AUDITORIA DE SEGURIDAD DE INFORMACIÓN

ÁNGEL FELIX DÁVALOS SUÑAGUA

davalosangel@hotmail.com

RESUMEN

La información en la actualidad es un elemento crítico para el éxito y la supervivencia de las empresas y organizaciones y es por esa razón que las mismas deciden la administración efectiva de la información y su resguardo considerando además la Tecnología de la Información (TI) relacionada y generada en esta sociedad global donde la información viaja a través del ciberespacio, son la restricción del tiempo, distancia y velocidad, siendo la información y la tecnología la que soporta la sobrevivencia de la empresa de ahí que la información es uno de los activos más importantes y valiosos de la empresa y organizaciones, el soporte, motivo por el cual los responsables de la empresa en su nivel jerárquico más elevado, optan por implantar métodos, modelos y sistemas de seguridad de la información, los mismos deben ser evaluados en su eficiencia y eficacia, es ahí donde la auditoria interviene permitiendo su revisión y análisis por medio de estándares, buenas prácticas, guías, etc. aceptadas y de aplicación internacional que permiten que se evidencie el estado de los Sistemas de Seguridad de la Información.

PALABRAS CLAVE

Seguridad, Información, Auditoria, Gobierno Corporativo, Estándares, Buenas Prácticas, Certificación, Modelos, Métodos y Principios.

ABSTRACT

The information today is a critical to the success and business survival and organizations and it is for this reason that administering them decide effective information and considering further safeguard Information Technology (IT) and related generated in this global society where information travels through cyberspace, they are the restriction of time, distance and speed information and being technology that supports survival of the company there the information is one of the active most important and valuable of the companies and organizations, the media,

why makers the company as a hierarchical level high, choose to implement methods models and security systems information, they should be evaluated on their efficiency and effectiveness, is where the audit involved allowing review and analysis through standards, best practices, and guides. and application accepted that allow international evidence of the state of the systems
Information Security.

KEYWORDS
Security, Information, Audit, Corporate Governance Standards, Best Practices, Certification, Models, Methods and Principles.

1. INTRODUCCION

En la trayectoria del desarrollo profesional como auditor, las auditorias permiten conocer una serie de empresas, y obtener experiencias de distintos tipos en diferentes áreas de conocimiento, entre ellas, Procesamiento Electrónico de Datos - PED, Sistemas de Información - SI, Tecnologías de la Información y Comunicación – TIC´s, etc., que permiten el desarrollo y crecimiento empresarial y de negocios. Es en este sentido la “Seguridad De La Información”, ha cobrado una importancia relevante en gran parte de las mismas, tanto empresas públicas como privadas, ya que la informaciónque genera la empresa, se ha convertido en un bien (Activo Real) en riesgo, que debe ser resguardado y protegido contra posibles daños, perdidas, manipulación, etc., que pueden tener como origen, tanto personal interno, como externo, personas jurídicas y naturales, con los cuales la empresa se desenvuelve de manera cotidiana en sus actividades, procesos, operaciones y transacciones de carácter, jurídico legal, administrativo, contable, financiero u otro.

2. CONTENIDO

A. Modelo de Seguridad Empresarial

Hoy en día las empresas con el propósito de reguardar la información han diseñado y determinado la arquitectura de seguridad empresarial, basada en liderazgo de la seguridad y progresa hacia abajo por medio de capas a diferencia del Modelo de Oficiales de Seguridad de la Información - OSI, que se divide en siete capas encapsuladas e independientes; Mientras que el Modelo de Seguridad Empresarial, las capas del modelo de seguridad son interdependientes, como se muestra en el grafico siguiente:

Nro. Capa		
7	Aplicación	Provee Servicios para las aplicaciones como transferencia de archivos
6	Presentación	Provee la representación de datos entre sistemas
5	Sesión	Establece, Mantiene, Administra las sesiones ejemplo, sincronización del flujo de datos.
4	Transporte	Provee integridad en la transmisión de datos punta a punta.
3	Red	Conecta y en ruta unidades de información
2	Enlace de Datos	Provee transferencia de unidades de información al otro lado del enlace físico.
1	Física	Transmite hileras de bits en el medio físico.

Tabla 1: Modelo ISO/OSI interconexión de capas en sistemas abiertos
Fuente: Normas ISO

Mientras que el Modelo de Seguridad Empresarial, las capas del modelo de seguridad son interdependientes, como se muestra en el grafico

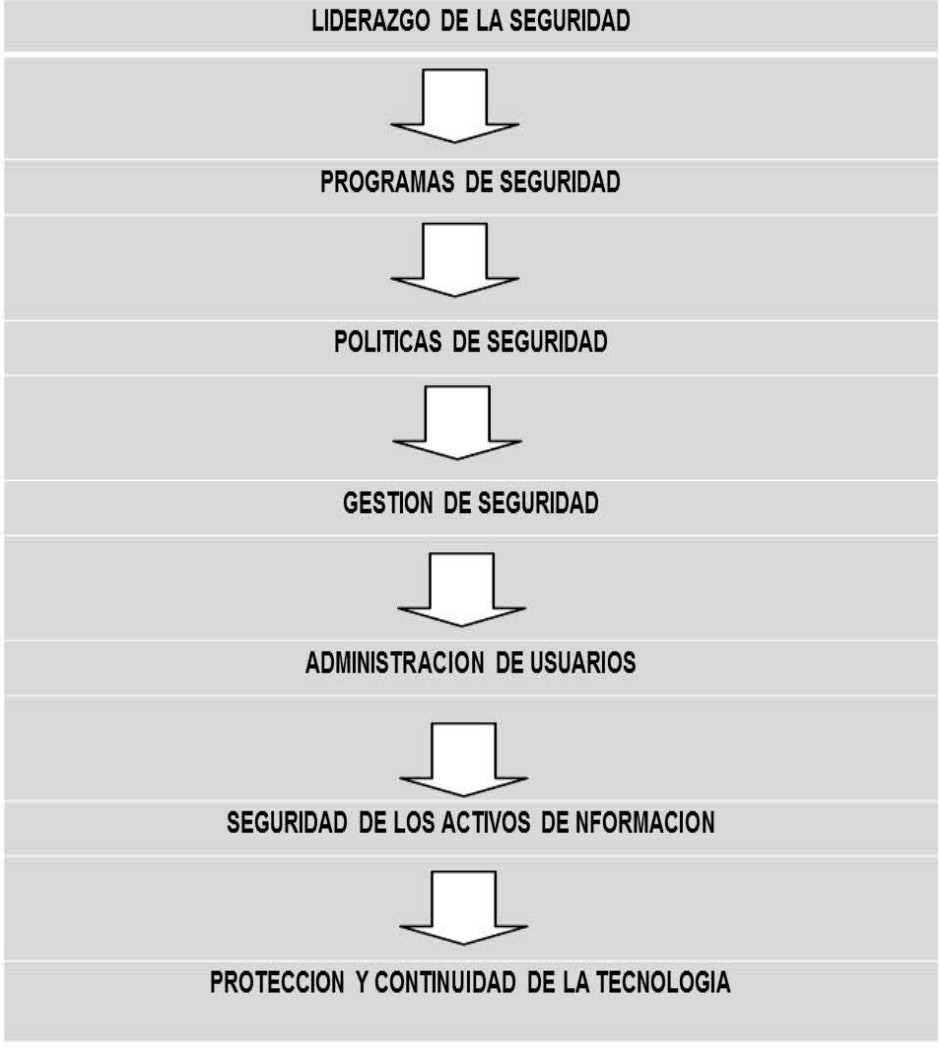


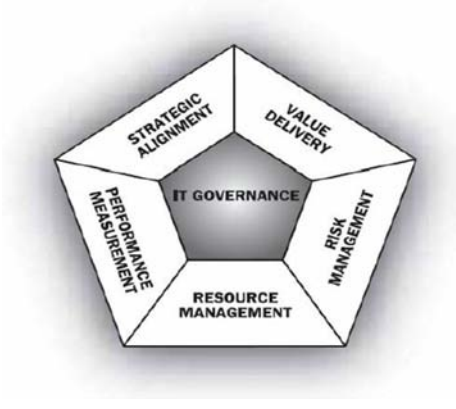
Grafico 1: Modelo de Seguridad Empresarial
Fuente: Revista Kaos Conceptual 2008

Este modelo se debe entender de la siguiente manera para la aplicación en las diferentes empresas:

1) Liderazgo de la Seguridad: Consiste y comprende el financiamiento de la seguridad, la postura a tomar en cuenta y la estrategia de seguridad.
2) Programas de Seguridad: Consiste en la estructura de la seguridad, capacidades y recursos del programa de seguridad.
3) Políticas de Seguridad: Consiste en las Políticas, estándares y directrices de seguridad.
4) Gestión de Seguridad: Consiste en las operaciones de la seguridad y la supervisión de la seguridad.
5) Administración de Usuarios: Consiste en la administración de usuarios y a la concientización de los mismos.
6) Seguridad de los Activos de Información: Consiste en la seguridad de las aplicaciones, seguridad de las bases de datos, seguridad de los host, seguridad de la red interna y seguridaddel perímetro de contingencias.
7) Protección y Continuidad de la Tecnología: Consiste en la previsión tomada por parte del personalresponsable sobre la parte física (mantenimiento preventivo y correctivo) asimismo de la previsión del cambio de tecnología y su costo respecto de la empresa, es decir seguridad física, instalaciones, equipamiento, hardware, soporte de datos, seguridad de robos, incendios, desastres naturales, etc.

B. Gobierno De Tecnología De La Información – TI

El Gobierno de Tecnologías de la Información es también conocido como Gobierno de TI, según el IT Governance Institute: "es responsabilidad del consejo de administración y de la dirección ejecutiva. Es una parte integral del gobierno corporativo y consiste en el liderazgo y estructura de la organización



Grafica 2: gobierno corporativo ti
Fuente: ISACA- modelo COBIT

C. Ciclo De La Seguridad

El de la auditoría de seguridad es revisar la situación y las cuotas de de la misma en los órganos más importantes de la de sistemas. Para ello, se fijan los supuestos de partida:

- El área auditada es la Seguridad.
- El área a auditar se divide en: Segmentos.
- Los segmentos se dividen en: Secciones.
- Las secciones se dividen en: Subsecciones.

Los segmentos a auditar, son:
-Segmento 1: Seguridad de cumplimiento de normas y estándares.
-Segmento 2: Seguridad de .
- Segmento 3: Seguridad de Software.
-Segmento 4: Seguridad de .
-Segmento 5: Seguridad de .
- Segmento 6: Seguridad de Proceso.
-Segmento 7: Seguridad de Aplicaciones.
-Segmento 8: Seguridad Física.

Conceptualmente la auditoria de sistemas en general y la de Seguridad en particular, ha de desarrollarse en seis fases bien diferenciadas:
-Fase 0. Causas de la realización del ciclo de seguridad.
-Fase 1. y del ciclo de seguridad.
-Fase 2. Ponderación de sectores del ciclo de seguridad.
-Fase 3. Operativa del ciclo de seguridad.
-Fase 4. Cálculos y resultados del ciclo de seguridad.
-Fase 5. Confección del informe del ciclo de seguridad.

D. Estándares De Seguridad De La Información

En la actualidad muchas empresas han adoptado regulaciones ya sea de carácter nacional o internacional que tienen impacto en las organizaciones sobre el uso y la seguridad de la información, es por ello que se debe medir el cumplimiento de las leyes, regulaciones, estándares u otra que le permita evaluar su sistema de seguridad de la información, entre los estándares más conocidos tenemos:

ISO 17799 – Códigos De Buenas Prácticas De Seguridad De La Información

Cabe aclarar que la ISO 17799, es el conjunto de controles basados en las mejores prácticas en la seguridad de la información, siendo un estándar internacional que cubre todos los aspectos de la seguridad de la información y propicia las bases para la protección de la información integrando al personal con los procesos y seguridad de sistemas.

I. Comprende los siguientes acápites:
II.Políticas de Seguridad
III. Aspectos Organizativos para la Seguridad
IV. Control y Clasificación de los Recursos de la Información (Activos)
V. Seguridad Ligada al Personal
VI. Seguridad Física y Ambiental o del Entorno
VII. Gestión de Comunicaciones y Operaciones
VIII. Control de Accesos
IX. Desarrollo y Mantenimiento de los Sistemas
X. Manejo de la Continuidad del Negocio
XI. Cumplimiento y Conformidad con la Legislación

Estos diez dominios se derivan 36 objetivos de control (Resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (Prácticas, procedimientos o mecanismos que reducen el nivel de riesgos).

El objetivo de la ISO 17799, es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad. Cabe aclarar que esta norma NO ES CERTIFICABLE, pero recoge la relación de controles a aplicar o al menos a evaluar para establecer un Sistema de Gestión de Seguridad de la Información – SGSI.

Para la evaluación por parte de auditoría en el marco de la ISO 17799, se trabaja con la seguridad en 4 niveles:

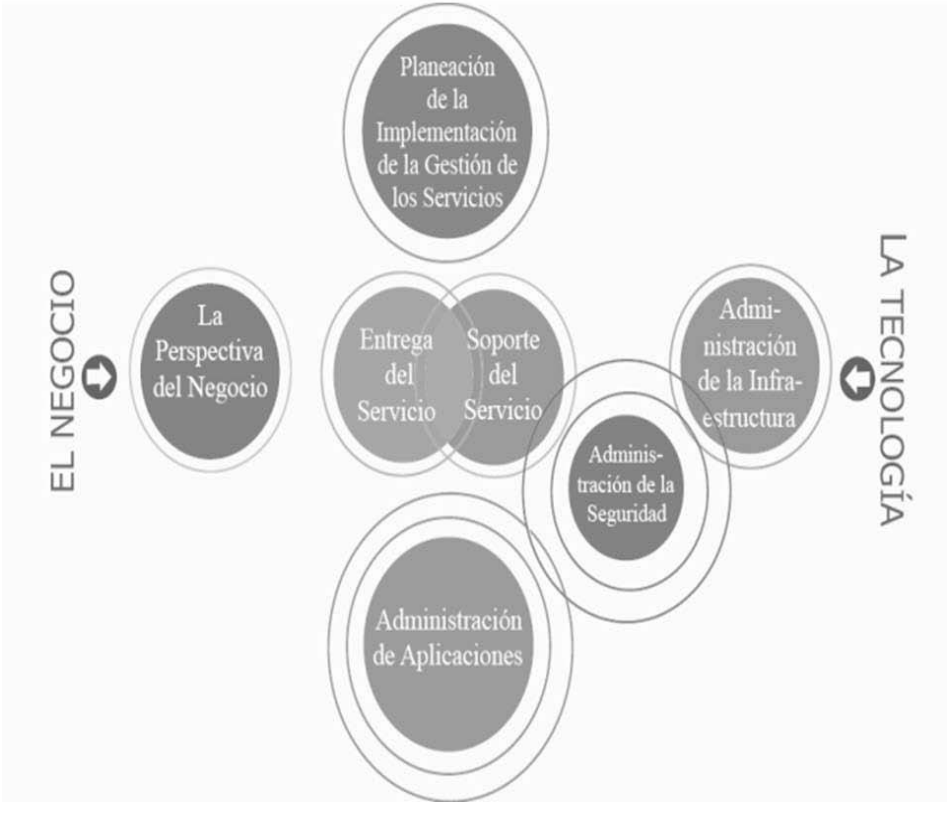
·Seguridad Lógica
·Seguridad Física
·Seguridad Organizativa
·Seguridad Legal

ISO serie 27000 : Fue aprobada y publicada como estándar internacional en octubre del 2005 y comprende:

- ISO 27000: Términos y definiciones que se emplean en todas la serie 27000
- ISO 27001: Norma principal de requisitos del Sistema de Gestión de Seguridad de la Información – SGSI.
- ISO 27002: Guía de buenas prácticas de objetivos de control y controles en cuanto a la seguridad de la información.
- ISO 27003: Guía de Implementación de Sistema de Gestión de Seguridad de la Información – SGSI.
- ISO 27004: Matrices y Técnicas de Medida de Sistema de Gestión de Seguridad de la Información – SGSI.
- ISO 27005: Guía para la Gestión de Riesgo de la Seguridad.
- ISO 27006: Requisitos de Acreditación de Entidades de Auditoria y Certificación.

ITIL

El significado de ITIL es Information Technology Infrastructure Librery (Biblioteca de la Infraestructura de las Tecnologías de la Información), como su nombre lo expresa es un grupo de libros, los cuales publican un conjunto de mejores prácticas para la Gestión de Servicios de Tecnología de la Información, conocidas como Gestión de Servicios de TI (ITSM - IT Service Management), el propósito de la Gestión de Servicios de TI es cerrar la brecha entre el Negocio y la Tecnología. En el siguiente diagrama se presenta los libros que integran a ITIL:



Grafica 3: ITIL y los libros relacionados
Fuente: Descubriendo ITIL

Los procesos de Soporte al Servicio son 6 de acuerdo con el siguiente detalle:

- Mesa de Ayuda
- Administración de Incidentes
- Administración de Problemas
- Administración de Cambios
- Administración de Configuraciones
- Administración de Liberaciones

Respecto de los Procesos de Entrega de Servicio son 5 de acuerdo con el siguiente detalle:

- Administración de Niveles de Servicio
- Administración Financiera
- Administración de Capacidad
- Administración de Continuidad
- Administración de Disponibilidad

Este tipo estándar es certificable y creada originalmente por el Gobierno de Gran Bretaña y actualmente se ha expandido su uso a múltiples organizaciones a nivel mundial, siendo publicada por la Organización de Comercio de dicho país.

COBIT

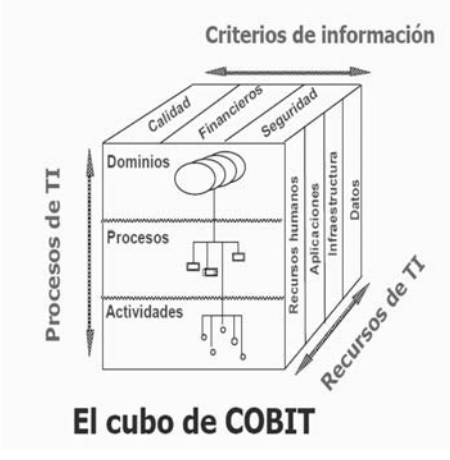
El COBIT significa Control Objectives For Information and Related Technology (Gobierno, Control y Auditoria de la Información y su Tecnología Relacionada), en su marco de referencia explica:

· El Enfoque en el Negocio
· La Orientación hacia los Procesos
· Los Recursos de TI

Comienza con la premisa de que la TI necesita entregar la información que la organización necesita para alcanzar sus objetivos. Se encarga de promover su enfoque a los procesos y a la propiedad de los procesos, dividiendo la TI en 34 procesos que pertenecen a cuatro dominios y provee un objetivo de control de alto nivel para cada uno de ellos;

- Planificar y Organizar
- Adquirir e Implementar
- Entregar y dar Soporte
- Monitorear y Evaluar

Debiendo ser analizados los componentes de un ambiente de TI de acuerdo a con la siguiente percepción:



Grafica 4: Cubo de COBIT
Fuente: ISACA-COBIT

Considera además las necesidades fiduciarias de calidad y seguridad de las organizaciones, proveyendo siete criterios de información que pueden ser usados genéricamente para definir genéricamente lo que el negocio requiere de TI, estos son soportados por un conjunto de más de 300 objetivos de control detallados:

- Efectividad
- Eficiencia
- Disponibilidad
- Integridad
- Confidencialidad
- Confiabilidad
- Cumplimiento

Los principios del marco de referencia del COBIT son:

Grafica 5: Principios Marco de referencia del COBIT
Fuente: ISACA-COBIT

Aplicación

Si se desea realizar Auditorías de Seguridad de la Información, se debe contar con el apoyo y conciencia de parte del plantel directivo, administrativo y ejecutivo de la empresa, con una visión estratégica de negocio de corto, mediano y largo plazo que permita la aplicación de:

- Modelos de Seguridad Empresarial
- Gobierno de TI
- Ciclos de Seguridad

Que puedan ser desarrollados e implementados dentro de la empresa y posteriormente ser evaluados por medio de Auditorias de Seguridad de la Información de acuerdo con estándares reconocidos y buenas prácticas de seguridad para luego ser certificados, permitiendo que la empresa garantice la seguridad de su información y su relación con la practica empresarial y de negocios en el ámbito de lo razonable y seguro para los interesados.

El profesional que se dedique a realizar Auditoria de Seguridad de la Información en las diferentes empresas tanto públicas como privadas, deberá contar con conocimientos tanto del área administrativa como de la tecnología y conocer los diferentes estándares con los cuales puede afrontar el trabajo encomendado y realizar el mismo con la profundidad necesaria de tal manera que beneficie a la empresa de acuerdo a las necesidades de la misma para su desarrollo no se debe olvidar que las herramientas utilizadas como ser:

- ISO 17799 – Códigos De Buenas Prácticas De Seguridad De La Información
- ISO SERIE 27000
- ITIL
- COBIT

Son las que apoyaran el desarrollo del trabajo para que luego sean informadas a los interesados y las mismas sirvan a la toma de decisiones.

3. CONCLUSION

Hoy en día la importancia de la administración de la seguridad de la información es un factor importante para proteger los activos de información, ya que se debe establecer una administración efectiva de la seguridad de la información, el advenimiento del comercio electrónico a través de los proveedores de servicios y directamente con los clientes, la perdida de barreras organizacionales y exposiciones de seguridad de alto perfil tales como riegos físicos (Robos, daños por siniestros, destrucción de equipamiento, etc.) y lógicos (Virus, acceso clandestino de redes, Violación de contraseñas, etc), han elevado el perfil de riesgo de la información y la necesidad de

administrar la Seguridad de la Información, motivo por el cual a cobrado importancia las Auditorias sobre la Seguridad de la Información, ya que las mismas permiten obtener una ventaja competitiva y satisfacer los requerimientos básicos del negocio, ya que las fallas pueden ser costosas para el mismo, las perdidas pueden ocurrir como resultado de la falla en la Seguridad de la Información. Un conjunto bien definido de políticas y procedimientos de seguridad puede prevenir perdidas y ahorrar dinero para la empresa y negocios, de ahí que la Auditoria de Seguridad de la Información cobra importancia como medio de detección de desviaciones de las políticas y procedimientos implantados por medio de herramientas de aplicación aceptadas a nivel mundial (Estándares, practicas, etc.) y permiten la retroalimentación para las correcciones o cambios oportunos en post de lograr mejorar la Seguridad de la Información y salvaguardar la misma.

4. BIBLIOGRAFIA

- Auditoria Un Enfoque Integral, 6ta. Edición, Alvin A.Arens, James K. Loebbecke, Edit. Prentice Hall, Mexico 1996
- Auditoria En Informatica, Un Enfoque Metodologico Y Práctico, 1ra. Edición, Lic. Enrique Hernández Hernández, Edit. Continental S.A. Mexico 1997.
- Auditoria Y Sistemas Informaticos, 1ra. Edición, Lázaro J. Blanco Encinosa, Edit. Latina Editores, Oruro – Bolivia 2001.
- Normas ISO
- Manual De Preparación Al Examen CISA 2003
- COBIT – Objetivos De Control Para La Información Y Tecnologías Aplicadas, 2da. Edición, Abril 2008.
- Descubriendo Itil, Asentti, Consultoría De TI Para Negocios.