Plan director de seguridad TrendTip

PRESENTACIÓN PARA LA DIRECCIÓN

Alumno: Beatriz Cantalejo García
Tutor: Antonio José Segovia Henares

Universitat de les Illes Balears

UNIVERSITAT ROVIRA i VIRGILI

Universitat Oberta de Catalunya

Universitat Autònoma de Barcelona

TrendTip

Índice

01 Introducción

Un Plan Director de Seguridad es uno de los elementos clave con los que debe contar una organización, ya que:

Provee los niveles de seguridad requeridos por la organización

Dota a la empresa de un plano de actuación frente a posibles amenazas

Toma como modelo de mejora continua PDCA **(Plan-Do-Check-Act)**.

La implementación de este se basa en las normas ISO 27001 y ISO 27002

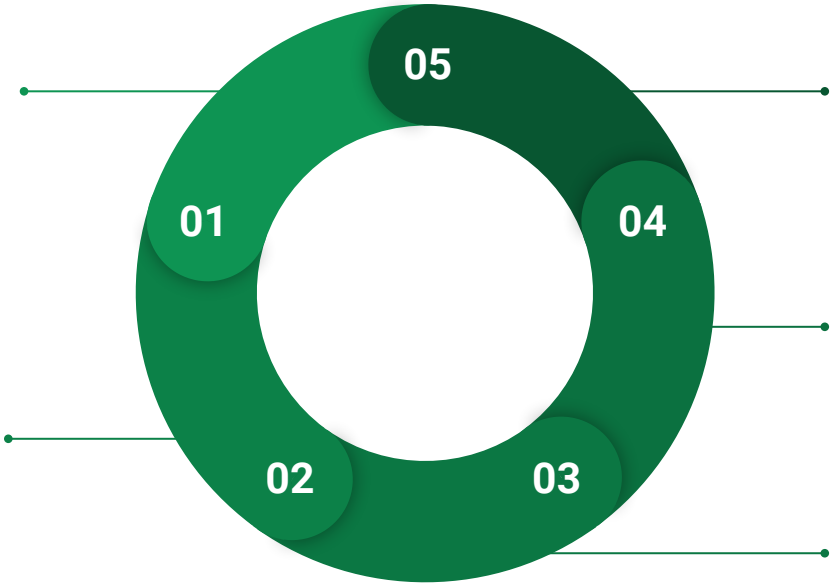
02 Fases del proyecto

Fase 1 -Situación inicial: Contextualización, objetivos y análisis diferencial

Introducción al Proyecto. Enfoque y selección de la empresa que será objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa con respecto la ISO/IEC 27001+ISO/IEC 27002

Fase 2 - Sistema de gestión documental

Elaboración Política de Seguridad. Declaración de aplicabilidad y Documentación del SGSI



Fase 5 - Auditoría de cumplimiento

Evaluación de controles, madurez y nivel de cumplimiento.

Fase 4: Propuesta de proyectos

Evaluación de proyectos que debe llevar a cabo la Organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de los mismos.

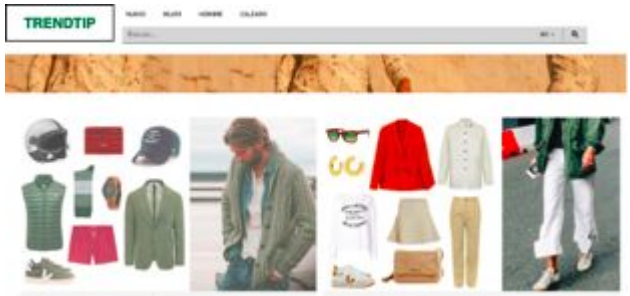
Fase 3 - Análisis de riesgos

Elaboración de una metodología de análisis de riesgos: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.

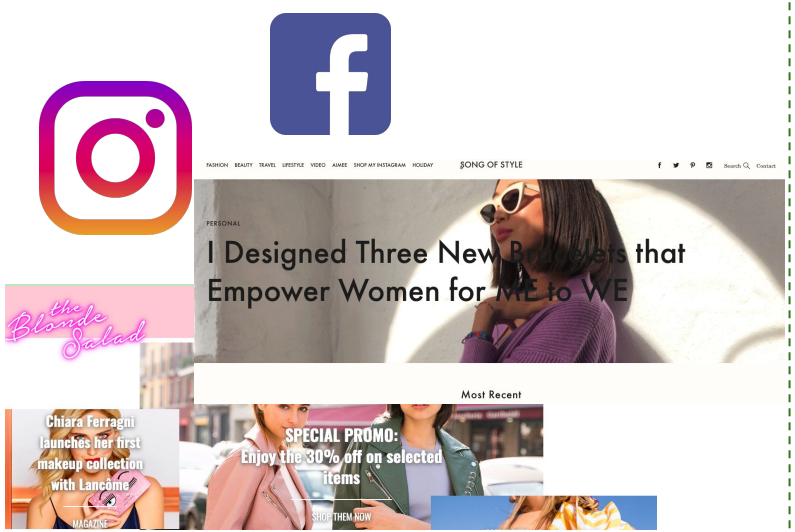
Fase 1: Situación inicial: Contextualización, objetivos y análisis diferencial

Alcance

La página web que hace de intermediaria entre los clientes y los proveedores finales:

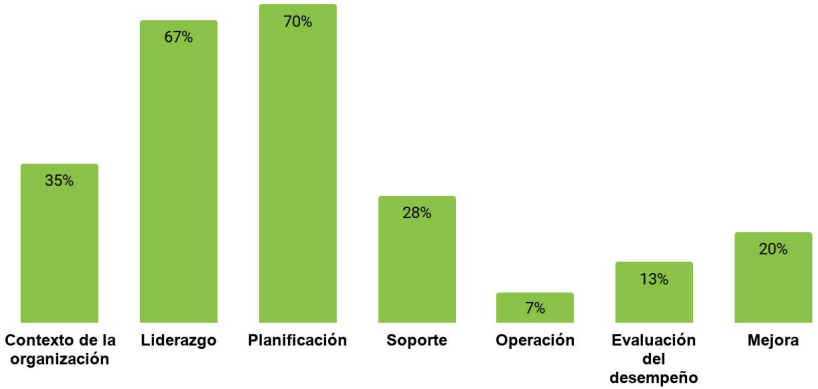


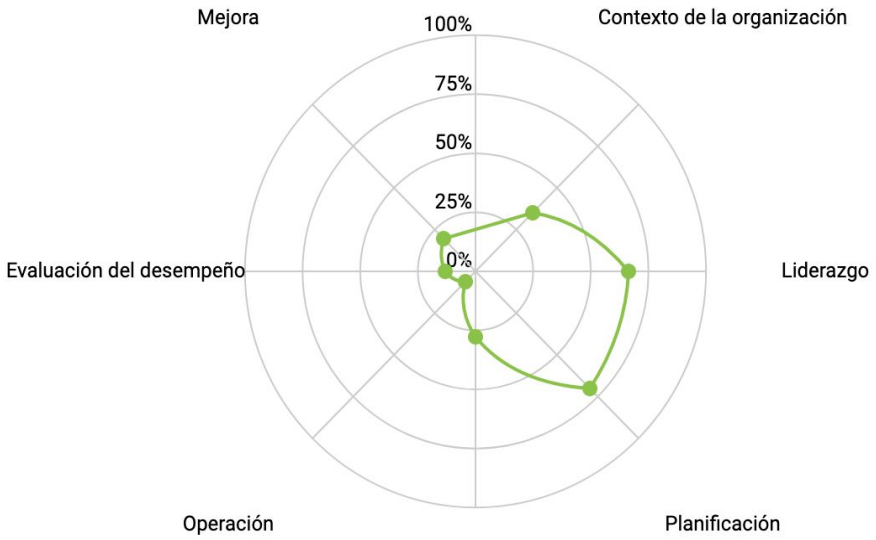
La búsqueda de tendencias y productos para su selección.



Situación inicial: Análisis diferencial ISO 27001

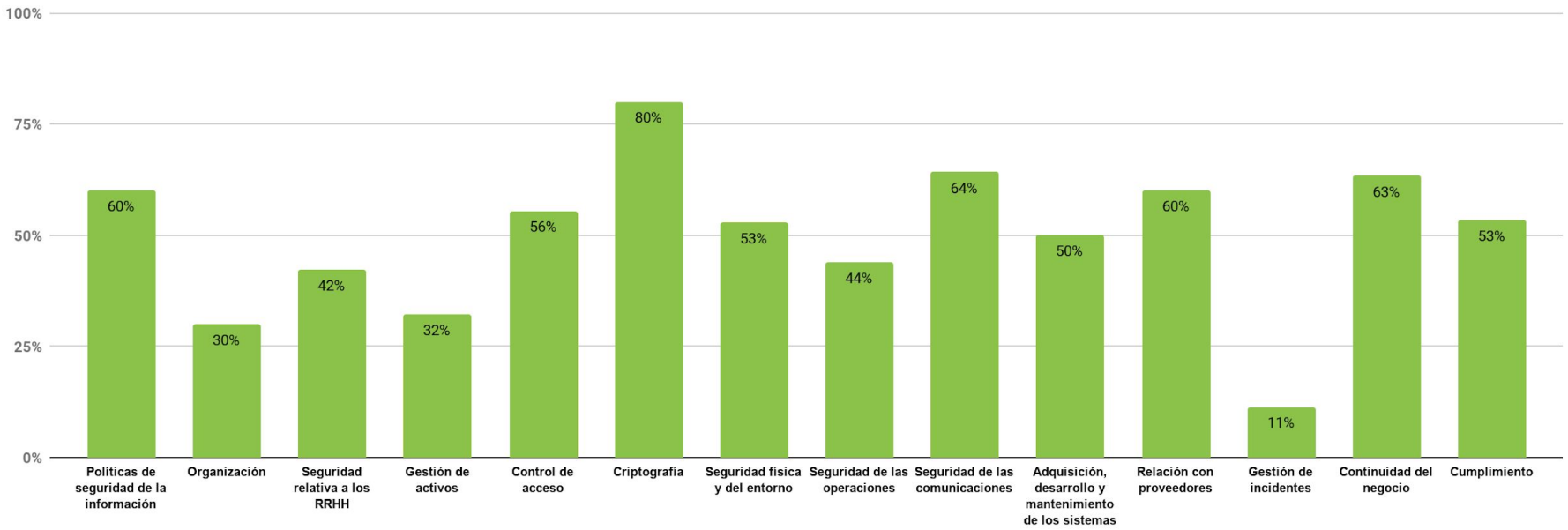
Porcentaje de cumplimiento de los controles de la ISO 27001





Situación inicial: Análisis diferencial ISO 27002

Porcentaje de cumplimiento de los controles de la ISO 27002



Fase 2: Sistema de gestión documental

Fase 2: Sistema de gestión documental

01 Política y normativa de seguridad

Norma de gestión de activos:
Norma gestión de la continuidad del negocio
Norma de gestión de incidentes
Norma de control de acceso
Norma de cumplimiento
Norma de operación
Norma de gestión de servicios cloud

02 Procedimiento de auditorías internas.

Documento donde se incluye una planificación de las auditorías que se llevarán a cabo

03 Procedimiento de revisión de la Dirección

La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información.

04 Gestión de indicadores

Indicadores para medir la eficacia de los controles de seguridad implantados

05 Gestión de roles y responsabilidades

El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema.

06 Metodología de análisis de riesgos

Sistemática que se seguirá para calcular el riesgo,

07 Declaración de aplicabilidad

Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.

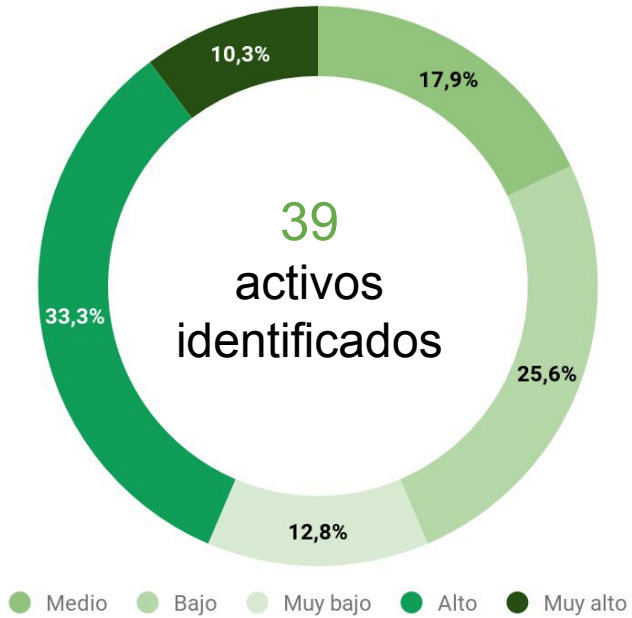
Fase 3: Análisis de riesgos

Fase 2: Análisis de riesgos

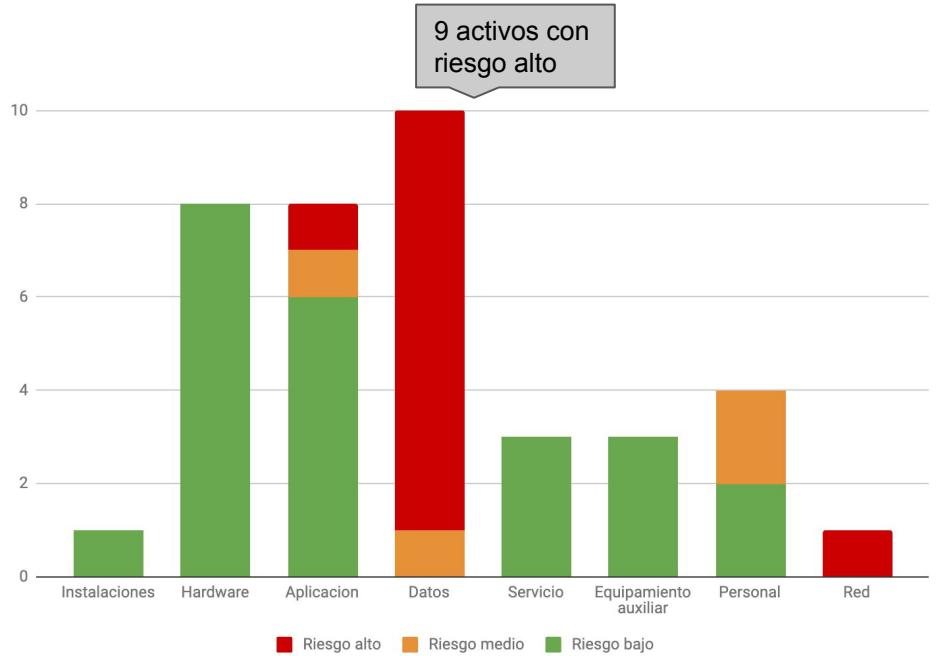
Inventario de activos	Valoración de los activos	Identificación y valoración de las amenazas	Categorización de las salvaguardas	Valoración del impacto y riesgo residual
Clasificación de los activos agrupándolos en varios tipos de acuerdo a la función que ejercen en el tratamiento	Valoración de los activos de acuerdo al impacto que puede causar en valor monetario su daño o pérdida	Identificación de todas las amenazas a las que los activos identificados se pueden ver expuestos .	En esta fase se caracterizan las salvaguardas a llevar a cabo para mitigar o reducir el riesgo.	Una vez analizado el impacto de las amenazas en las distintas dimensiones de seguridad, y dado que conocemos los valores de los diferentes activos, podemos determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas.

05 Fase 3: Análisis de riesgos

Valoración de los activos



Activos que superan el nivel de riesgo



Fase 4: Propuesta de proyectos

05 Fase 4: Proyectos propuestos

01 Plan de continuidad

3100 €

Definir una serie de mecanismos y medidas que aseguren la disponibilidad de los servicios críticos con el objetivo de reducir el impacto de los incidentes en la imagen de la organización

02 Plan de concienciación

1200 €

Concienciar a los empleados de TrendTip sobre los procedimientos y políticas de seguridad y el buen uso de los recursos.

03 Política de backups

Definir una política de backups que garantice la recuperación de los datos en caso de incidentes de seguridad

04 Plan de control de cambios

Verificar que los cambios y modificaciones que se llevan a cabo en los sistemas de información están controlados y son revisados.

05 Anonimización de la BBDD

1200 €

Identificar y ocultar la información de carácter sensible de la BBDD.

06 Plan de gestión de incidentes

Proveer de procedimientos de gestión de incidentes acordes con la criticidad de sus actividades de negocio para garantizar el más rápido tratamiento.

07 Implementación de un servicio de monitorización

1600 €

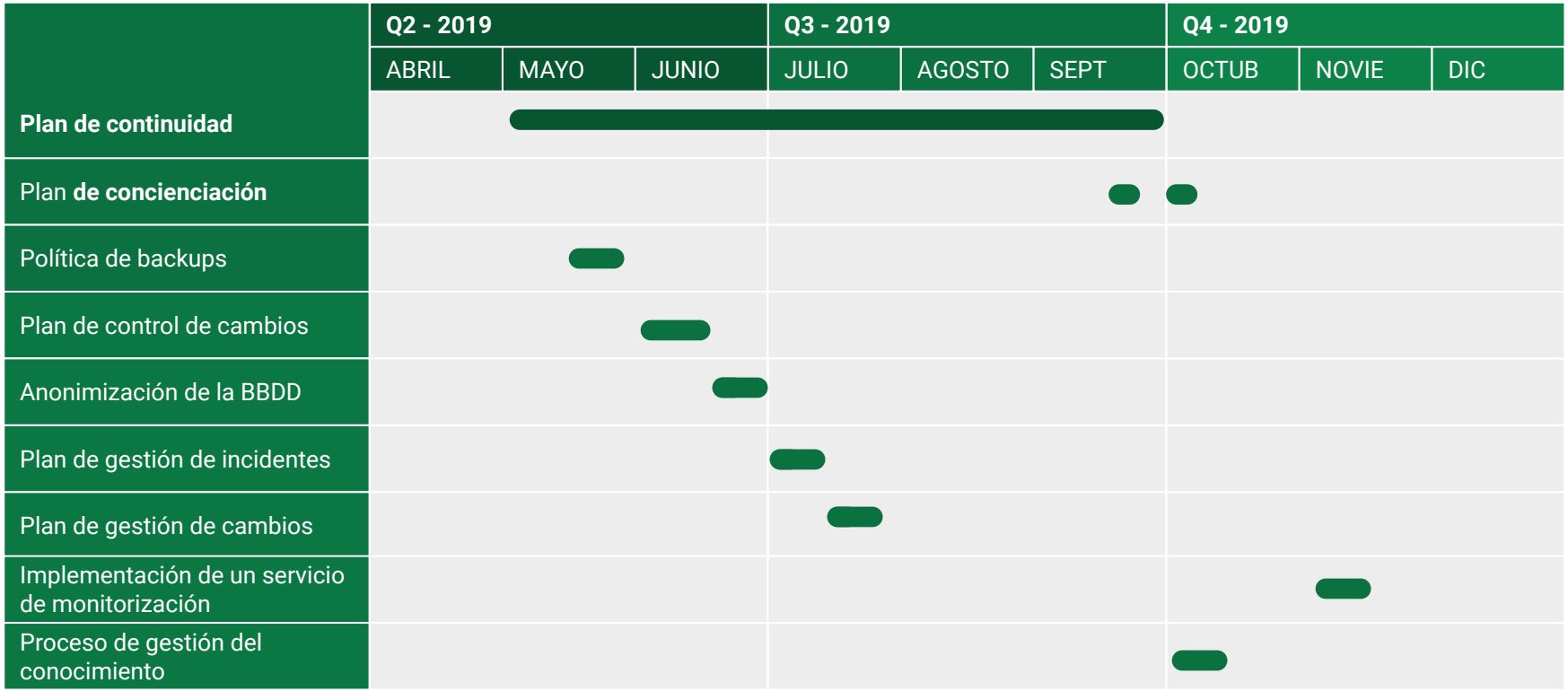
Verificar que los servidores web tienen las capacidades necesarias para prestar el servicio y detectar degradaciones del servicio.

08 Proceso de gestión del conocimiento

1200 €

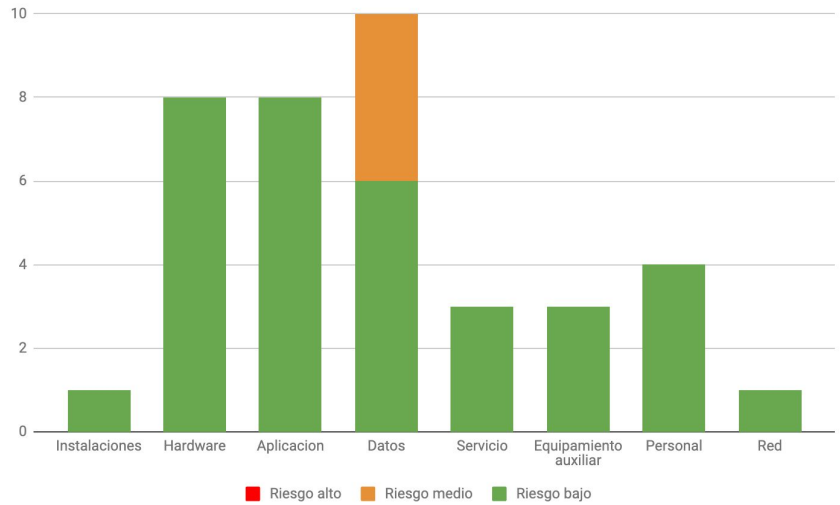
Retener y asegurar el conocimiento, entendiendo por conocimiento la capacidad de las personas de, en base a la información adquirida, tomar la decisión más adecuada para la organización.

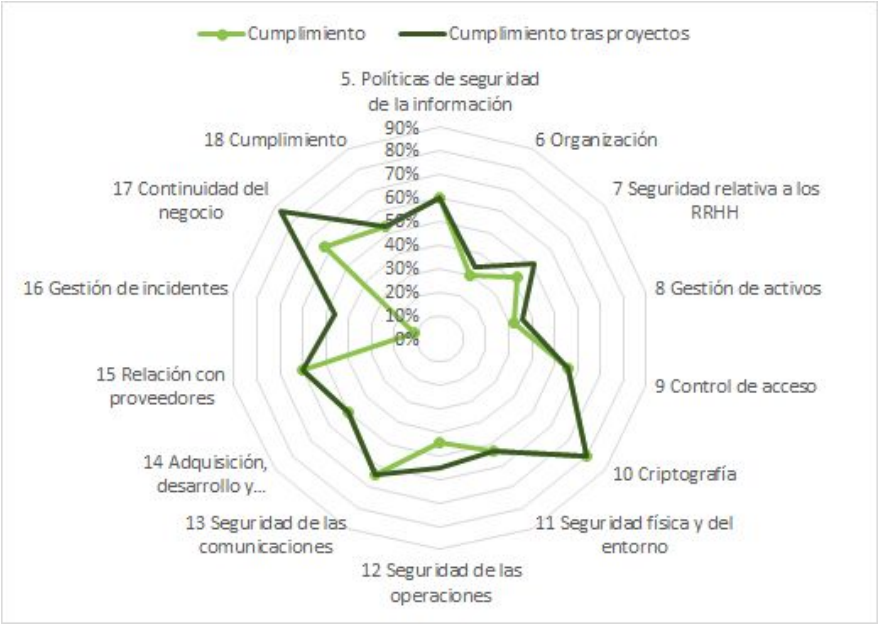
Fase 4: Planificación



Fase 4: Resultados

Riesgo después de la aplicación de proyectos

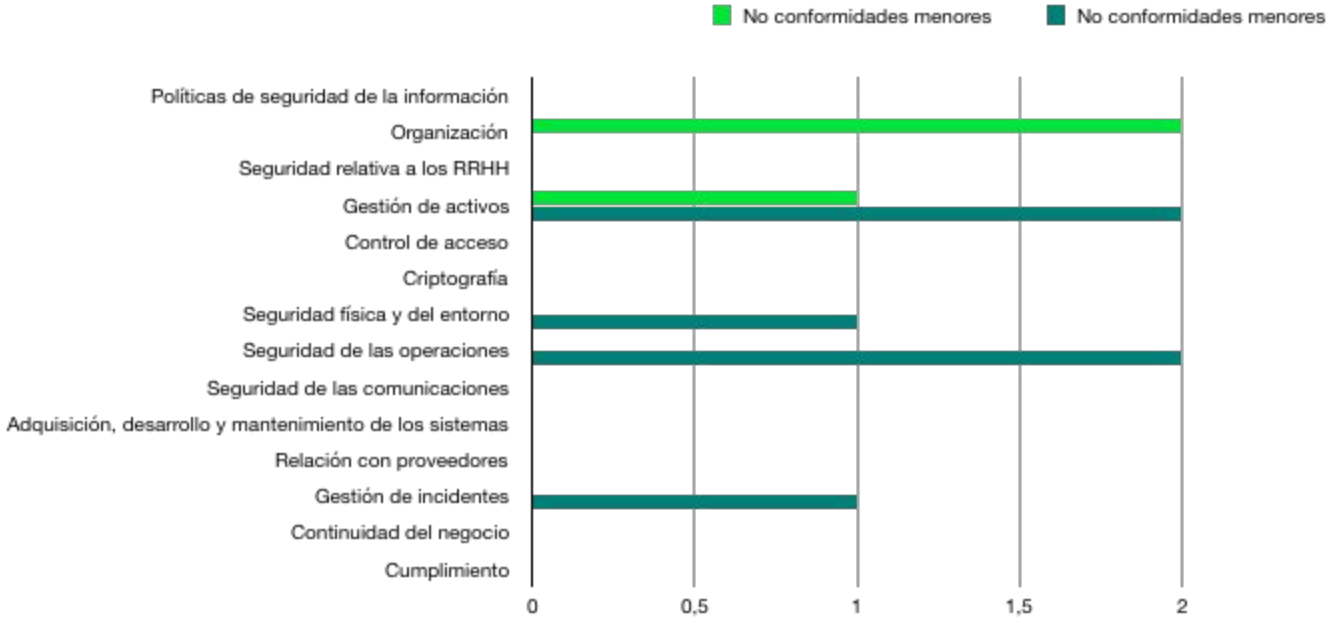




Fase 5: Auditoría de cumplimiento

05 Conclusiones - Auditoría de cumplimiento

- El 55% de los controles ha superado la auditoría contra la norma.
- El 15% de los controles ha presentado No Conformidades Mayores
- El 30% de los controles ha presentado No Conformidades Menores



05 Conclusiones

39

Activos identificados

8500 €

De inversión para la ejecución de los 8 proyectos propuestos

2

No conformidades mayores

12

Activos con riesgo alto de materialización de amenazas

50,9 %

Controles de la ISO 27002 con estado de madurez Reproducible tras la ejecución de los proyectos

4

No conformidades menores