# ELABORACIÓN DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN

## RESUMEN EJECUTIVO

**Nombre Estudiante: Ruth Aguilar Escobar**

**Programa:** Posgrado en Seguridad en servicios y aplicaciones

**Nombre Consultor:** Arsenio Tortajada Gallego

**Centro:** UOC

**Data Entrega:** 06/2017

## RESUMEN EJECUTIVO

## I INTRODUCCION

El presente proyecto ha consistido en la elaboración de un Plan Director de Seguridad para la empresa A2, un proveedor de servicios financieros, principalmente seguros de vida.

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

## II OBJETIVO

Implementación de este plan de seguridad de la información que sirva de guía corporativa para la implantación de las medidas de seguridad de la información y los sistemas de información dentro de la organización.

## III METODOLOGIA

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

- En la fase 1 se ha descrito la organización sobre la que se implanta el proyecto y se ha realizado 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 empresa si bien tiene implementados algunos controles, el nivel de implementación es relativamente bajo. Con un 50% con respecto a la ISO27001 y 63% con respecto a la 27002, muestra que la empresa ya tiene cuenta con algunas medidas de seguridad, pero que necesitan estas ser revisadas para llegar a objetivos mas 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 de revisión por la 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 Dirección para concretizar la aprobación del documento de las políticas de seguridad, para crea la estructura de seguridad y asignar roles y responsabilidades y aprobar el procedimiento de la 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 los diferentes dominios de activos de . 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. Entre los activos con mayores riesgos se han podido identificar los datos correspondientes a los clientes, el código fuente de

las aplicaciones de gestión, los registros de los servidores de producción, y ciertas categorías de personal.

- En la fase 4 teniendo como se han planteado 11 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 naces como una respuesta los riesgos que se han identificado, estos proyectos no solo tienen el objetivo de mitigar los riesgos sino también oros beneficio colaterales. Para cada uno de estos proyectos se especifica la descripción, le responsable de la ejecución, los activos que afectara, los dominios de la seguridad que serán afectados, así como los riesgos a los que se desean mitigar. Además de una estimación en días, los recursos necesarios y los costos estimados. 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 optimo que se persigue, se constata que ha habido una evolución importante en el nivel 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 han propuesto 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 empresa.

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.

El éxito de este plan requiere de la participación y del compromiso de todos los miembros del personal 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 constituye la única guía corporativa que implementa de 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.