Estudio del estándar para la seguridad de la información ISO 27002 y su comparación con los estándares ISO 27001, COBIT y OSSTMM

“Santander, tierra de retos”

Oscar Fernando González Flórez

Cod.33197030

Director: Mag. Roberto Carvajal Salamanca

OBJETIVO GENERAL

PROYECTO

Realizar una profundización del estándar para la seguridad de la información ISO 27002 que permita efectuar una comparación con los estándares ISO 27001, COBIT y OSSTMM.

OBJETIVOS ESPECIFICOS

PROYECTO

- **Estado del Arte sobre software de apoyo a la implementación de Sistemas de Gestión de Seguridad de Información (SGSI).**

PROYECTO

- **Establecer una comparación entre las siguientes estándares para la gestión de la información ISO 27002 – ISO 27001 – COBIT – OSSTMM que permita determinar las diferencias, similitudes y otros aspectos importantes de los mismos.**

PROYECTO

- **Diseñar y desarrollar un prototipo de una herramienta que apoye la gestión de controles de seguridad de la información, tomando como estándar ISO 27002.**

ESTADO DEL ARTE

ISO/IEC 27002

Se refiere a una serie de aspectos sobre la seguridad de las tecnologías de información, estableciendo diez dominios de control que cubren por completo la gestión de la seguridad de la información:

- Política de Seguridad
- Organización de la Seguridad
- Gestión de Activos
- Seguridad ligada a los recursos humanos

PROYECTO

- Seguridad física y ambiental.
- Administración de comunicaciones y operaciones.
- Control de Acceso.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de Incidentes en la Seguridad de la Información.
- Gestión de la continuidad del negocio.
- Cumplimiento de la normatividad.

Cuadro comparativo de herramientas de Sistemas de Gestión de Seguridad de la Información

PROYECTO

CUADRO COMPARATIVO DE HERRAMIENTAS SGSI					
HERRAMIENTA CARACTERISTICA	**GXSGSI**	**GLOBAL SGSI**	**E-PULPO**	**MEYCOR COBIT KP**	**SECUWARE SECURITY**
Creador	SIGEA	AUDISEC	INGENIA	DATASEC	SECUWARE
Sistemas operativo	WINDOWS XP/VISTA/2000/2003	WINDOWS XP/VISTA/2000/2003	INSTALADO EN UN APPLIANCE HARDWARE PLATAFORMA VIRTUAL CLOUD INGENIA	WINDOWS XP/VISTA/WINDOWS 7/2000/SERVER 2003-2008	WINDOWS XP/VISTA/2000 ADMINISTRACIÓN: WINDOWS 2000 PROFESIONAL Y SERVER/XP/2003 SERVER
Licencia	COMERCIAL	COMERCIAL	GNU GPL V2	COMERCIAL	COMERCIAL
Estándares Incluidos	UNE 71502 – ISO 27001 – ISO27002	ISO27001	ITIL-LOPD-ENS-ISO27001-ISO27002-ISO20000	ISO27001-COBIT-ISO27002-ISO20000-COSO I-COSOII	NINGUNO (SUITE EMPRESARIAL)
Gestión Documental	-	X	X	X	-
Gestión de Incidencias	X	X	X	X	-
Autoevaluación	-	X	-	X	-

CONTEXTO REGIONAL Y NACIONAL

Son escasos los antecedentes de herramientas de administración de información de controles de seguridad informática a nivel regional y nacional; esto no permite encontrar una referencia para emplear como referencia.

Comparativo ISO27001/27002 COBIT Y OSSTMM

PROYECTO

CUADRO COMPARATIVO DE ESTÁNDARES				
Comparación / Detalle	**ISO 27001**	**ISO27002**	**COBIT**	**OSSTMM**
Creación	Estándar creado en octubre del 2005	Su versión inicial se llamo ISO17799 creada en el año 2000 y actualizada y renombrada en octubre del 2005.	La primera edición fue en le año de 1996. A sido actualizada en cuarto ocasiones hasta el año 2012 versión 5.0	Primera edición del manual fue publicada en el año 2000 y su actualización actual es la versión 3
Creadores	International Organization for Standardization y por la comisión International Electrotechnical Commission.	International Organization for Standardization y por la comisión International Electrotechnical Commission.	ITGI (Instituto de Administración de TI) su creador	Consenso entre más de 150 expertos internacionales sobre el tema, que colaboran entre sí mediante Internet.
Alcance	Definir el ámbito del sistemas de gestión de la información	Expone los objetivos de seguridad a perseguir , consideración(controles) y sugerencias para los controles de Seguridad de a información	Define controles de Gobierno de Tecnologías de la información, que es el sistema por el cual se dirigen y controlan las TI en las Organizaciones	Testeo (pruebas) de la Seguridad.
Orientación	Estándar de Calidad	Estándar de Calidad	Guía de controles	Manual de pruebas
Tamaño	Consta de 39 objetivos de control y 133 controles	Consta de 11 dominios, 39 objetivos de control y 133 controles	Consta de 4 Dominios, 34 procesos de tecnologías de información y 318 objetivos de control.	Consta de 6 fases

PROYECTO

	ISO 27001	ISO27002	COBIT	OSSTMM
Fortalezas	Como Estándar se sitúan en el mayor nivel de cumplimiento .	Como Estándar se sitúan en el mayor nivel de cumplimiento .	Se basa en prácticas para garantizar el Gobierno de TI, proporcionando un nivel intermedio de cumplimiento .	Permite evaluar el nivel de seguridad de las tecnologías de información en un nivel intermedio
Debilidades	Es necesario para su éxito la implementación de la ISO27002	Es necesario para su éxito la implementación de la ISO27001	Esta orientada solo al gobierno de TI.	Esta orientada sólo a tecnologías de Información Basadas en la Web .

Conclusiones Cuadro Comparativo ISO27001/27002 COBIT Y OSSTMM

- La toma de decisiones sobre la seguridad de los activos críticos de información se basa en información a priori (Análisis de Riesgos) y a posteriori (Auditoría e Indicadores).

- Si se decide obtener la certificación ISO27002 del Sistema, mejora la imagen del organismo y se contribuye a generar confianza entre los usuarios y la empresa.

PROYECTO

Prototipo de sistema Web que apoya la gestión de controles de un Sistema de Gestión de Seguridad de la Información

PROYECTO

CONCLUSIONES

- Se desarrolló un sistema web basado en software libre para el apoyo en la toma de decisiones sobre seguridad de sistemas de información basado en el estándar internacional ISO 27002.

- No se pudo acceder a un referente sobre el contexto estudiado a nivel regional y nacional; dado que las herramientas existentes son diseñadas por firmas de auditoría para casos específicos.

PROYECTO

- Por medio de los SGCSI (Sistemas de Gestión de Configuración de Sistemas de Información) se pueden abarcar lo referente al HPVA (Hacer, Planear, Verificar, Actuar), teniendo como base la norma ISO 27002 con sus respectivos dominios y controles; para su aplicación en las organizaciones y de ésta manera el equipo de seguridad soportar sus decisiones apoyado en los resultados obtenidos en la auditoria.

PROYECTO

- Por medio de este trabajo de grado se puede establecer que en el contexto general de las organizaciones el control de la gestión de seguridad de la información se encuentra aislada a la toma de decisiones; permitiéndonos por medio de la herramienta generada un soporte sólido para establecer políticas claras y bien definidas, que apoye el proceso de evaluación.

RECOMENDACIONES

El sistema generado permite la adaptación de otros estándares diferentes a la ISO 27002, tales como OSSTMM y COBIT

GRACIAS