



METODOLOGIA DE CONTROL INTERNO, SEGURIDAD Y AUDITORIA INFORMATICA

GRUPO NO. 10



NORMATIVA


- Debe definir de forma clara y precisa todo lo que debe existir y ser cumplido , tanto desde el punto de vista conceptual, como práctico, desde lo general a lo particular.

Debe inspirarse en :

- Políticas
- Marco jurídico
- Políticas y normas de la empresa
- Experiencia
- Prácticas profesionales

ORGANIZACION DEL SISTEMA INFORMATICO

- ✓ La integran las personas con funciones específicas y con actuaciones concretas, procedimientos definidos metodológicamente y aprobados por la dirección de la empresa. Sin el nada es posible.
- ✓ Funciones
- ✓ Procedimientos
- ✓ Planes (seguridad, contingencias, auditorias)

- 
- ✓ Seguridad
 - ✓ Control Interno Operativo
 - ✓ Eficiencia y Eficacia
 - ✓ Tecnología Informática
 - ✓ Continuidad de Operaciones
 - ✓ Gestión de Riesgos

ESTRUCTURAS DE ORGANIZACIÓN DE LAS EMPRESAS Y AREAS DEDICADAS A LA AUDITORIA EXTERNA

- ✓ Grandes Empresas dedicadas a la auditoria
- ✓ Despachos o Empresas Medianas dedicadas a la auditoria
- ✓ Pequeños despachos o Auditores Independientes

ESTRUCTURA DE ORGANIZACIÓN DE LAS ÁREAS DE AUDITORÍA INTERNA

- ✓ MACROEMPRESAS
- ✓ EMPRESAS GRANDES
- ✓ EMPRESAS MEDIANAS
- ✓ EMPRESAS PEQUEÑAS
- ✓ MICROEMPRESAS
- DOS METODOLOGÍAS A EVALUAR:

METODOLOGIA

Auditoría Informática → solo identifica el nivel de “exposición” por falta de controles.

Análisis de Riesgos → facilita la “evaluación” de los riesgos y recomienda acciones


Definiciones para profundizar en estas metodologías

Amenaza → una persona o cosa vista como posible fuente de peligro o catástrofe (inundación, incendio, robo de datos, sabotaje, agujeros publicados, etc.)

Vulnerabilidad → la situación creada, por la falta de uno o varios controles, con los que la amenaza pudiera acaecer y así afectar al entorno informático (falta de control de acceso lógico, de versiones, inexistencia de un control de soporte magnético, etc.).


Riesgo → la probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad (los datos estadísticos de cada evento de una base de datos de incidentes).

Exposición o Impacto → la evaluación del efecto del riesgo. (es frecuente evaluar el impacto en términos económicos, aunque no siempre lo es, como vidas humanas, imágenes de la empresa, honor, etc.).



Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático

Establecer como prioridad la seguridad y protección de la información del sistema computacional y de los recursos informáticos de la empresa.




Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.






Objetivos de Control

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoria Informática interna/externa.

-


- 
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático.
 - Establecer como prioridad la seguridad y protección de la información del sistema computacional y de los recursos informáticos de la empresa.
 - Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.

- 
- Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.
 - Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.
 - Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.


- 
- Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.
- 

Procedimientos de Control

- Procedimiento:
- Manera de hacer, método práctico para hacer algo. Su importancia radica en que se busca contribuir en la eficiencia y eficacia de las actividades de la empresa, por medio de una sucesión lógica, cronológica y congruente de sus actividades de trabajo.
- Control:
- Verificación, comprobación, intervención, fiscalización


- 
- La empresa en el momento de implementar el sistema de control interno, debe para el cumplimiento de los objetivos organizacionales

Manual de procedimientos

- El manual de procedimientos es un componente del sistema de control interno, el cual se crea para obtener una información detallada, ordenada, sistemática e integral que contiene todas las instrucciones, responsabilidades e información sobre políticas, funciones, sistemas y procedimientos de las distintas operaciones o actividades que se realizan en una organización.
- 



Tecnología de la Seguridad

- El cambio constante de nuestro entorno, el rápido desarrollo tecnológico, la necesidad de integrar nuevos sistemas y aplicaciones, provoca, en muchos casos, descuidos importantes en la seguridad de las organizaciones. Los cambios legales que obligan a adoptar medidas de seguridad para la protección de la información, la proliferación del "hacking" o los virus, la creciente extensión de las redes de las empresas, su integración con Internet y su uso masivo, hace necesario una vigilancia permanente del estado de la seguridad de los sistemas.
- 




■ **CATÁLOGO DE SERVICIOS**

- Consultoría Integral de Seguridad.
- Auditoria e implantación del Gobierno TI.
- Auditorias de Sistemas de Gestión de Seguridad en la Información (SGSI).

■ **CONSULTORÍA DE SEGURIDAD**



- Planes de Seguridad Corporativos.
- Políticas de Seguridad.

■ **AUDITORIA DE SEGURIDAD INFORMÁTICA**

- Evaluación de Seguridad de los Sistemas de Información.
 - Análisis integral de vulnerabilidades.
 - Test de Intrusión Externo e Interno.
- 

Herramientas

- **LAS HERRAMIENTAS DE CONTROL**
- Son elementos software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objeto de control
- La normativa
- La organización
- Metodologías
- Objetivos de control
- Procedimientos de control
- Tecnologías de seguridad
- Herramientas

- 
- 
- - Las herramientas de control (software) más comunes son:
 - Seguridad lógica del sistema:
 - Seguridad lógica complementaria al sistema
 - Seguridad lógica para entornos distribuidos.
 - Control de copias
 - Gestión de soportes magnéticos
 - Gestión y control de impresión y envíos de listados por red
 - Control de proyectos