PRESENTACION DE RESULTADOS DEL ESTUDIO DE IMPLANTACION DEL SGSI

Imagen tomado de: http://www.atletaergo.com/wp-content/uploads/2012/06/resultados0.jpeg

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

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

Resultados análisis de riesgos

Nivel de riesgo

En relación al análisis de riesgo realizado en se estima la frecuencia en que podrían ocurrir las amenazas en cada uno de los activos y el impacto porcentual identificado, en caso de que ocurra dicha amenaza, se evidenció que el nivel de riesgos que actualmente se encuentra la universidad es *alto,* en las dimensiones de seguridad de disponibilidad y confiabilidad. En la dimensión de Integridad se detectó un nivel de riesgo medio.

Disponibilidad	Integridad	confiabilidad
Alto	Medio	Bajo

Nivel de riesgo aceptable : Es el riesgo que la institución puede asumir después de aplicar los controles mínimos de seguridad. De acuerdo a los resultados el nivel de riesgo aceptable es *medio.*

Resultados análisis de riesgos

Nivel de riesgo Residual: es el riesgo que se encuentra por debajo del riesgo aceptable, es decir, es el riesgo que sigue existiendo después de aplicar los controles de seguridad. Este nivel de riego es *bajo*

Riesgos a reducir

Los riesgos que se deben reducir en la institución son aquellos que afectan las tres principales dimensiones de seguridad (confiabilidad, disponibilidad, integridad) y de acuerdo al análisis de riesgo realizado, actualmente la institución se encuentra en riesgo de sufrir amenazas a los activos que generan y almacenan la información que se debe procesar para el cumplimiento de su misión institucional. Los riesgos que se evidencian en la organización son:

- ✓ Falta de la debida protección física de los equipos informáticos, de comunicaciones y redes
- ✓ Falta de protección en los sistemas de información en manipulación y control de acceso
- ✓ Falta de desarrollo de software seguro
- ✓ Desconocimiento de políticas y tecnicas mínimas de seguridad por parte de los empleados.

Análisis de costo- beneficio

El costo- beneficio que la universidad puede obtener al invertir en la implementación de un SGSI ISO/IEC 2700: 2005 certificables, es a través de la implementación de medidas preventivas y las medidas curativas.

La estimación de costo de implementación de cada grupo de medidas de seguridad se realiza de acuerdo al esfuerzo por los gestores y equipos de personal estratégicos, personal técnico de instalación, herramientas, sistemas técnicos diseñados para evitar, controlar o recuperar los daños que pueden sufrir los activos informáticos sobre determinada amenaza de seguridad.

La estimación de costo en pesos colombianos por cada medida de seguridad se presenta en la siguiente tabla 2.

Análisis de costo- beneficio

MEDIDAS O SALVAGUARDIAS DE SEGURIDAD	TIEMPO DE INSTALACION EN MESES	ESTIMACION DE COSTOS EN PESOS
[HW]Protección de los Equipos Informáticos	2	$ 80.000.000
[AUX] Elementos Auxiliares	1	$ 20.000.000
[L] Protección de las Instalaciones	2	$ 30.000.000
[SW] Protección de las Aplicaciones Informáticas	3	$ 120.000.000
[SI] Protección de los Soportes de Información	3	$ 10.000.000
[P] Gestión del Personal	4	$ 25.000.000
Total	**15**	**$ 285.000.000**

Tabla No. 2 de estimación de costos de las medidas de seguridad

Con la implantación de las medidas mencionadas en la tabla 2, la universidad reduciría los riesgos detectados en un 5%, equivalente a muy bajo

PLAN DE ACCION

Los planes de acción que se consideran debe hacer la universidad son:

1. La dirección deberá establecer compromiso de la implantación del sistema de gestión de la seguridad informática SGSI bajo normativa ISO/IEC 27000:2005 a través del plan de actividades de cada una de las fase que componen el SGSI

2. Se debe presentar ante el consejo superior el costo que se estima para la implantación con su debida justificación para que sea aprobado por dicho consejo

3. Dada la aprobación respectiva, la dirección deberá seleccionar y asignar el equipo de personal apropiado para la implementación del SGSI y deberá programar la fecha de inicio y terminación.

PLANES DE ACCION

4. La dirección deberá crear el comité de seguridad de la información de la institución para la debida evaluación y verificación del proceso de implementación del SGSI

5. Una vez asignado o contratado el personal que implementará el SGSI, éste deberá presentar el cronograma de actividades a desarrollar , los responsables de cada una de las actividades y los costos que se puedan requerir en la implementación e cada uno de los controles de seguridad

6. Al estar definidos los anteriores items, la dirección deberá oficializar ante los funcionarios de la institución la puesta en marcha del proceso de implantación del SGSI