ESTADO DE CUMPLIMIENTO DE LOS CONTROLES DE SEGURIDAD EN LA UNIVERSIDAD

Tomado de: http://3.bp.blogspot.com/_ZyTVfswPHds/S03546fQ42I/AAAAAAAABHQ/CJqhD-XJsqQ/s400/inteco.jpg

UAB Universitat Autònoma de Barcelona
UOC www.uoc.edu
Universitat Rovira i Virgili

Lorena Suárez Sierra
Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Controles de seguridad de la información

- Los controles de seguridad de la ISO/IEC 27000:2005 , estandariza un grupos de controles que una empresa debe tener para considerar que tiene un plan o un sistema de seguridad implementado para su información. Los grupos de controles son:

- ✓ Política de Seguridad
- ✓ Gestión de comunicación y operaciones
- ✓ Control de acceso
- ✓ Gestión de activos
- ✓ Seguridad ligada a los recursos humanos
- ✓ Seguridad física y ambiental
- ✓ Gestión de comunicaciones y operaciones
- ✓ Adquisición, desarrollo y mantenimiento de los sistemas de información
- ✓ Gestión de incidentes de la seguridad de la información
- ✓ Gestión de la continuidad del negocio
- ✓ Cumplimiento

Sistema de seguridad de la información actual en la universidad

De acuerdo al diagnóstico previo realizado con el análisis diferencial que se plantea en la primera etapa del SGSI, se puede afirmar que, la institución se encuentra en un nivel *muy bajo* sobre la seguridad de su información porque no existe un grupo de controles implementados totalmente, solamente existen pocos subcontroles implementados y la mayoría sin implementar o parcialmente implementados. En consecuencia, en la primera fase del SGSI se concluye que:

- De acuerdo al volumen de información manejada por la universidad y el tamaño actual, se estima realizar la implantación del SGSI por áreas o dependencias.

- Actualmente no existe planteado compromiso por parte de la dirección para la disposición y los recursos económicos necesario para la implantación del SGSI.

Tomada de: http://www.audienciaelectronica.net/wp-content/uploads/2011/11/SeguridadInformatica01.jpg

Sistema de seguridad de la información actual en la universidad

- No existe capacitación en relación a la seguridad de la información a los empleados que manejan y administra los sistemas informáticos físicos y lógicos
- No existe una programación a corto y mediano plazo sobre la implementación de controles de seguridad en la empresa, es decir no se tiene contemplado.
- No existe concientización por parte del personal de proteger debidamente los activos informáticos que posee y los sistemas de información que manejan.
- Se ve con mucha claridad el riesgo de presentar incidentes de seguridad en la información en la universidad.

Objetivos

- En relación al diagnóstico general realizado en la universidad se considera plantear los siguientes objetivos :

Objetivo General

Elaborar el plan de implementación de Sistema de Gestión de la Seguridad de la Información bajo la ISO/IEC 27001:2005.

Objetivos específicos

- Analizar y conocer a fondo el grado de seguridad de información que actualmente posee la empresa
- Realizar planes de acción que permitan involucrar al personal encargado de la oficina de sistemas para todo el proceso de planeación para la implementación del SGSI
- Realizar el análisis de riesgos para la evaluación exahustiva de los activos que la empresa actualmente posee y la valoración de los mismos.
- Proponer las medidas correctoras planificadas para garantizar el nivel de seguridad más adecuado a las necesidades de la universidad.

Objetivos

Objetivos específicos

- Definir los documentos que soportan los sistemas de seguridad de la organización
- Definir los planes de continuidad de negocio necesario para la preservación en caso de incidentes
- Determinar las amenazas a las que se encuentra expuesta la organización
- Definir los costos de inversión que aseguren la implentación del SGSI con todos los recursos físicos, lógicos y de personal necesario.
- Definir los planes de capacitación para la formación en el área de la seguridad informática al personal de la oficina de sistemas de la universidad.

Actividades a corto, mediano y largo plazo para la protección de la información en l Univesidad

CORTO PLAZO

- Definición de compromiso por parte de la dirección para la implantación del SGSI bajo normativa ISO/IEC 27000
- Determinación del alcance (áreas relevantes para la implantación del SGSI)
- Determinación del personal responsable de la implantación
- Creación y definición del comité de seguridad de la información en la empresa
- Estimación y reserva de recursos económicos y físicos

MEDIANO PLAZO

- Cuerpo documental para el cumplimiento normativo
- Análisis de riesgos
- Planes de tratamiento de riesgos
- Auditoría de cumplimiento
- Planes de continuidad de negocio
- Auditoría interna

Largo Plazo

- Implementación del SGSI a toda la empresa
- Auditoría interna para certificación del SGSI ISO/IEC 27000:2005
- Solicitud de auditoría externa para certificación

Conclusiones y recomendaciones

- Implantar un SGSI no genera dividendos pero salvaguarda el activo mas importante que es la "*información*"
- La seguridad de la información es la continuidad del negocio a pesar de la materialización de las amenazas
- La tecnología de la información y las comunicaciones avanza vertiginosamente para volver a las empresas mas competitivas pero trae consigo la amenaza latente de los delincuentes y ociosos cibernauticos
- Implementación de un SGSI incluye la capacitación y concientización de los funcionarios de la empresa, evitando el ataque de ingeniería social[1]

[1]**Ingeniería Social:** s la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos