Auditoria informática

Determina si la TI controla y protege los activos corporativos, al mismo tiempo que garantiza la integridad de los datos y alinea los objetivos generales de una empresa.

Objetivos de la auditoria informática

- El control de la función informática.
- El análisis de la eficiencia de los Sistemas Informáticos.
- La verificación del cumplimiento de la Normativa en este ámbito.
- La revisión de la eficaz gestión de los recursos informáticos.

Sirva para mejorar ciertas características en la empresa como

- Desempeño.
- Fiabilidad.
- Eficacia.
- Rentabilidad.
- Seguridad.
- Privacidad.

La auditoría se especializa en

- **Auditoría:** evaluación basada en criterios con la intención de emitir un informe final que incluya las acciones acordadas para las áreas de no conformidad.
- **Consultoría:** evaluación basada en criterios con la intención de emitir un informe final que incluirá “observaciones y recomendaciones”.
- **Asesoramiento / Asistencia:** participación en diversas actividades utilizando habilidades específicas basadas en riesgos, control orientado a objetivos, habilidades de facilitación, talentos analíticos y de síntesis.

Tecnología informática

Es una herramienta estratégica que brinda rentabilidad y ventajas competitivas a los negocios frente a otros negocios similares en el mercado, pero puede originar costos y desventajas si no es bien administrada por el personal encargado.

Cobit

Es el marco de referencia a través del cual las organizaciones crean políticas y procedimientos que ayudan a lograr los objetivos de la empresa, está conformada por herramientas que los gerentes de la empresa pueden utilizar para asegurarse de que los facilitadores de los procesos de la empresa estén bajo control en la búsqueda de los objetivos corporativos.

ISO 27001

Es el estándar internacional para la seguridad de la información. Establece la especificación para un sistema de gestión de seguridad de la información (SGSI).

Controles internos

El control interno es un mecanismo intrínseco a la empresa y orientado a prevenir, corregir errores o irregularidades.

- El control interno tiene por foco único el departamento de informática.
- En el control interno informático el examen es de modo continuo.
- Quien realiza el control interno informa solo a la dirección del departamento de informática y es personal interno de la empresa

Auditoría interna

- La auditoría estudia un momento concreto de la historia de la actividad de una empresa.
- La auditoría informática abarca todos los componentes de los sistemas de información.
- El auditor reporta a la dirección general de la empresa.
- Realiza una monitorización continua del mantenimiento, supervisión y mejora del sistema de control.

Auditoría externa

- Realizada por un auditor externo.
- Comprobar si las conclusiones de la auditoría interna son correctas.
- El auditor reporta a la dirección general de la empresa.
- Trata de mitigar o eliminar el riesgo existente en la auditoría interna por la independencia de esta.

Auditoria de datos

La auditoría de datos habilita a una organización la identificación de quien crea modifica, elimina y accede los datos, cuando y como son accedidos. O bien, la estructura de los datos.

Mejores practicas de la auditoria de datos

- Responsabilidad segregada
- Mantener el sistema de auditoría de datos independiente
- Hacerla escalable, Ampliable y eficiente, Flexible, completa
- Gestión centralizada
- Asegurar la plataforma de auditoría de datos.
- Identificación de los datos.
- Análisis de datos

Auditoria: explotación

se ocupa de producir resultados informáticos de todo tipo: listados impresos, archivos en todos los medios para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc.

Auditoria: desarrollo

Revisión del proceso completo de desarrollo de proyectos por parte de la empresa auditada. El análisis se basa en cuatro aspectos fundamentales:

1. **revisión de las metodologías utilizadas**: Se analizarán éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
2. **Control interno de las aplicaciones**: Se deberá revisar las mismas fases que presuntamente han debido seguir el área correspondiente al desarrollo.
3. **Satisfacción de usuarios**: Una aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicito.
4. **Control de procesos y ejecuciones de programas críticos**: Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran podría provocar graves y altos costos de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial informativo, etc.

Auditoria: Sistemas

Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas.

- **Sistemas Operativos:** Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera.
- **Software Básico:** Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora.
- **Software de teleproceso (tiempo real):** No se incluye en software básicos por su especialidad o importancia.
- **Tunning:** Es un conjunto de técnicas de observación y medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto.

Administración de base de datos: Asegurarse que Explotación conoce suficientemente, las que son accedidas por los Procedimientos que ella ejecuta. Analizará los Sistemas de salvaguarda existentes, que competen igualmente a Explotación.

Auditoria: Comunicaciones y redes

Revisión de la topología de Red y determinación de posibles mejoras, análisis de caudales y grados de utilización.

Hacking ético

La forma de comprobar las medidas de seguridad es poniéndolas a prueba y para ello surge este servicio. Se trata de un test de intrusión que intenta utilizar las mismas técnicas de hacking y herramientas que los atacantes para de esta manera poner a prueba la seguridad informática.

Herramientas y técnicas para la auditoria informática

- **Cuestionarios:** Conjunto de preguntas a las que el sujeto puede responder oralmente o por escrito, cuyo fin es poner en evidencia determinados aspectos.
- **Entrevistas:** es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.
- **Checklist**

Seguridad física

Es la parte más importante del mantenimiento de la seguridad de un sistema informático, y es a menudo pasada por alto por los administradores de sistemas descuidados que asumen que, con echar de vez en cuando un vistazo rápido a los sistemas, es protección suficiente.

Seguridad de redes

Es la segunda parte más importante del mantenimiento de unos sistemas seguros. Si bien la seguridad física juega un papel importante, si opera en sus sistemas en un entorno de red / multiusuario, el sistema es mucho más susceptible a los ataques externos que un sistema autónomo.

Protocolos/servicios

Aunque en general es seguro asumir que el software que viene preinstalado en un nuevo sistema es razonablemente seguro, siempre se debe consultar con los desarrolladores de software sobre parches de seguridad, notas de versión y otra información relevante para su configuración particular.

Seguridad de usuarios

Desarrolle un método estándar para la creación y mantenimiento de cuentas de usuario. Desarrollar políticas aceptables de uso claras y concisas y comunicarlo así a los usuarios.

Seguridad de datos

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.

Contraseñas

Requerir contraseñas únicas y complejas de todas las cuentas de usuario en el sistema, no es aceptable tener cuentas de “invitados” u otras cuentas que no requieren ningún tipo de autenticación. Las contraseñas deben contener al menos 8 caracteres y una combinación de letras y números, mayúsculas y minúsculas.

Trazas y/o huellas

Las trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las trazas no deben modificar en absoluto el Sistema.

Análisis de riesgos

- **Riesgo:** Es todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas.
- **Seguridad:** Es una forma de protección contra los riesgos
- **La gestión de riesgos** debe garantizarle a la empresa la tranquilidad de tener identificados sus riesgos y los controles que le van a permitir actuar ante una eventual materialización o simplemente evitar que se presenten.
- **la identificación de activos de información**, es decir todos aquellos recursos involucrados en la gestión de la información.

Información personal identificable (PII)

se refiere a cualquier dato que pueda ayudar a identificarte, como tu dirección o nombre. Las organizaciones usan PII para mejorar la experiencia en línea de los usuarios.

Robo de PII

Los atacantes pueden robar PII a las empresas, lo que a menudo se conoce como una violación de datos.

OCTAVE

es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo. El método OCTAVE permite la comprensión del manejo de los recursos, identificación y evaluación de riesgos que afectan la seguridad dentro de una organización.

El método OCTAVE se enfoca en tres fases para examinar los problemas organizaciones y tecnológicos

- Identificación de la información a nivel gerencial
- Identificación de la información a nivel operacional
- Identificación de la información nivel de usuario final

Estos tres métodos dan lugar a otros 5 procesos para completar los 8 de los que consta OCTAVE

- Consolidación de la información y creación de perfiles de amenazas.
- Identificación de componentes claves.
- Evaluación de componentes seleccionados.
- Análisis de riesgos de los recursos críticos.
- Desarrollo de estrategias de protección.

OCTAVE Fase 1

La primera fase engloba los activos, las amenazas, las vulnerabilidades de la empresa u organización, las exigencias de seguridad y las normas existentes.

- **El primero de estos procesos** consiste en la identificación del conocimiento de los altos directivos. En este punto se procederá a la recopilación de información de los niveles de seguridad, de los principales activos y sus posibles motivos de preocupación y de las estrategias de protección con las que cuente la empresa u organización en ese momento.
- **El segundo de los procesos** se basa en la identificación del conocimiento, una vez más, de los directivos, pero en este caso de áreas operativas. Su meta principal a nivel operativo es la recolección de información.
- **El proceso número tres** tiene que ver con la identificación del conocimiento del personal. Llegados a este punto se toma información de miembros de personal sobre requisitos de seguridad, de los principales activos y sus posibles motivos de preocupación y de las estrategias de protección con las que cuente la empresa u organización en ese momento.
- **El cuarto y último proceso de esta fase** consiste en la composición de perfiles de amenaza. En este punto el equipo de análisis se encargará de evaluar la información recopilada en los procesos anteriores. Posteriormente ser pasará a seleccionar 5 activos críticos y sobre los mismos se definen requisitos y amenazas.

OCTAVE Fase 2

Esta segunda fase engloba los componentes claves y las vulnerabilidades técnicas. En ella se continua con los procesos comenzados en la fase anterior, permitiendo un desarrollo correcto del análisis y la gestión de los riesgos en el interior de la empresa u organización.

- **El quinto proceso** comprende la identificación de componentes clave, sistemas importantes para activos críticos.
- **El sexto y último proceso** de esta fase Nene que ver con la evaluación de los componentes que hayan sido seleccionados.

OCTAVE Fase 3

Esta última fase, la tercera, engloba la evaluación de los riesgos y la ponderación de los mismos, la estrategia de protección y el plano de reducción de los riesgos. La fase número 3 de la metodología OCTAVE la componen dos procesos.

- **El proceso número siete** está basado en la realización de un análisis de riesgos. En el mismo se identificarán los riesgos susceptibles de darse sobre los activos críticos de la empresa u organización.
- **El último proceso de todos, el ocho**, constituye el desarrollo de una serie de estrategias de protección. En las mismas se definirán las acciones y planes a llevar a cabo para proteger los activos críticos.

Metodología Megerit

Es una metodología de análisis y gestión de riesgos de los Sistemas de Información, elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas de España.

Ventajas

- Es metódica por lo que se hace fácil su comprensión.
- Comprende los procesos de análisis y gestión de riesgos.
- Usa un modelo de análisis de riesgos cualitativo y cuantitativo.
- Soporta herramientas comerciales EAR y no comerciales PILAR.

Desventajas

- No toma en cuenta un análisis de vulnerabilidades.
- La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión y en la evaluación.
- La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.