Sistema de Gestión de la Seguridad de la Información.

RESUMEN EJECUTIVO

Estudiante: Luis Fernando Echeverría

Programa: Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Consultor: Antonio José Segovia Henares.

Centro: Universitat Oberta de Catalunya.

Entrega: Enero de 2018.

RESUMEN EJECUTIVO

I INTRODUCCION

El presente proyecto ha consistido en la elaboración de un Plan Director de Seguridad para una institución de educación superior pública con alcance a los procesos medulares que se encuentran dentro de los Procesos Agregado de Valor Docencia.

Este Plan director de seguridad se basa en el estándar internacional ISO/IEC 27001:2013 y la guía de buenas prácticas ISO 27002:2013.

II OBJETIVO

El plan director de seguridad es una hoja de ruta que debe seguir la institución para conseguir gestionar de forma adecuada la seguridad, para la definición del plan director de seguridad se deberán contemplar lo siguiente:

Objetivo General

Definir un plan director de seguridad de la información que esté acorde con los lineamientos generales que la institución educativa debe seguir para garantizar la protección y el buen uso de la información y los sistemas de información que la entidad utiliza.

Objetivos específicos

- Crear proyectos basados en los resultados obtenidos en el análisis de riesgos y que estén alineados de acuerdo a las normas ISO/IEC 27001 e ISO/IEC 27002.
- Definir directrices en materia de la seguridad de la información.
- Identificar el nivel de seguridad existente en los sistemas, servicios y aplicaciones en la administración de la información.
- Identificar los riesgos a los cuales están expuestos los activos de la institución.
- Definir los roles, las responsabilidades en materia de seguridad para estudiantes, docentes y personal administrativo.
- Crear y promover la cultura de seguridad de la información dentro de la institución.
- Implantar y hacer un seguimiento del plan de seguridad definido.

III METODOLOGIA

La metodología del desarrollo del proyecto está estructurada en 5 fases:

- En la fase 1 se realiza una descripción de la organización sobre la que se implanta el proyecto y se ha elaborado un análisis diferencial de la situación actual de la seguridad con respecto a las normas ISO 27001:2013 e ISO 27002:2013. Los resultados de este análisis muestran que la institución por ser una entidad nueva tiene que implementar varios controles, el nivel de implementación es bajo. Con un 20% con respecto a la ISO27001 y 28% con respecto a la 27002, muestra que la institución cuenta con una medida baja de seguridad, por lo que se ve una necesidad urgente de implementar un SGSI con los objetivos más altos.

- En la fase 2 se han definido los documentos de base que se necesitan para el cumplimiento normativo de la ISO 27001:2013: Documento de Política de Seguridad; Procedimiento de Auditorías Internas; Gestión de Indicadores; Procedimiento Revisión por Dirección; Gestión de Roles y Responsabilidades; Declaración de Aplicabilidad; y la Metodología de Análisis de Riesgos. En esta etapa es primordial la participación de la Alta Dirección para su aprobación y sobre todo fijar el Procedimiento de Revisión por parte de la Dirección.

- En la fase 3, se ha realizado el análisis de riesgos siguiendo la metodología MAGERIT v3, este análisis parte de la identificación y valoración de todos los activos de la organización de acuerdo a las diferentes dimensiones de seguridad. Para luego realizar un análisis de amenazas a las que está expuesta la organización y, por último, se ha calculado el impacto y riesgo potencial de cada uno de los activos. Como resultado se han identificado los diferentes niveles de riesgo de los activos. Se encontraron 46 activos en estado de riesgo potencial Alto y Muy Alto, entre los activos con mayores riesgos se han podido identificar los datos correspondientes a estudiantes, docentes y personal administrativo.

- En la fase 4 teniendo como se han planteado 4 proyectos a implementar con el fin de mitigar los principales riesgos que se han encontrado en la fase 3. Estos proyectos buscan en general mejorar el estado de la seguridad de la información de la organización. Si bien estos surgen como una respuesta a los riesgos que se han identificado, estos proyectos no solo tienen el objetivo de mitigar los riesgos sino también otros beneficios colaterales. Para cada uno de estos proyectos se especifica el código del proyecto, nombre del proyecto, dominios afectados, objetivo, descripción, responsable de la ejecución, duración, costes, así como los riesgos a los que se desean mitigar. Además del impacto sobre las dimensiones de la seguridad, se presenta un plan de implantación de estos proyectos en los diferentes plazos.

- En la fase 5, se ha realizado una auditoria de cumplimiento, que mide el grado de cumplimiento con respecto a los controles de la norma. Estos resultados confirman

una mejora en los niveles de seguridad con respecto a los niveles que se habían obtenido en la fase inicial. Si bien el nivel no es el objetivo que se persigue, se constata que ha habido una evolución importante en el nivel de cumplimiento para la mayoría de los dominios de la norma. Por otro lado, esta auditoria ha permitido identificar principalmente las no conformidades y para las cuales se propondrán acciones correctoras.

IV CONCLUSIONES

- Tras haber finalizado todas las fases del proyecto, y en base a los resultados obtenidos se concluye que la implantación del plan director de seguridad ha mejorado el nivel de seguridad de la información en la institución.

- La implementación de un Plan de Seguridad de la Información es un proceso continuo que busca mejorar de los niveles de Seguridad en el manejo de la Información y que esté acorde a las necesidades institucionales.

- El éxito de este plan requiere de la participación y del compromiso de todos los miembros de la institución (estudiantes, docentes y personal administrativo) y principalmente de la Dirección. Es la dirección que debe garantizar el cumplimiento de los planes y objetivos de la seguridad del a información.

- Este plan debe ser la única guía corporativa que implementa las medidas de seguridad de la información y los sistemas de información dentro de la organización.

- El plan de formación/concientización es fundamental para el éxito de este plan. Si bien se ha logrado mejorar los niveles de concientización del personal, se recomienda que el proceso de formación sea continuo.