Estudiante: Valeria Logroño

Nivel: Octavo "A" TI

Fecha: 14/05/2022

Auditoría Ofimática

Sistema Informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento de la oficina.

Las aplicaciones ofimáticas a más de realizar las tareas para las que fueron creadas, deben hacerlo de manera eficaz y eficiente. Por lo tanto, en el entorno ofimático se espera que estas aplicaciones faciliten el trabajo de cada empleado, permitiendo el intercambio de información entre los diversos procesos de la organización.

Controles de auditoría

Economía, eficacia y eficiencia

Determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones

El equipo auditor debe comprobar los procesos de adquisición y el cumplimiento de los productos solicitados se ajusten a las actividades que se pretendan desarrollar.

Determinar y evaluar la política de mantenimiento definida en la organización

El equipo auditor verifica la garantía de los productos para determinar que no existan pagos innecesarios, también que los usuarios conozcan estas garantías. Además, la existencia de un historial de incidencias y los recursos para solucionarlas.

Evaluar la calidad de las aplicaciones de entorno ofimático desarrollada por personal de la propia organización

El equipo auditor debe determinar la existencia de un departamento responsable de controlar el desarrollo de toda la organización y también debe determinar si la metodología de desarrollo y de pruebas se ajustan a las disposiciones de toda la organización

Evaluar la corrección del procedimiento existente para la realización de los cambios de versiones y aplicaciones.

El equipo auditor se ocupará de determinar el análisis de problemas de integración y compatibilidad de los nuevos productos previamente a su implantación; y de la planificación de formación de los usuarios finales que utilizarán estos productos; y si los encargados de mantenimiento tienen los conocimientos suficientes para que los cambios no repercutan en el funcionamiento de la organización.

Determinar si los usuarios cuentan con suficiente formación y documentación de apoyo necesaria para desarrollar sus tareas de un modo eficaz y eficiente

Equipo de auditoria se encarga de verificar la existencia del plan de formación y comprobar que se compruebe los conocimientos adquiridos una vez realizada la formación.

Determinar si el sistema existente se ajusta a las necesidades reales de la organización.

El equipo auditor valorará el uso que se le a los equipos existentes, elaborando una relación con los equipos que no se encuentren operativos, con los que se usan con frecuencia y los que se utilizan escasas ocasiones.

Seguridad

Determinar si existen garantías suficientes para proteger los accesos a la información de la empresa

El equipo auditor examinara la documentación en materia de seguridad existente en la organización y comprobara que se hayan definidos, al menos, procedimientos de clasificación de información, control de acceso, identificaciones y autentificación.

Determinar si el procedimiento de generación de respaldo es fiable y garantiza la recuperación de información

El equipo auditor examinara el procedimiento de copias de seguridad, verificando la suficiencia de las prioridades, la correcta y el adecuado almacenamiento de soportes, analizara cada procedimiento de notificación y gestión de incidencias registradas.

Determinar si el procedimiento de generación de las copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad.

El equipo auditor debe verificar el procedimiento de copias de seguridad seguido en la organización, verificando la suficiencia de la prioridad, la correcta asignación de responsabilidades y al adecuado almacenamiento de soporte.

Determinar el grado de exposición ante la pasibilidad de interrupciones de virus

El Equipo auditor debe analizar la seguridad en cada uno de los puntos del sistema en los cuales se puedan introducir virus, dispositivos, modem, acceso a red y siempre procurar revisar la normativa que se debe llevar a cabo para la instalación o actualización de productos de antivirus o seguridad, siempre se debe analizar la configuración de los equipos y la instalación de programas que permitan detectar la existencia de virus

Normativa vigente

Determinar sí en el entorno ofimático se producen situaciones que puedan suponer infracciones a lo dispuesto en la Ley Orgánica 51/1999. de protección de datos de carácter personal (LOPD).

El equipo auditor debe comprobar la existencia de un inventario de archivos que maneje datos de carácter personal y constatar que este inventariado contiene todos los archivos gestionados en los entornos informáticos.

Determinar sí en el entorno ofimático se producen situaciones que puedan suponer infracciones a lo dispuesto en la Ley Orgánica 51/1999. de protección de datos de carácter personal (LOPD).

El equipo auditor siempre elaborar una relación exhaustiva de las aplicaciones residentes en equipos ofimáticos que contengan información verificando así las copias ilegalmente utilizadas.

Auditoría Física

La Auditoría Física no se limitar a comprobar la existencia de los medios físicos, sino también su funcionalidad. racionalidad y seguridad

Seguridad Física

Garantiza la integridad de los activos humanos, lógicos y materiales de un CPD. La contingencia o proximidad de un daño se entiende como Riesgo de Fallo.

Antes

Obtener y mantener un Nivel adecuado de Seguridad Física sobre los activos, es decir tener un conjunto de acciones para evitar el fallo o aminorar las consecuencias que de él se puedan derivar.

- Ubicación del edificio.
- Ubicación del CPD dentro del edificio.
- Compartirmentación
- Elementos de construcción.
- Potencia eléctrica.
- Sistemas contra incendios
- Control de accesos.
- Selección de personal.
- Seguridad de los medios.
- Medidas de protección.
- Duplicación de medios.

Durante

Ejecución del Plan de Contingencia, desastre es cualquier evento que. cuando ocurre, tiene la capacidad de interrumpir el proceso de una empresa. El Plan de Contingencia inexcusablemente debe tener:

- Análisis de Riesgos de Sistemas Críticos
- Período Crítico de Recuperación
- Análisis de Aplicaciones Críticas
- Prioridades de Proceso
- Objetivos de Recuperación
- Centro Alternativo de Procedo de Datos
- Asegurar la Capacidad de las Comunicaciones
- Asegurar la Capacidad de los Servicios de Back up

Después

Los Contratos de Seguros vienen a compensar, en mayor o menor pérdidas, gasto« o responsabilidades que se pueden derivar para el CPD.

De entre la gama de seguros existentes, se pueden señalar:

- Centros de proceso y equipamiento
- Reconstrucción de medios software:
- Gastos extra
- Interrupción del negocio
- Documentos y registros valiosos
- Errores y omisiones Cobertura de fidelidad
- Transporte de medios
- Contratos con proveedores y de mantenimiento

Áreas de la Seguridad Física

Organigrama de la empresa

Se conocerá las dependencias orgánicas, funcionales y jerárquicas de los departamentos y de los distintos cargos y empleos del personal pudiendo analizar, con ayuda de documentación histórica.las apropiadas Separación de Funciones y Rotación en el Trabajo.

Auditoría Interna

Departamento independiente o subordinado, el cual debe guardar las auditorías pasad», las Normas, Procedimientos y Planes que sobre la Seguridad Física

Administración de la seguridad

Ampara las funciones, dependencias, cargos y responsabilidades de los distintos componentes:

- Director o Responsable de la Seguridad Integral.
- Responsable de la Seguridad Informática.
- Administradores de Redes.
- Administradores de Bases de Datos.
- Responsables de la Seguridad activa y pasiva del Entorno físico

C entro de proceso de datos e instalaciones

Entorno en el que se encuentra incluso el CPD como elemento físico y en que debe realizar su función informática.

Equipos y comunicaciones

Son los elementos principales del CPD: Host. terminales, computadores personales. equipos de almacenamiento masivo de datos, impresoras, medios y sistemas de telecomunicaciones.

Computadores personales

Son elementos muy potentes e indiscretos que pueden acceder a prácticamente cualquier lugar donde se encuentren los Datos por lo que merecen especial atención tanto desde el punto de vista de acceso a los mismos como a la adquisición de copias no autorizadas.

Seguridad física del personal

Accesos y salidas seguras así como medios y rutas de evacuación, extinción de incendios y medios utilizados para ello, sistemas de bloqueo de puertas y ventanas, zonas de descanso y de servicios. Normas y Políticas emitidas y distribuidas por la Dirección referentes al uso de las instalaciones por el personal.

Fuentes

Se señalan a continuación algunas Fuentes que deben estar accesibles en todos los Centro de Proceso de Datos.

- Políticas. Normas y Planes sobre Seguridad emitidos v distribuidos tanto por la Dirección de la empresa como por el Departamento de Seguridad.
- Auditorias anteriores, generales y parciales, referentes a la Seguridad Física.
- Contratos de Seguros, de Proveedores y de Mantenimiento.
- Entrevistas con el personal de segundad. personal informático v de otras actividades, responsables de seguridad personal contratado para la limpieza y mantenimiento de locales, etc.
- Actas e Informes de técnicos y consultores.
- Plan de Contingencia y valoración de las Pruebas.
- Informes sobre accesos y visitas.
- Informes sobre evacuaciones reales.
- Políticas de Personal.
- Inventarios de Soportes (papel y magnéticas)

Técnicas y Herramientas del Auditor

Técnicas

Observación de las instalaciones, sistemas, cumplimiento de Normas y Procedimientos no solo como espectador sino también como actor; comprobando por si mismo el perfecto funcionamiento v utilización. Revisión analítica de:

- Documentación sobre construcción y preinstalaciones.
- Documentación sobre seguridad física.
- Políticas y Normas de Actividad de Sala
- Normas y Procedimientos sobre seguridad física de los dalos.
- Contratos de Seguros y de Mantenimiento.

Entrevistar con directivos y personal, fijo o emporal.

Consultas a técnicos y peritos.

Herramientas

- Cuaderno Je campo / grabadora Je audio
- Máquina fotográfica/cám ara de video Su uso debe ser discreto y siempre con el consentimiento del personal si éste va a quedar identificado en cualquiera de las náguinas.

Responsabilidades de los **Auditores**

El Auditor Informático Interno, no debe desarrollar su actividad como una mera función policial dando la impresión a los usuarios informáticos y al resto de empleados de que se encuentran permanentemente vigilados. Responsabilidades para cada tipo de auditor:

Auditor informático interno

- Revisar los controles relativos a Seguridad Física.
- Revisar el cumplimiento de los Procedimientos.
- Evaluar Riesgos.
- Revisión del cumplimiento de las Políticas y Normas sobre Seguridad Física
- · Efectuar auditorias programadas e imprevistas.
- Emitir informes v efectuar el seguimiento de las recomendaciones.

Auditor informática externo

- Revisar las funciones de los auditores
- Mismas responsabilidades que los auditores internos.
- Revisar los Planes de Seguridad y Contingencia. Efectuar Pruebas.
- Emitir informes v recomendaciones.

Fases

Siguiendo la Metodología EDPAA y sin perjuicio de alguna pequeña diferencia, màs que nada en el orden o el ámbito de las fases, el Ciclo de Vida quedaría:

- Fase 1: Alcance de la Auditoría
- Fase 2: Adquisición de Información General
- Fase 3: Administración y Planificación
- Fue 4: Plan de Auditoria
- Fase S: Resultado de las Pruebas
- Fase 6: Conclusiones y Comentarios
- Fase 7: Borrador del Informe
- Fase 8: Discusión con los Responsables de Área
- Fase 9: Informe Final
- Informe
- Anexo al Informe
- Carpeta de Evidencias
- Fase 10: Seguimiento de las Modificaciones acordadas.