Plan Director de Seguridad

Resumen Ejecutivo

Autor: Luis Rodríguez Conde
Dirección: Antonio José Segovia Henares
Fecha: Junio, 2017

Universitat Rovira i Virgili
Universitat Oberta de Catalunya
Universitat Autònoma de Barcelona

Contenido

1. Introducción
2. Motivación del proyecto
3. Enfoque y alcance del proyecto
4. Esquema general del Plan Director
5. Conclusiones

1. Introducción

- El objetivo del presente documento es presentar el resumen ejecutivo de la implementación de un Plan Director de Seguridad para la implementación de la ISO/IEC 27001:2013 sobre la empresa Ícaro S.A.

- A continuación se presenta la motivación del proyecto, el enfoque escogido y las principales conclusiones tras su elaboración.

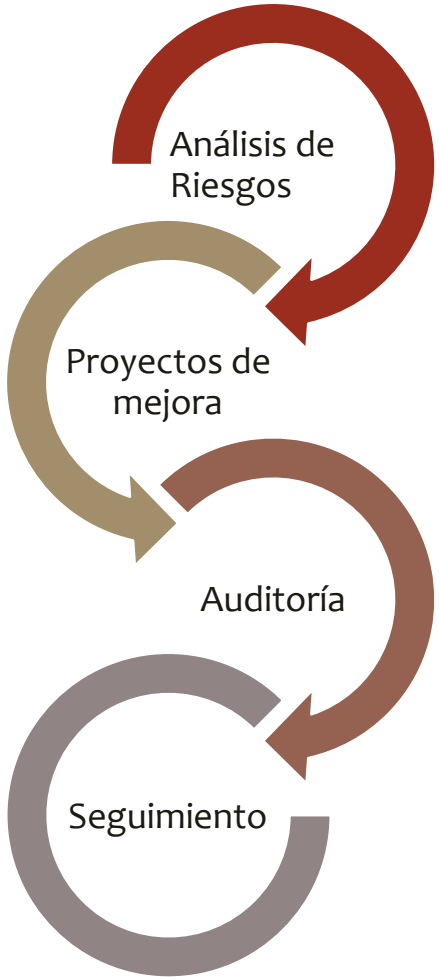
2. Motivación del proyecto

- Ícaro S.A. es una empresa dedicada al diseño, implementación y administración de sistemas de gestión de plantas solares fotovoltaicas en España. Actualmente la empresa se encuentra en una etapa de crecimiento donde algunos fondos de inversión están interesados en apostar por ella.
- Debida a esta situación se ha identificado la necesidad de mejorar y alinear sus procesos de negocio con el cumplimiento de los estándares internacionales para afrontar este nuevo reto.
- De esta iniciativa general, surge la motivación de definir un Plan Director de Seguridad de la Información, el cual permitirá a la empresa en primer lugar conocer su nivel actual en esta materia y definir las acciones necesarias para alcanzar el nivel de seguridad deseado y en segundo lugar identificar los procesos que le permitan ejecutar una mejora continua.

3. Enfoque y alcance del proyecto

- El proyecto está alineado bajo los estándares ISO/IEC 27001 y 27002 en su ultima versión del año 2013.
- El alcance del mismo son todos los sistemas de información que dan soporte a los procesos, actividades y servicios de la empresa.
- Actividades principales del Plan Director de Seguridad:
  - Análisis diferencial contra la ISO/IEC 27002 para conocer el estado previo.
  - Identificación de los activos relacionados con los procesos, actividades y servicios relacionados con la información.
  - Valoración de los activos identificados.
  - Análisis de amenazas de los activos respecto a las cinco dimensiones de seguridad.
  - Análisis del nivel de riesgo respecto a los activos, su valoración y sus amenazas.
  - Proposición de proyectos para la mitigación de los riesgos identificados como críticos.
  - Realización de una auditoría de cumplimiento tras la implementación de los proyectos.

4. Esquema general del Plan Director de Seguridad



- Se realiza un análisis de riesgos de la situación actual

- Se proponen mejoras para mitigar los riesgos y se ejecutan estas.

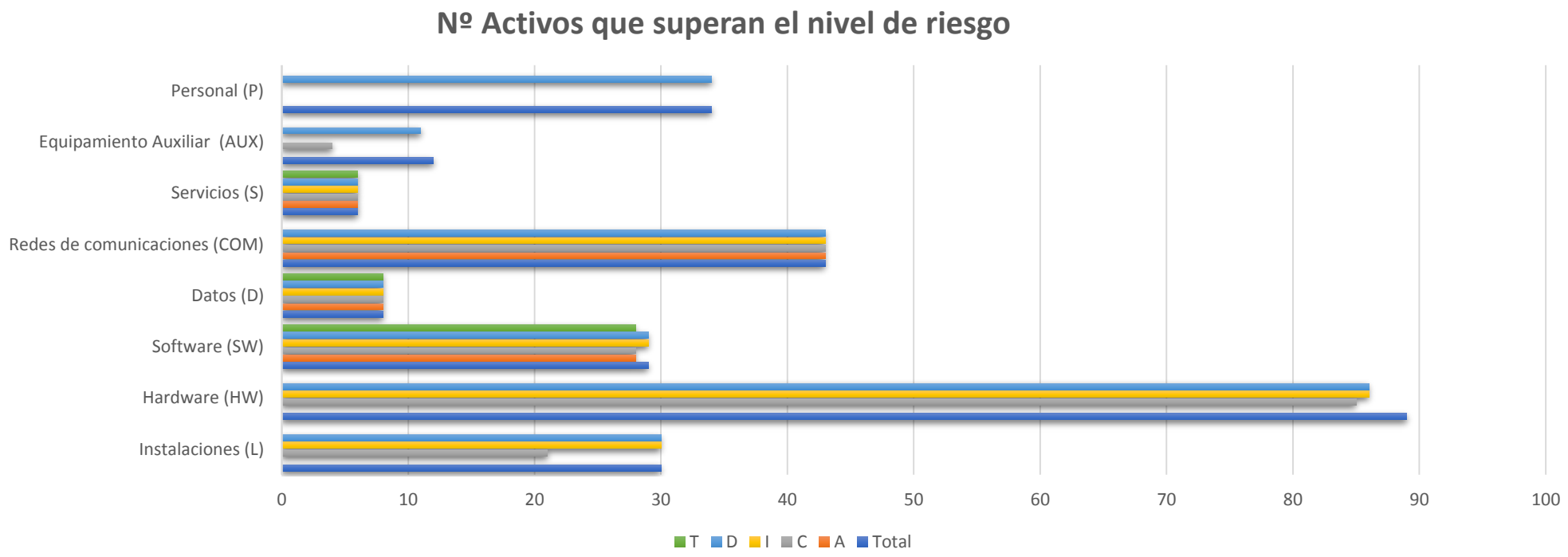
- Se realiza una auditoría para comprobar el impacto de las mejoras implantadas. De esta pueden salir No Conformidades que se deberán solventar.

- Se realiza seguimiento del mismo para mantener la mejora continua

5.1 Conclusiones

Análisis de riesgos

- Se han identificado 248 repartidos en 8 ámbitos.
- Se ha utilizado la metodología MAGERIT para:
  - Valoración de económica -> Estimada en 22.165.750€
  - Valoración por dimensiones de seguridad -> Valoración media de 6 puntos
  - La valoración de amenazas
- Una ve realizada la valoración se analiza el impacto y a parir de este el nivel de riesgo.



5.2 Conclusiones
Proposición de proyectos

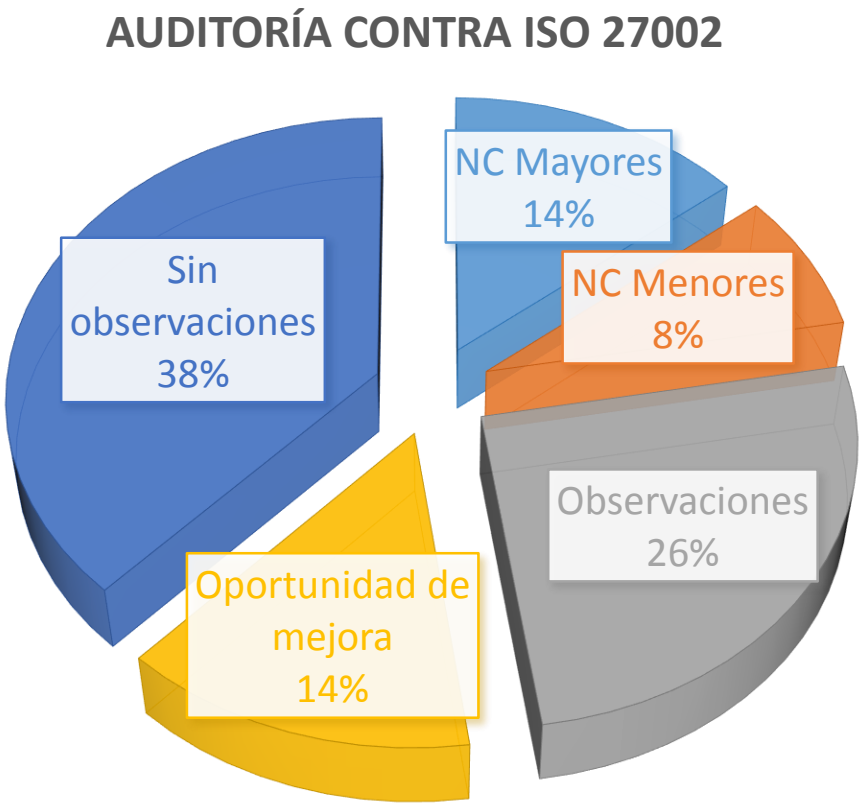
- Se han propuesto un total de 13 proyectos para mitigar los riesgos identificados que superan el nivel permitido. Se listan a continuación

- Mejora de la política de seguridad
- Formación continúa en materia de seguridad
- Mejora de la seguridad física en la plantas
- Mejora de la seguridad física en los acceso
- Mejora de la disponibilidad del sistema Sirio
- Cifrado de datos y en las comunicaciones del sistema Sirio.
- Cifrado de datos en PC's y móviles
- Virtualización entorno corporativo
- Comunicaciones profesionales acceso a Internet.
- Red MPLS para conexión de las plantas
- Mejora de la seguridad perimetral de CPD
- Revisión de la seguridad de la información
- Modelo de relación con proveedores.

- Para la planificación, se estima que la implantación de todos ellos conjuntamente será de un año.

5.3 Conclusiones
Auditoría contra ISO 27002

- El 78% de los controles ha superado la auditoría contra la norma.
- El 14% de los controles ha presentado No Conformidades Mayores
- El 8% de los controles ha presentado No Conformidades Menores



5.3 Conclusiones
Objetivos conseguidos

- Se ha establecido el estado inicial de la seguridad de la información de la organización, así como los objetivos a alcanzar tras la implantación del SGSI.
- Se ha definido y desarrollado el esquema documental necesario para el cumplimiento normativo de la ISO 27001:2013.
- Se ha realizado el análisis de riesgos de la organización del que se ha obtenido la lista de todos los activos de la empresa, las amenazas posibles a las que está expuesta la organización así el impacto y el riesgo de todos los activos de la empresa que ha permitido identificar los activos más prioritarios en cuanto a seguridad de la información.
- Se han definido y completado con éxito una serie de proyectos para mejorar la seguridad de la información de la organización, teniendo en cuenta al análisis de riesgos obtenido.
- Se ha evaluado el nivel de madurez de la seguridad de la información de la organización respecto a la norma ISO 27002:2013.
- Se ha conseguido reducir el riesgo de los activos de la organización.
- Tras la realización de todas las fases, se ha conseguido mejorar significativamente el estado inicial de la seguridad de la información de la organización.
- Se ha logrado la concienciación y colaboración de los empleados en materia de seguridad de la información.
- Existe el compromiso de revisar y mejorar el estado de la seguridad de la información de la organización de manera periódica.

Gracias por su atención

Universitat Rovira i Virgili

Luis Rodríguez Conde