución a los usuarios, el tiempo de conservación e indicar que se debe hacer después de su uso (destruirlo o almacenarlo en un lugar bajo llave).
- → Cuando se anulan documentos en la aplicación, esta no debe permitir imprimirlos y para control se debe generar reporte de documentos anulados.

- → En la petición por parte de los usuarios de nuevos reportes, debe existir una petición escrita autorizada por el jefe del área usuaria, con su respectiva justificación.
- → Verificar que los reportes generados por la aplicación, sean lo suficientemente completos para facilitar la toma de decisiones de la compañía.
- → Para los documentos que son titulo valor, verificar que tanto los que se encuentren en blanco como los diligenciados, estén adecuadamente controlados y se les haya asignado una persona responsable de su inventario y custodia.

Continuidad y respaldos de sistemas en producción

Una de las tareas más importantes en la gestión de las TI es la de mantener la continuidad del negocio. Es primordial que una organización muy presente cuales son los riesgos de que los servicios que presta dejen de operar porque los sistemas están fuera de línea. Sea los aplicativos que ha adquirido la organización, sistemas operativos, servidores, bases de datos, etc. Todo ello requiere de total atención por parte de la Alta Gerencia y los Gerentes o Jefes de TI para que el negocio pueda levantar sus sistemas y bases de datos en el menor tiempo posible, pues cada segundo que pasa la empresa pierde.

Los siguientes principios ayudan a tener una mejor perspectiva de lo que el Auditor de TI debe tomar en consideración como buenas prácticas.

Respaldos

- **Realizar copias de seguridad periódicas:** la copia de seguridad puede ser para medios de almacenamiento (discos duros, cintas, etc.) o puede ser una ubicación remota mediante servicios de la nube. Las organizaciones deben realizar copias en diferentes medios, según sea el periodo que hayan establecido (diario, semanal, mensual).

  Las copias de seguridad de la máquina virtual no deben estar expuestas a la internet, y así evitar los ransonware.
- **Prueba de la confiabilidad del proceso de respaldo:** Si se implementa un nuevo medio para respaldar, la administración debe garantizarse que el proceso esté registrando todos los datos del respaldo.

  Se debe implementar una verificación de redundancia cíclica para los metadatos.
- **Uso de almacenamiento seguro:** Las ubicaciones de los respaldos deben ser distintos al de la organización y que sea segura. Si se utilizan los servicios en la nube, la información debe estar encriptada. Y los procedimientos de encriptación, gestión de claves debe estar verificado.

- **Realizar restauraciones de prueba:** se debe proporcionar una prueba para restaurar la copia de seguridad, al menos una vez al año. Dicha prueba debe documentarse, aún si fuere capturas de pantalla que muestren los datos restaurados. Esto garantiza que el respaldo funciona como debe ser.

Recuperación

- **Identificar y clasificar aplicaciones críticas:** Los principios de desarrollo de un plan de continuidad del negocio/plan de recuperación de desastres (BCP/DRP)9 incluyen un paso para identificar las aplicaciones críticas y clasificarlas en importancia de las operaciones. Esta lista se vuelve estratégicamente valiosa si alguna vez se necesita para proporcionar al equipo de recuperación un modelo de cómo restaurar el software de aplicación.
- **Crear un equipo de recuperación con roles y responsabilidades:** El equipo debe incluir todas los roles y funciones necesarias para restaurar de manera rápida y completa las operaciones de la computadora. Debe haber un documento que identifique a los miembros del equipo, sus respectivos roles y los pasos que cada uno tomaría para restaurar las operaciones.
- **Proporcionar una copia de seguridad para todos los componentes esenciales de las operaciones computacionales:** El corazón de un

BCP/DRP es proporcionar un medio de respaldo para proporcionar los componentes esenciales de las operaciones computacionales. El sitio debe incluir un edificio, electricidad, muebles y otras necesidades básicas para albergar las operaciones computacionales. Por lo general, el sitio sigue el mismo principio que el almacenamiento de datos de respaldo, ya que se encuentra a una distancia segura de las instalaciones de la entidad, pero no demasiado lejos para llegar de manera oportuna si es necesario para recuperar las operaciones

- **Proporcionar pruebas regulares y efectivas del plan:** Los principios de respaldo y recuperación sugieren que el paso más importante es proporcionar una prueba completa del BCP/DRP en un intervalo regular para garantizar que realmente funcione y para mejorar el plan a fin de que sea más eficiente y efectivo.

AUDITORÍA AL PROCESO DE DESARROLLO DE SISTEMAS

La auditoría al proceso de desarrollo de software busca identificar las debilidades en las prácticas de software realizadas durante el ciclo de vida del mismo con el fin de mejorar la capacidad de los procesos desarrollados en esta dependencia y mantener o darle continuidad a aquellas prácticas que han sido exitosas.

Importancia

- Los avances en tecnologías de los computadores han hecho que actualmente el desafío más importante y el principal factor de éxito de la informática sea la mejora de la calidad del software.
- El gasto destinado a software es cada vez superior al que se dedica a hardware.
- El software como producto es muy difícil de validar. Un mayor control en el proceso de desarrollo incrementa la calidad del mismo y disminuye los costos de mantenimiento.
- El índice de fracasos en proyectos de desarrollo es demasiado alto, lo cual denota la inexistencia o mal funcionamiento de los controles en este proceso.
- Las aplicaciones informáticas, que son el producto principal obtenido al final del desarrollo, pasan a ser la herramienta de trabajo principal de las áreas informatizadas, convirtiéndose en un factor esencial para la gestión y la toma de decisiones.

PLANTEAMIENTO Y METODOLOGIA

Las funciones que tradicionalmente se asignan al área de desarrollo son:

- Planificación del área y participación, en la medida que corresponda, en la elaboración del plan estratégico de informática.
- Desarrollo de nuevos sistemas.

- Estudio de nuevos lenguajes, técnicas, metodologías, estándares, herramientas, etc. Relacionados con el desarrollo y adopción de los mismos cuando se considere oportuno para mantener un nivel de vigencia adecuado a la tecnología del momento.
- Establecimiento de un plan de formación para el personal adscrito al área.
- Establecimiento de normas y controles para todas las actividades que se realizan en el área y comprobación de su observancia.

Esta auditoría se desglosa en dos grandes apartados

- Auditoría de la organización y gestión del área de desarrollo.
- Auditoría de proyectos de desarrollo de sistemas de información.

Para cada objetivo de control se especifican una o más técnicas de control también denominadas simplemente controles, que contribuyan a lograr el cumplimiento de dicho objetivo. Además, se aportan una seria de pruebas de cumplimiento que permitan la comprobación de la existencia y correcta aplicación de dichos controles.

Los objetivos de control se agrupan en varias series:

- -Organización y gestión del área de desarrollo
- -Proyectos de desarrollo de sistemas de información

    - Aprobación, Planificación Y Gestión Del Proyecto.
- Análisis
    - Análisis de requisitos
    - Especificación funcional
- -Diseño
    - Diseño técnico
- -Construcción
    - Desarrollo de componentes
    - Desarrollo de procedimientos de usuario
- -Implantación
    - Pruebas, implantación y aceptación

CLASES DE ESTUDIO QUE REALIZA EL AUDITOR DE TI

Dependiendo de lo que se busque examinar y la forma en que se realiza podemos encontrar diferentes tipos de auditoría entre los que podemos encontrar:

- **Auditoría externa o legal**: es la más conocida popularmente y consiste en el análisis de las cuentas del balance anual de una empresa a través de un profesional auditor externo por requerimiento legal. Tiene efecto de inscripción en el Registro Mercantil.
- **Auditoría interna:** se lleva a cabo por los propios empleados del negocio, para investigar la validez de los métodos de operaciones y su

coherencia con respecto a la política general de la empresa. Para ello se evalúan ciertos detalles que intervienen en los procesos y mecanismos internos. Es una herramienta clave para el control interno y una vez finalizado el análisis emitirá un informe a la dirección o a órganos superiores del equipo, para evaluar posibles soluciones en referencia a los problemas encontrados.

- **Auditoría operacional:** este tipo de auditoría se desempeña por un profesional cualificado para ello y tiene como objetivo valorar la empresa y su gestión para aumentar la eficacia y la eficiencia, hacia una mejora importante en la productividad. No tiene porqué desarrollarse por alguien interno de la empresa, sino que la propia Dirección podrá contratar a un profesional especializado en ello. El auditor analizará el sistema y propondrá ideas con mejoras útiles.
- **Auditoría de sistemas o especiales**: en este grupo encontramos otro tipo de auditorías dirigidas a evaluar otro tipo de factores no económicos, como es el caso de la auditoría de software, entre otros muchos.
- **Auditoría pública gubernamental:** se desarrolla por el Tribunal de Cuentas gracias a las competencias adquiridas por la Ley Orgánica de 1984.
- **Auditoría integral:** esta auditoría evalúa por completo toda la información financiera, estructura de la organización, los sistemas de

control interno, cumplimiento de leyes y objetivos empresariales para dar una visión global y certera del cumplimiento de la empresa.

- **Auditoría forense:** se realizan en las investigaciones criminales con el objetivo de esclarecer los hechos ocurridos.
- **Auditoría fiscal:** esta auditoría se realiza con el objetivo de velar por el cumplimiento de las leyes tributarias, para que las empresas y organizaciones paguen sus impuestos de forma correcta.
- **Auditoría financiera:** también denominada auditoría contable. Se encarga de examinar y revisar los estados financieros y la preparación de informes de acuerdo a normas contables establecidas.
- **Auditoría de recursos humanos:** se utiliza para hacer una revisión de la plantilla, las necesidades que posee la empresa y la gestión del talento.
- **Auditoría ambiental:** se analizan todas las actividades de la empresa para controlar e intentar reducir al máximo el impacto que poseen el medioambiente.

REFERENCIAS

Argudo, C. (20 de Abril de 2017). *Tipos de auditoría.* Obtenido de Emprende Pyme: https://www.emprendepyme.net/tipos-de-auditoria.html

Auditoria de aplicativos en funcionamiento. (s.f.). *Controles en la entrada de datos*. Obtenido de Auditoria de aplicativos en funcionamiento: https://audcontrolgrp4.weebly.com/controles-en-la-entrada-de-datos.html

Caurin, J. M. (29 de Diciembre de 2016). *Auditoría de los sistemas de información organizacional*. Obtenido de Gestiopolis: https://www.emprendepyme.net/que-es-una-auditoria-de-software.html

Cooke, I. (2018). *Auditoría básica de SI: Respaldo y recuperación.* Obtenido de ISACA: https://www.isaca.org/Journal/archives/2018/Volume-1/Pages/backup-and-recovery-spanish.aspx