Plan director de seguridad TrendTip

PRESENTACIÓN PARA EMPLEADOS

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:

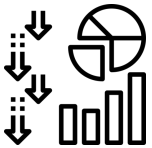
- Provee los niveles de seguridad requeridos por la organización

- 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

TrendTip

01. Fases del Plan Director de Seguridad

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5
				
Situación actual: Contextualización, Objetivos y Análisis Diferencial	**Sistema de Gestión documental**	**Análisis de riesgos**	**Propuesta de proyectos**	**Auditoría de cumplimiento**

TrendTip

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

TrendTip

Situación inicial: Contexto y Objetivos

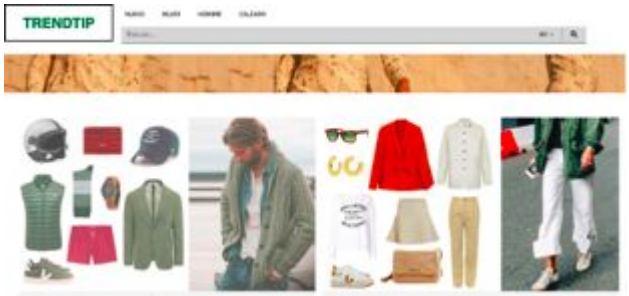
TrendTip es una empresa online de moda cuyo objetivo **es servir de escaparate a los pequeños comercios textiles y de calzado,** haciendo de intermediario entre éstos y sus potenciales compradores. Se trata de una **página web** donde se muestran las últimas tendencias de moda, mostrando looks completos en los que se mezcla prendas de distintos comercios. En ella, **el cliente tiene la opción de hacer clic en las distintas prendas elegidas y ser redirigido a la página web de empresa textil** elegida para poder efectuar la compra del producto.

El nuevo Plan Director de Seguridad tiene como objetivos:

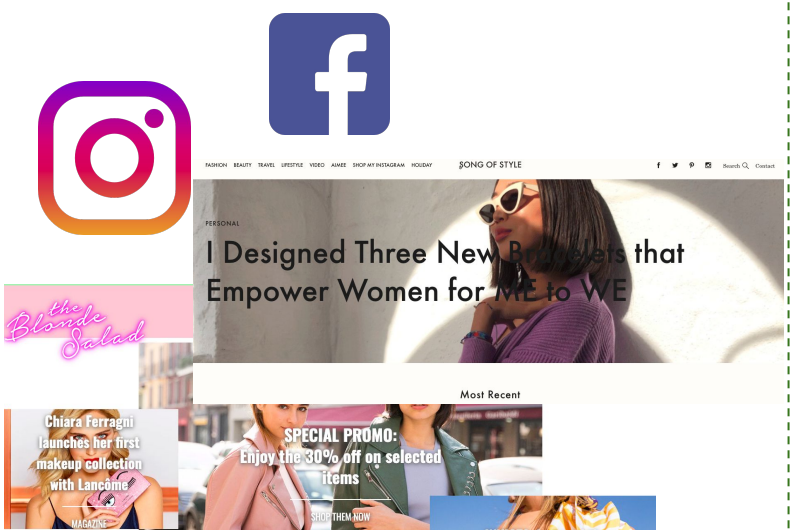
- Conseguir un mayor número de visitas y aumentar los beneficios económicos
- Ampliación del número de proveedores partners con los que trabaja

Situación inicial: Alcance

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

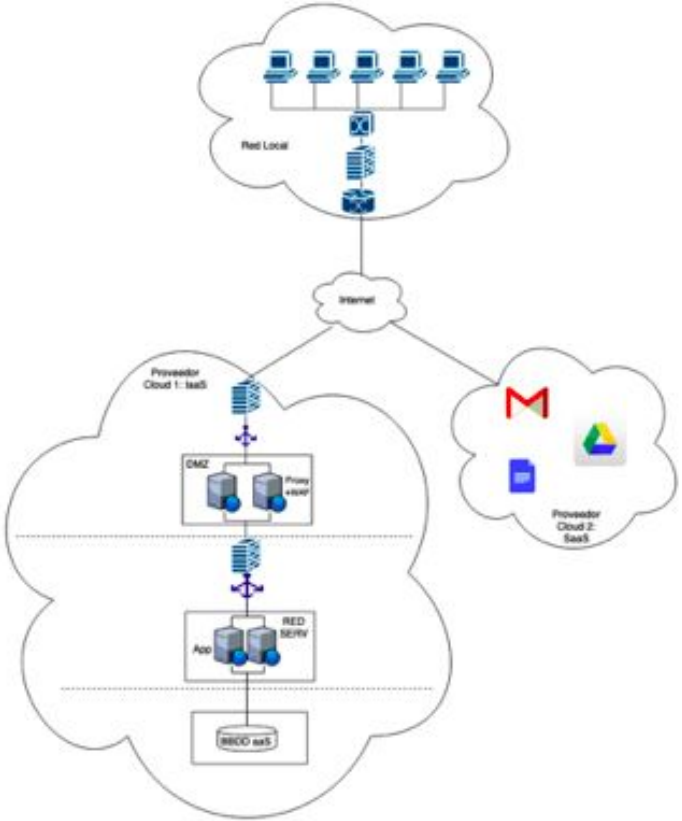


La búsqueda de tendencias y productos para su selección.



TrendTip

Situación inicial: Infraestructura



Para asegurar la máxima disponibilidad del servicio se ha contratado dos servicios en la nube:

- IaaS (Infraestructure as a Service): se han contratado dos servidores donde se aloja la página web de la empresa y la base de datos de los proveedores textiles. Se ha diseñado una arquitectura en 3 capas.
- SaaS (Software as a Service): se han contratado servicios en la nube (SaaS) de almacenamiento de documentos y ofimática para toda la gestión estratégica, de recursos humanos y del plan comercial de la empresa.

Situación inicial: Organización

TrendTip cuenta con alrededor de 4 empleados en la organización, su organigrama se muestra a continuación

CEO: fundador de la empresa y encargado de:

- Toma de decisiones estratégicas
- Gestión de Recursos Humanos
- Gestión de Recursos económicos.

Responsable IT:

- Administrador de sistemas
- Responsable de seguridad
- Analista funcional
- Arquitecto de sistemas

Responsable de ventas:

- Estudiar el mercado en busca de nuevas tendencias
- Negociar y contratar nuevos proveedores

Responsable de Marketing:

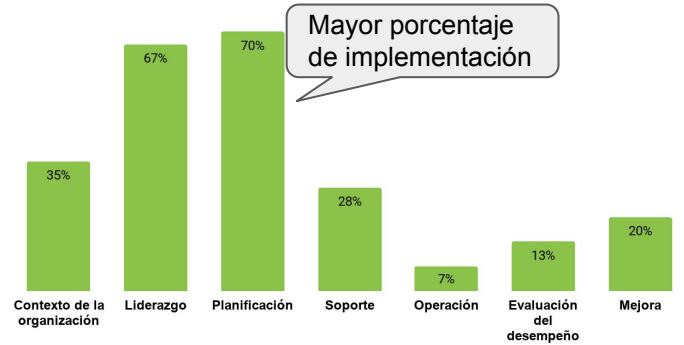
- Gestionar Redes sociales
- Gestionar acciones publicitarias.

Situación inicial: Análisis diferencial ISO 27001

Niveles de madurez

Porcentaje	Criterio	Descripción
0%	Inexistente	No existen controles de seguridad de la información establecidos.
20%	Realizado informalmente	Existen procedimientos para llevar a cabo ciertas acciones en determinado momento. Estas prácticas no se adoptaron formalmente y/o no se les hizo seguimiento y/o no se informaron adecuadamente.
40%	Planificado	Los controles de seguridad de la información establecidos son planificados, implementados y repetibles.
60%	Bien definido	Los controles de seguridad de la información además de planificados son documentados, aprobados e implementados en toda la organización.
80%	Cuantitativamente controlado	Los controles de seguridad de la información están sujetos a verificación para establecer su nivel de efectividad.
100%	Mejora continua	Los controles de seguridad de la información definidos son periódicamente revisados y actualizados. Estos reflejan una mejora al momento de evaluar el impacto.

Resultados análisis diferencial

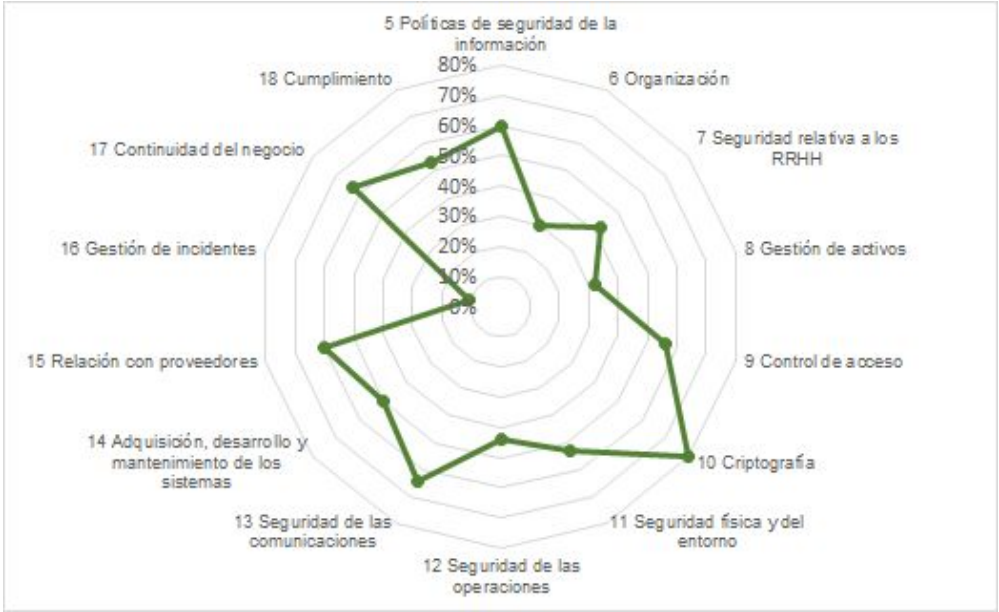


ISO/IEC 27001	Control	Cumplimiento
4	Contexto de la organización	35 %
5	Liderazgo	67 %
6	Planificación	70 %
7	Soporte	28 %
8	Operación	7 %
9	Evaluación de desempeño	13 %
10	Mejora	20 %

Situación inicial: Análisis diferencial ISO 27002

Resultados análisis diferencial ISO 27002

ISO/IEC 27002	Control ISO 27002	Cumplimiento
5	Políticas de seguridad de la información	**60 %**
6	Organización	**30 %**
7	Seguridad relativa a los RRHH	**42 %**
8	Gestión de activos	**32 %**
9	Control de acceso	**56 %**
10	Criptografía	**80 %**
11	Seguridad física y del entorno	**53 %**
12	Seguridad de las operaciones	**44 %**
13	Seguridad de las comunicaciones	**64 %**
14	Adquisición, desarrollo y mantenimiento de los sistemas	**50 %**
15	Relación con proveedores	**60 %**
16	Gestión de incidentes	**11 %**
17	Continuidad del negocio	**63 %**
18	Cumplimiento	**53 %**



TrendTip

Fase 2: Sistema de gestión documental

TrendTip

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.

TrendTip

Fase 3: Análisis de riesgos

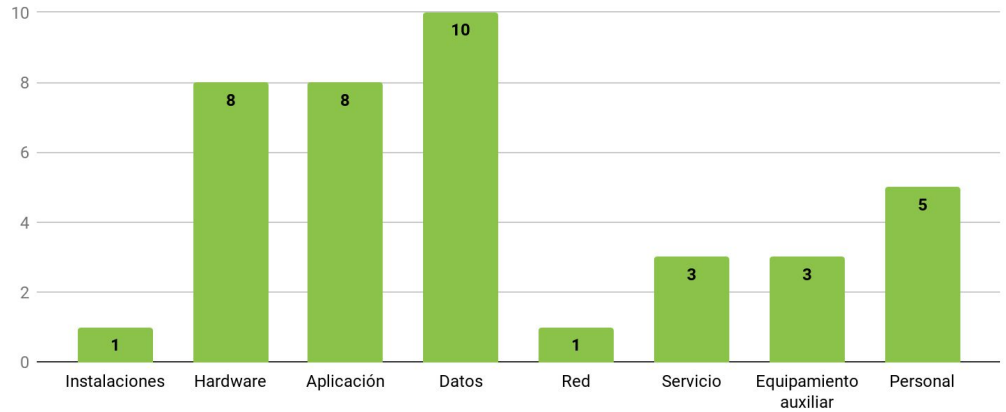
Fase 2: Análisis de riesgos

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.

Análisis de riesgos: Inventario de activos

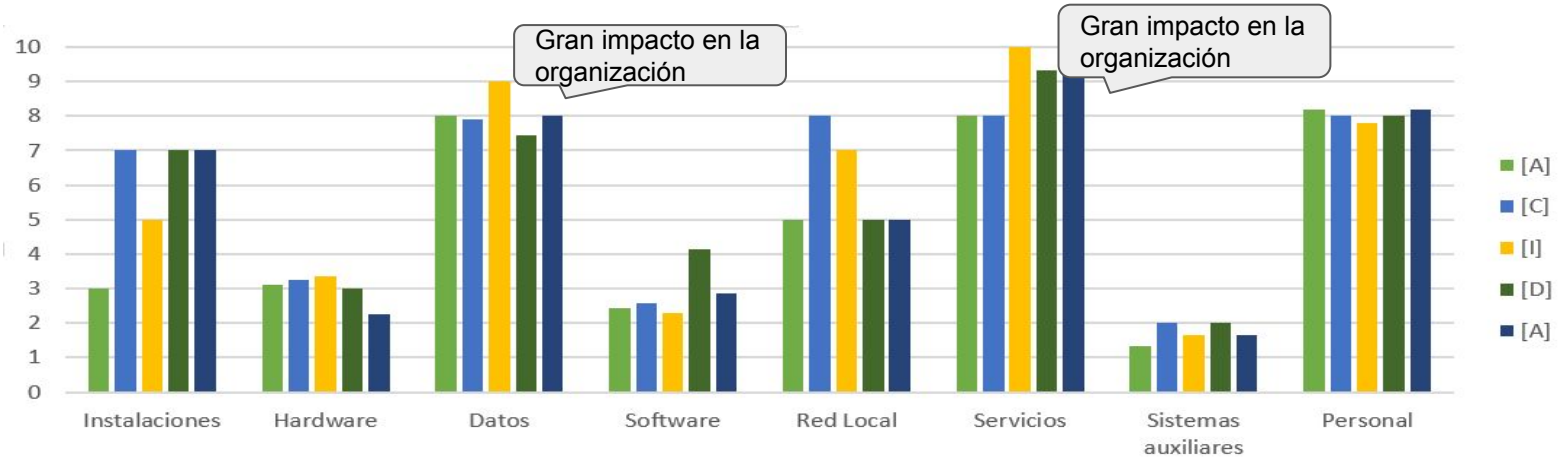
El inventario de activos se realiza siguiendo la metodología MAGERIT. Esta clasifica los activos en las siguientes categorías:

01 Instalaciones	**04 Datos**	**07 Equipamiento auxiliar**
02 Hardware	**05 Red**	**08 Personal**
03 Aplicación.	**06 Servicios.**	



Valoración de los activos

Se ha utilizado la metodología MAGERIT para la realizar la **valoración** de las Dimensiones de Seguridad: **Autenticidad, Confidencialidad, Integridad, Disponibilidad y Auditabilidad/Trazabilidad**



VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

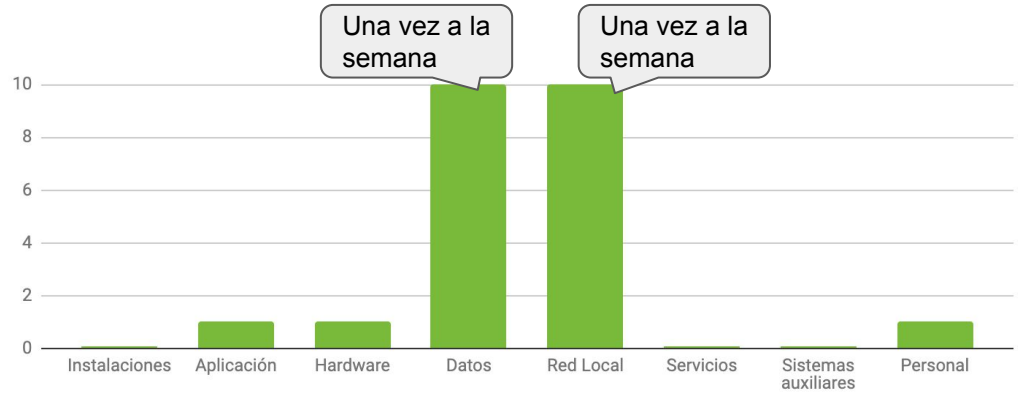
Frecuencia de las amenazas

Los activos están expuestos a amenazas y estas pueden afectar a los distintos aspectos de la seguridad. Según la metodología de MAGERIT, estas amenazas se dividen en:

- **Desastres naturales**
- **De origen industrial**
- **Errores y fallos no intencionados**
- **Ataques intencionados**

A continuación se muestra una gráfica con la frecuencia estimada de aparición de la amenaza por cada uno de los grupos de activos.

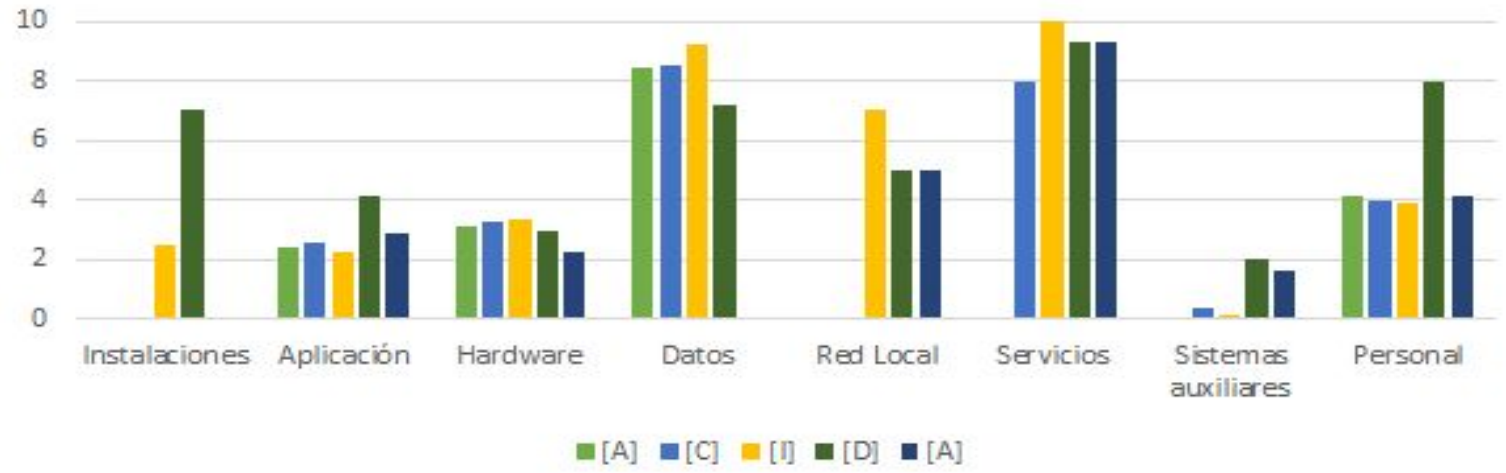
Frecuencia	Descripción	Valor
Muy alta	una vez al día	100
Alta	una vez a la semana	10
Media	una vez al mes	1
Baja	una vez al año	1/10
Muy baja	una vez cada 10 años	1/100



Impacto potencial

Podemos determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas. Así pues, definimos impacto potencial:

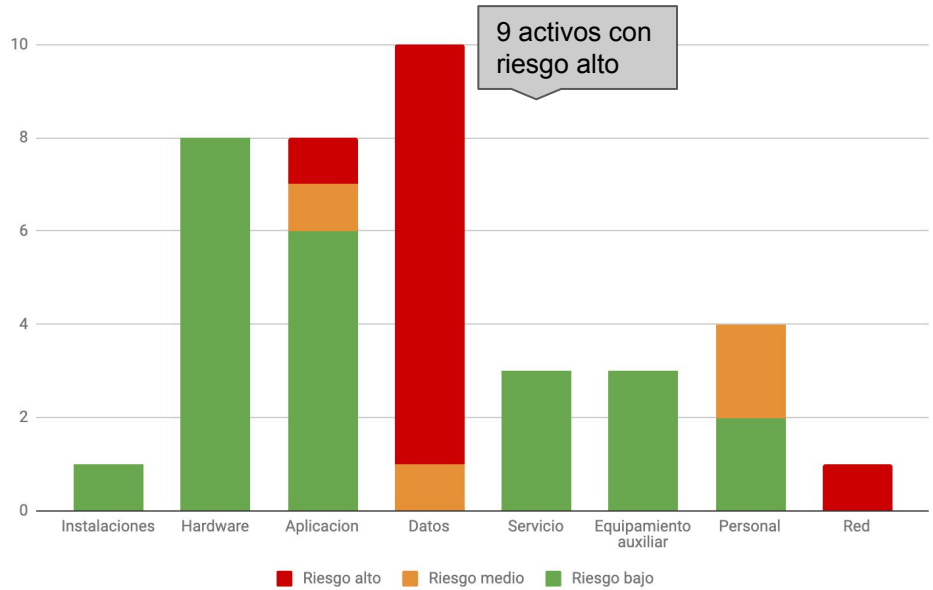
Impacto potencial = valor del activo * impacto materialización de la amenaza



Riesgo aceptable y riesgo residual

Definimos riesgo como la

Riesgo = Frecuencia materialización amenaza * Impacto Potencial



TrendTip

Fase 4: Propuesta de proyectos

TrendTip

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.

Proyectos propuestos: Plan de continuidad

Objetivo

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

Cuadro de Mando

Personal

Contratación de servicio externalizado

Presupuesto

3100€

Planificación

	Proyectos	Duración	Comienzo
PR1	**Plan de Continuidad del negocio**		06.05.19
Fase 1	BIA	2 días	06.05.19
Fase 2	Selección de estrategias	1 día	08.06.19
Fase 3	Definir y desarrollar el plan de continuidad	5 días	09.05.19
Fase 4	Pruebas que garanticen la efectividad	2 horas/prueba	01.06.19

Proyectos propuestos: Plan de concienciación

Objetivo

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

Cuadro de Mando

Personal

Contratación de servicio externalizado

Presupuesto

1200€

Planificación

	Proyectos	Duración	Comienzo	Septiembre 2019				
				9	10	11	12	13
PR1	**Programa de concienciación**	5 días	09.09.19					
Fase 1	Evaluación del nivel de concienciación	10 horas	09.09.19					
Fase 2	Presentación de los resultados de la evaluación	2 horas	10.09.19					
Fase 3	Distribución y redacción del material de seguridad	12 horas	11.09.19					

	Proyectos	Duración	Comienzo	2019											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
PR1	**Curso de concienciación**	2 horas	10.10.19												

Proyectos propuestos: Política de backups

Objetivo

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

Cuadro de Mando

Personal

Responsable IT

Presupuesto

No requiere de presupuesto adicional

Planificación

	Proyectos	Duración	Comienzo	Mayo 2019				
				20	21	22	12	13
PR1	Política de backup	5 días	20.05.19					

Proyectos propuestos: Plan de control de cambios

Objetivo

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

Cuadro de Mando

Personal

Responsable IT

Presupuesto

No requiere de presupuesto adicional

Planificación

	Proyectos	Duración	Comienzo	Junio				
				L	M	X	J	V
PR1	Procedimiento gestión de cambios	3 días	10.06.19					

Proyectos propuestos: Anonimización de la BBDD

Objetivo

Identificar y ocultar la información de carácter sensible de la BBDD

Cuadro de Mando

Personal

Contratación de servicio externalizado

Presupuesto

1200€

Planificación

	Proyectos	Duración	Comienzo	Junio 2019							
				17	18	19	20	21	24	25	26
	Anonimización BBDD	2 días	17.06.19								
Fase 1	Análisis de riesgos	16 horas	17.06.10								
	Evaluación y análisis de riesgos	16 horas	17.06.19								
Fase 2	Identificación usuarios potenciales de conocimiento	24 horas	19.06.19								
	Toma de requisitos	3 horas	19.06.19								
	Diseño solución	5 horas	19.06.19								
	Desarrollo de solución	10 horas	20.06.19								
	Implantación solución	6 horas	21.06.19								
Fase 3	Implementación de medidas de seguridad	24 horas	24.06.19								
	Implementación medidas	1 día	24.06.19								

Proyectos propuestos: Plan de gestión de incidentes

Objetivo

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

Cuadro de Mando

Personal

Responsable IT

Presupuesto

No requiere de presupuesto adicional

Planificación

	Proyectos	Duración	Comienzo	Julio				
				L	M	X	J	V
PR1	Plan de gestión de incidentes	3 días	22.07.19					

Proyectos propuestos: Servicio de monitorización

Objetivo

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

Cuadro de Mando

Personal

Contratación de servicio externalizado

Presupuesto

1600€

Planificación

	Proyectos	Duración	Comienzo	Julio 2019 L	M	X	J	V
	Implementación de servicio de monitorización	5 días	03.06.19					
Fase 1	Diseño de los planes de prueba	6 horas	03.06.19					
Fase 2	Implementación de las pruebas	10 horas	03.06.19					
Fase 3	Implementación de medidas de recolección de métricas	4 horas	03.06.19					
Fase 4	Integración con herramientas de monitorización	12 horas	04.06.19					

Proyectos propuestos: Gestión del conocimiento

Objetivo

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.

Cuadro de Mando

Personal

Contratación de servicio externalizado

Presupuesto

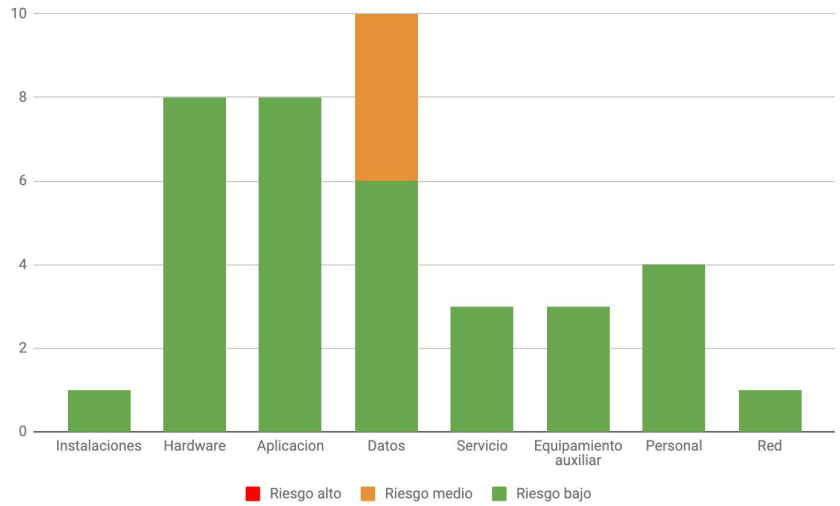
1200€

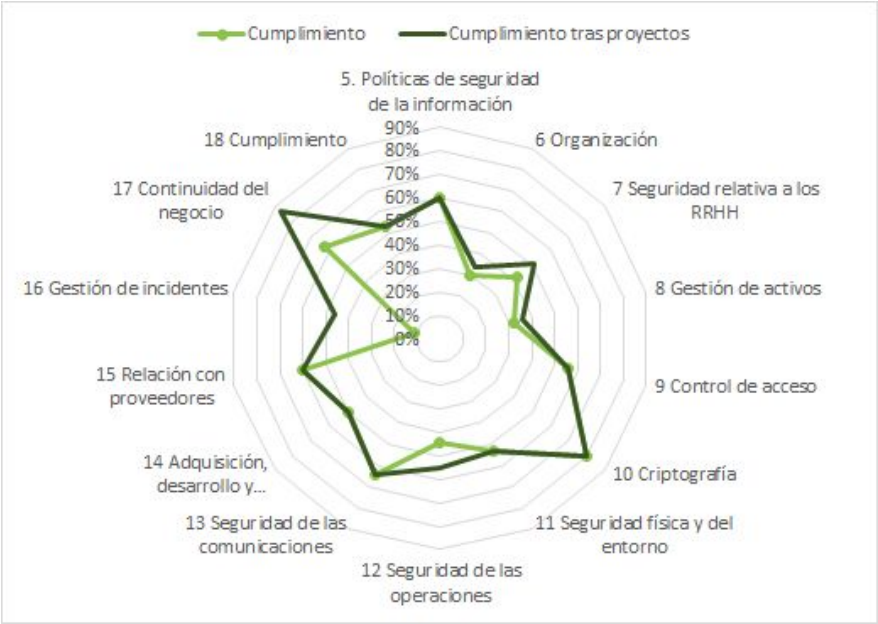
Planificación

	Proyectos	Duración	Comienzo	Octubre L	M	X	J	V
PR1	**Plan de gestión del conocimiento**	5 días	02.10.19					
Fase 1	Iniciación	1 día	02.10.19					
	Identificación procesos de negocio	3 horas	02.10.19					
	Identificación usuarios potenciales de conocimiento	3 horas	02.10.19					
	Identificación tecnología necesaria para ejecutar los procesos	2 horas	03.10.19					
Fase 2	Ejecución	3 días	03.10.19					
	Identificar los procesos que muestran brechas de conocimiento	6 horas	03.10.19					
	Documentar los procesos identificados	16 horas	03.10.19					
	Informar de los recursos de conocimiento disponibles	2 horas	05.10.19					
Fase 2	Finalización	1 día	06.10.19					
	Documentar las lecciones aprendidas	8 horas	06.10.19					

Fase 4: Resultados

Riesgo después de la aplicación de proyectos

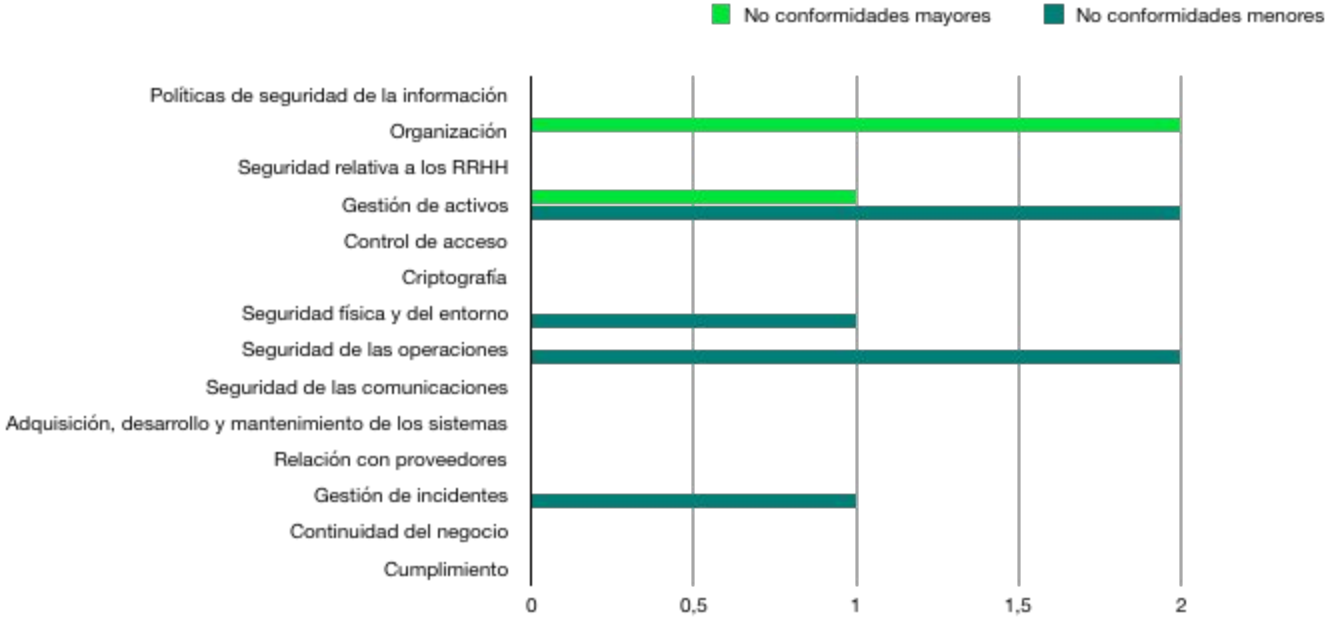




Fase 5: Auditoría de cumplimiento

05 Conclusiones - Auditoría de cumplimiento

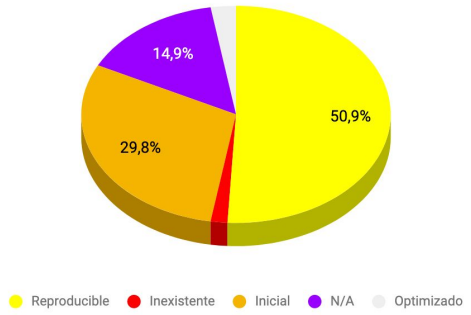
- El 55% de los controles ha superado la auditoría contra la norma.
- El 15% de los controles ha presentado No Conformidades Mayores
- El 30% de los controles ha presentado No Conformidades Menores



05 Nivel de madurez tras proyectos

Efectividad	CMM	CRITERIO
0-9%	L0	Inexistente
10%	L1	Inicial/Ad-hoc
50%	L2	Reproducible, pero intituitivo
90%	L3	Proceso definido
95%	L4	Gestionado y medible
100%	L5	Optimizado

Madurez CCM de los controles ISO



	Control ISO 27002	Nivel de madurez inicial	Nivel de madurez tras proyectos	
5.	Políticas de seguridad de la información	60 %	60 %	=
6	Organización	30 %	34 %	↑
7	Seguridad relativa a los RRHH	42 %	51 %	↑
8	Gestión de activos	32 %	36 %	↑
9	Control de acceso	56 %	56 %	=
10	Criptografía	80 %	80 %	=
11	Seguridad física y del entorno	53 %	53 %	=
12	Seguridad de las operaciones	44 %	55 %	↑
13	Seguridad de las comunicaciones	64 %	64 %	=
14	Adquisición, desarrollo y mantenimiento de los sistemas	50 %	60 %	↑
15	Relación con proveedores	60 %	60 %	=
16	Gestión de incidentes	11 %	46 %	↑
17	Continuidad del negocio	63 %	87 %	↑
18	Cumplimiento	53 %	53 %	=

TrendTip

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

05 Conclusiones

01 **Ampliación del alcance**

02 **Siguientes iteraciones del modelo de gestión**

03 **Impacto de una posible evolución del modelo de negocio de la empresa**