UOC
Universitat Oberta de Catalunya
www.uoc.edu

UAB
Universitat Autònoma de Barcelona

Universitat Rovira i Virgili

UIB
Universitat de les Illes Balears

Presentación Trabajo Fin de Máster

Proceso de adecuación de la seguridad de la Información en una pequeña empresa

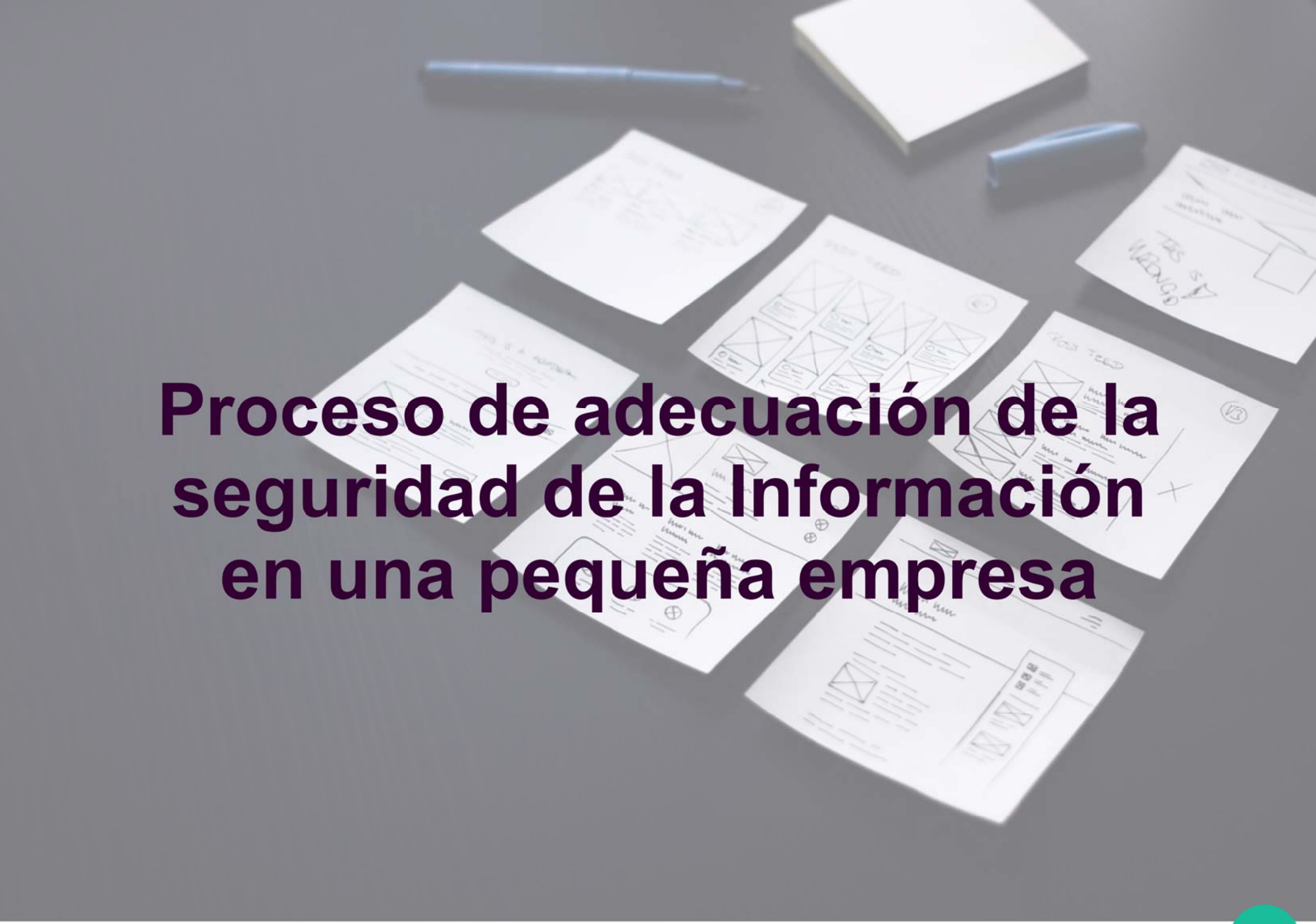
Nombre estudiante: José Sureda Uceda

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Nombre consultor: Arsenio Tortajada Gallego

Centro: Universitat Oberta de Catalunya

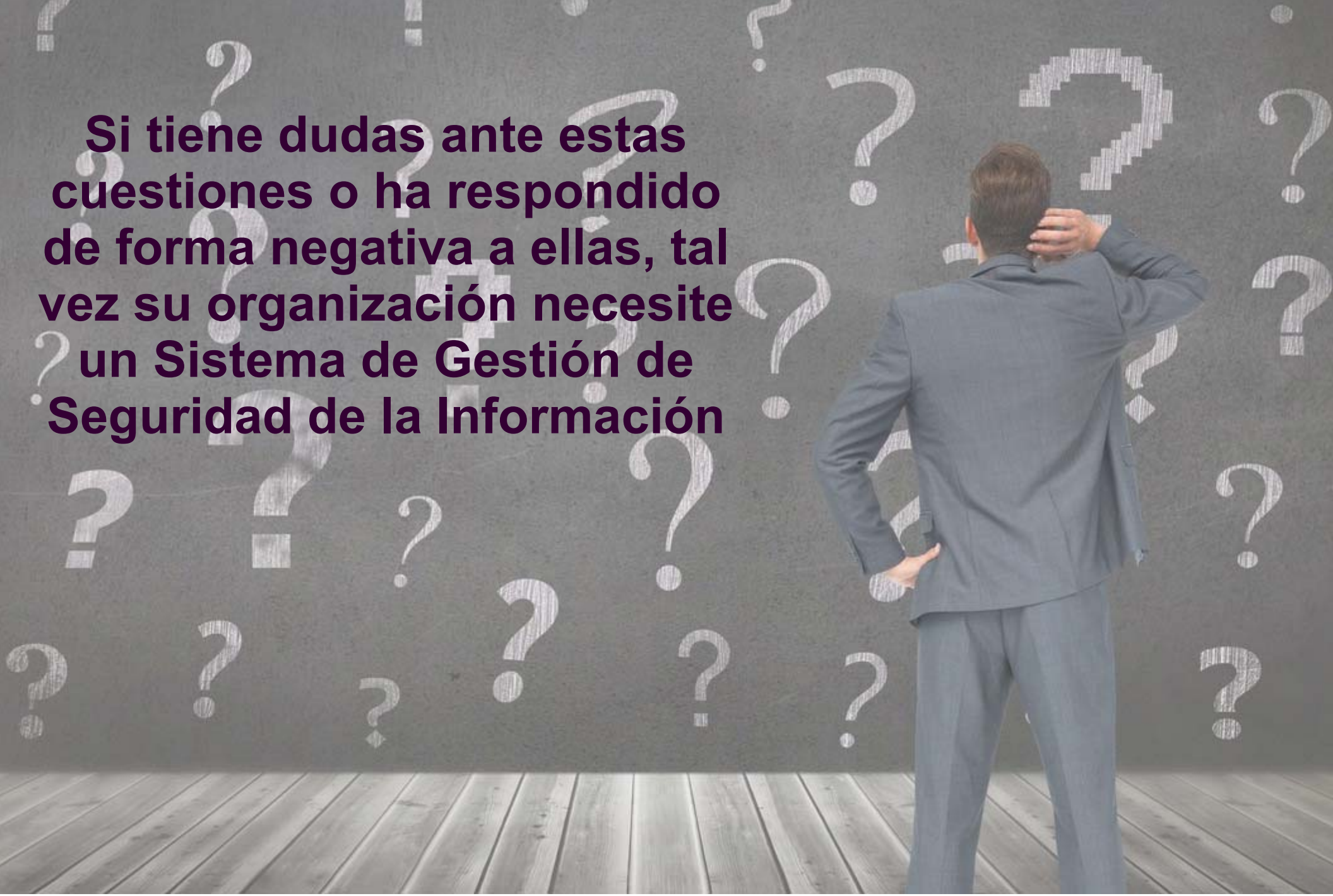
Fecha: diciembre 2019



Proceso de adecuación de la seguridad de la Información en una pequeña empresa

Si tiene una empresa o es autónomo plantéese las siguientes preguntas

[illegible]


Si tiene dudas ante estas cuestiones o ha respondido de forma negativa a ellas, tal vez su organización necesite un Sistema de Gestión de Seguridad de la Información

¿Qué es un Sistema de Gestión de Seguridad de la Información?

Son todas aquellas acciones relacionadas entre ellas que permiten conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información de una empresa u organización

Las empresas necesitan garantizar la disponibilidad, integridad y confidencialidad de su información

contexto y justificación del trabajo

Las microempresas y pequeñas empresas, al igual que las grandes, han incorporado el uso de las nuevas tecnologías con las que tratan grandes cantidades de información

Sin embargo diferentes estudios reflejan la siguiente situación:

- **Las microempresas españolas son las que menos invierten en ciberseguridad, con un 6,5% del presupuesto total destinado a las TIC**

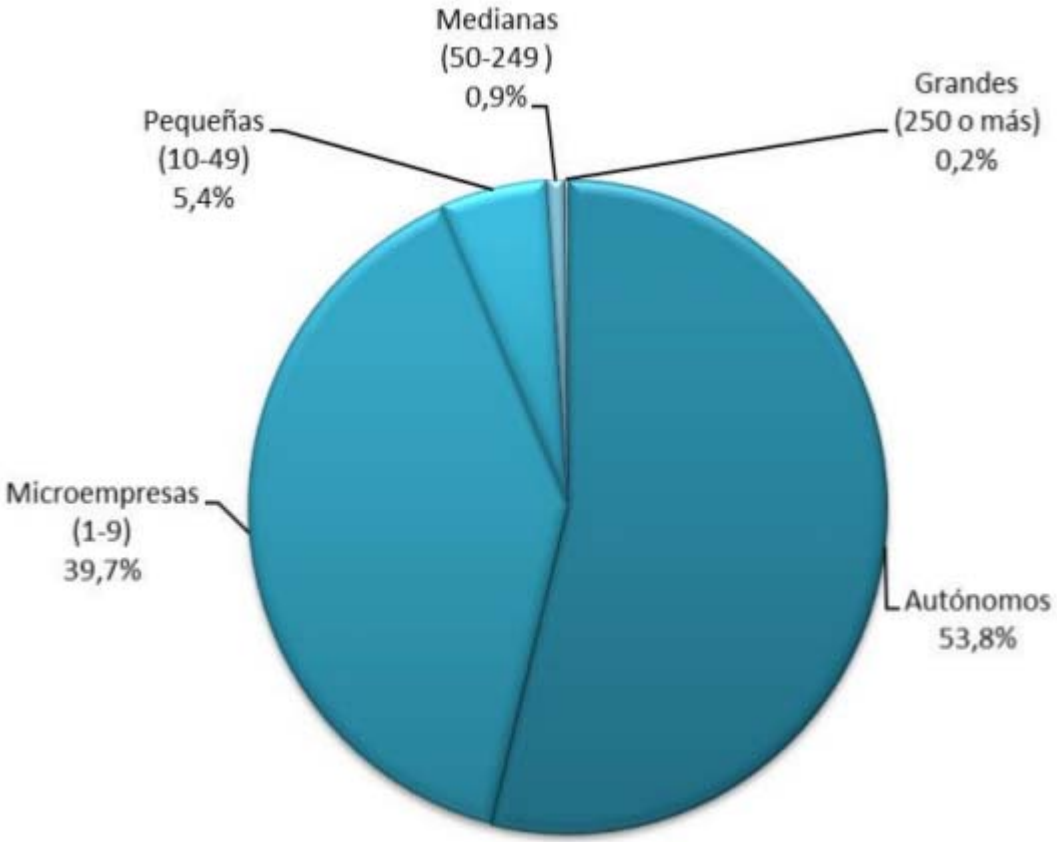
- **El 99,8% del tejido empresarial español no se considera un objetivo atractivo para un ciberataque**

- **Durante el año 2018, sólo en España se registraron al menos 120.000 incidentes de ciberseguridad, siendo las pequeñas y medianas empresas las más afectadas**

- **El impacto medio de un ataque oscila entre los 20.000 y los 50.000 euros**

Esta situación de fragilidad y escaso interés que existe en las pequeñas empresas en relación a la seguridad de su información, es lo que ha motivado el presente Proyecto Fin de Máster

Se pretende que el resultado final pueda ser un modelo o guía para que otras empresas similares puedan aplicarlo en su negocio



Viendo que las microempresas, pequeñas empresas y autónomos representan el 98,8% del total en España, supone un mercado amplio en el que trabajar

Para que el proyecto pueda ser una muestra aplicable en otras empresas se ha llevado a cabo en un entorno real

Objetivos generales del Proyecto

- **Transmitir la importancia de conocer cual es el estado de protección de la seguridad de la información en relación a los estándares y la normativa legal vigente**

- **Concienciar a las microempresas y pequeñas empresas para que integren la seguridad de la información en su modelo de negocio**

- **Educar sobre los beneficios que puede aportar la implantación de un Sistema de Gestión de Seguridad de la Información**

Objetivos específicos del Proyecto

- **Describir el estado inicial de la empresa TurisTech Balear (nombre ficticio) en relación a la seguridad de la información**
- **Crear la documentación requerida en un SGSI**
- **Implantar una metodología para la gestión de los riesgos**
- **Definir los proyectos para adecuar el estado inicial a los niveles definidos en el Plan Director**
- **Definir un plan de auditorías internas**

Enfoque y método seguido

La estrategia acordada consiste en implantar un Sistema de Gestión de Seguridad de la Información...

...y para ello es necesario diseñar un Plan Director de Seguridad

El conjunto de objetivos, proyectos y actividades a partir de un análisis detallado de las necesidades de la organización en materia de seguridad de la información, se conoce como Plan Director de Seguridad.

La implantación del SGSI se ha fundamentado en los siguientes elementos:

- Estándar ISO/IEC 27001
- Estándar ISO/IEC 27002
- Método MAGERIT
- Metodología PDCA
- Modelo de Madurez de la Capacidad (CMM)

El proyecto se ejecutará en 6 fases:

- Fase 1. Situación actual
- Fase 2. Sistema de gestión documental
- Fase 3. Análisis de riesgos
- Fase 4. Propuesta de proyectos
- Fase 5. Auditoría de cumplimiento
- Fase 6. Presentación de resultados

- Fase 1 -
Situación inicial de TurisTech Balear

Para realizar la valoración se ha usado la norma ISO/IEC 27002 y el Modelo de Madurez de la Capacidad (CMM)

Efectividad	CMM	Significado	Descripción
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocido. No se ha reconocido que exista ningún problema a resolver.
10%	L1	Inicial	Estado inicial donde el éxito de las actividades de los procesos se basa la mayor parte de las veces en un esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas en nivel corporativo.
50%	L2	Repetible, pero intuitivo	Los procesos similares se llevan a cabo de manera similar por diferentes personas con la misma tarea. Se normalizan las "buenas practicas" en base a la experiencia y al método. No hay comunicación o capacitación formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante capacitación.
95%	L4	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, existen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

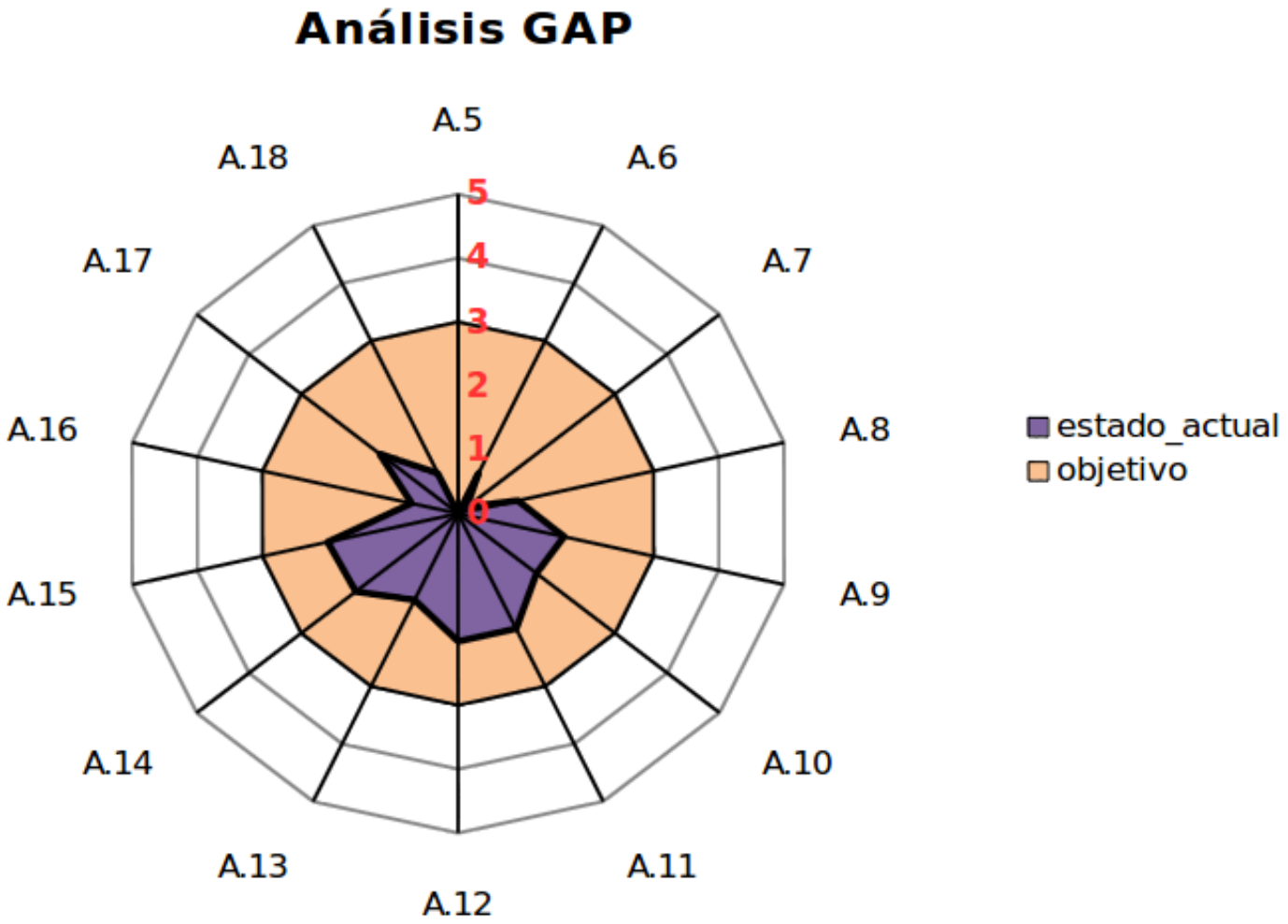
- **El análisis consiste en verificar el grado de cumplimiento de los controles de la norma 27002 incluidos en el alcance del SGSI**

- **Para ello se asigna a cada control el nivel CMM en el que se encuentra**

CONTROL			Evaluación	Valor	Total
le seguridad de la información					0,0%
A.5.1 Directrices de gestión de la seguridad de la información					0,0%
	A.5.1.1	Políticas para la seguridad de la información	0 - No existente	0	0,0%
	A.5.1.2	Revisión de las políticas para la seguridad de la información	0 - No existente	0	0,0%
ión de la seguridad de la información					14,5%

- **El objetivo de la empresa es situarse en un nivel L3 CMM**

El análisis GAP muestra la diferencia entre la situación actual y el punto objetivo



- Fase 2 -
Sistema de Gestión Documental

La gestión documental es un aspecto fundamental para la conformidad con la norma ISO/IEC 27001

Se basa en una pirámide jerárquica de documentos, que indica como se organizan

TurisTech Balear a obtenido la siguiente documentación:

- Fase 3 -
Análisis de Riesgos

Mediante el análisis de riesgos se ha obtenido la siguiente información:

- Inventario de activos de información
- Valoración de los activos
- Identificación de las amenazas
- El impacto de las amenazas
- Determinar el nivel de riesgo aceptable
- Identificar los activos que superan el nivel de riesgo aceptable

- Fase 4 -
Propuestas de proyectos

En esta fase se realiza una propuesta de proyectos a corto, medio y largo plazo

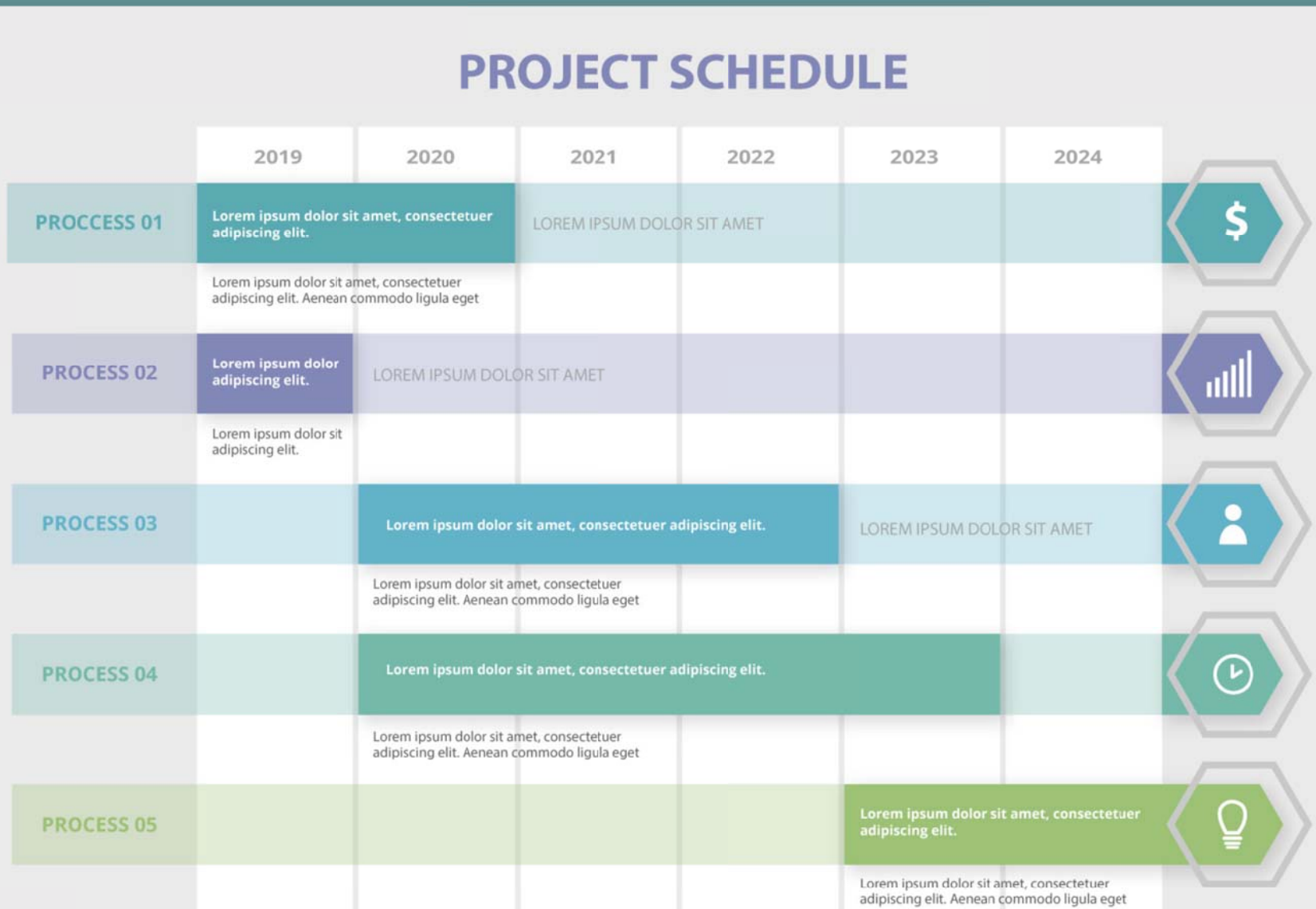
Los objetivos son:

- Redecir el riesgo de los activos que superan el umbral establecido
- Mejorar el cumplimiento de las áreas situadas por debajo del nivel L3 CMM

Estas mejoras favorecerán la seguridad de la información de la empresa a nivel global

Los criterios usados para planificar los proyectos son:

- Resultado del análisis diferencial inicial
- Nivel de riesgo obtenido en el AARR
- Coste económico
- Recursos necesarios



Los proyectos se ejecutarán en un plazo de 3 años de forma secuencial

Propuestas anuales

PROYECTOS A CORTO PLAZO - AÑO 2020				
Proyecto	**Duración**	**Inicio**	**Fin**	**Coste**
Organización interna de la seguridad de la información y el teletrabajo	1 mes	07/01/2020	07/02/2020	1.000 €
Plan de gestión de activos	2 meses	10/02/2020	10/04/2020	2.000 €
Plan de continuidad de los servicios MBE y MBE-CM	3 meses	10/04/2020	10/07/2020	5.400 €
Revisión del cumplimiento de LOPDGDD	1 mes	13/07/2020	13/08/2020	1.800 €
Gestión de incidentes de seguridad de la información	3 meses	07/09/2020	07/12/2020	3.000 €
			Total	**13.200 €**

Propuestas anuales

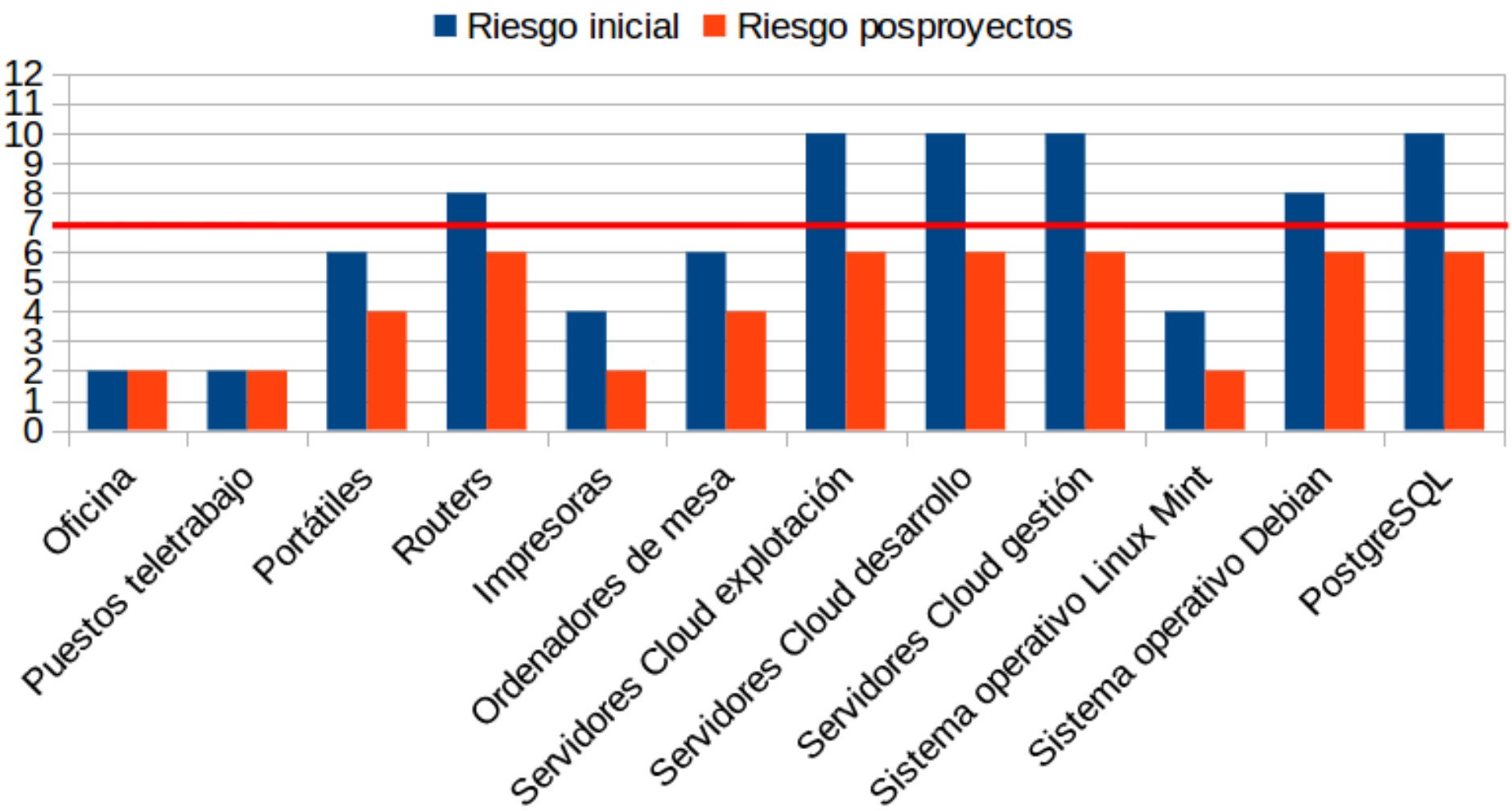
PROYECTOS A MEDIO PLAZO - AÑO 2021				
Proyecto	**Duración**	**Inicio**	**Fin**	**Coste**
Gestión de seguridad en las comunicaciones	10 días	11/01/2021	29/01/2021	750 €
Plan de gestión de accesos	2 meses	01/02/2021	10/04/2020	2.000 €
Plan de formación y concienciazión en materia de seguridad de la información	3 meses	05/04/2021	30/06/2021	2.400 €
Plan de mejora del sistema de monitorización y registros de eventos	1 mes	01/07/2021	30/07/2021	1.500 €
Plan de cumplimiento normativa PCI DSS SAQ A-EP	3 meses	01/09/2021	01/12/2021	3.000 €
			Total	**9.650 €**

Propuestas anuales

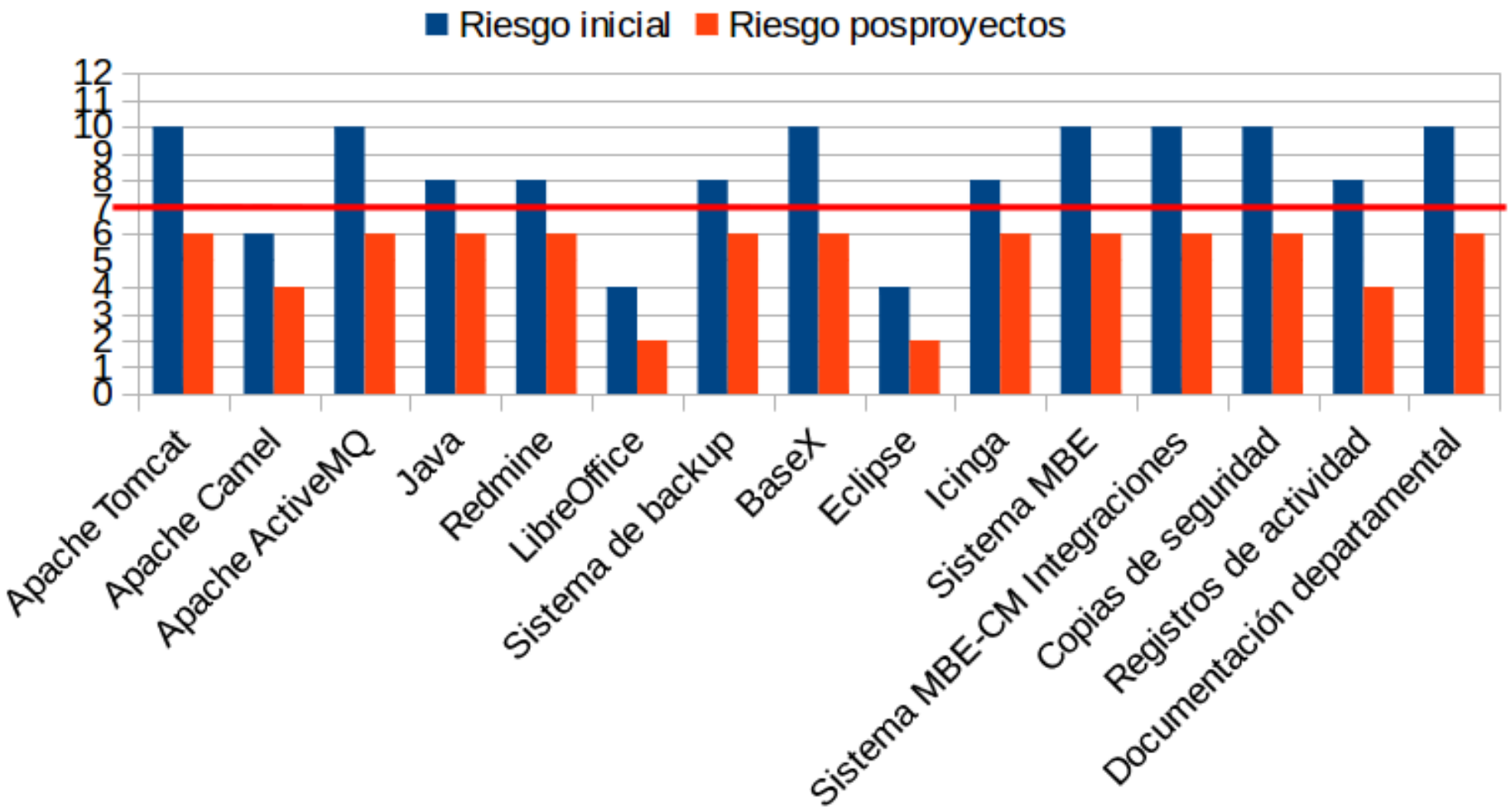
PROYECTOS A LARGO PLAZO - AÑO 2022				
Proyecto	**Duración**	**Inicio**	**Fin**	**Coste**
Plan de mejora de los sistemas criptográficos	1 mes	09/01/2022	09/02/2022	1.500 €
Procedimiento de gestión de altas y bajas de personal	1 mes	14/02/2022	14/03/2022	1.000 €
			Total	**2.500 €**

Resultados posproyectos

Evolución del riesgo



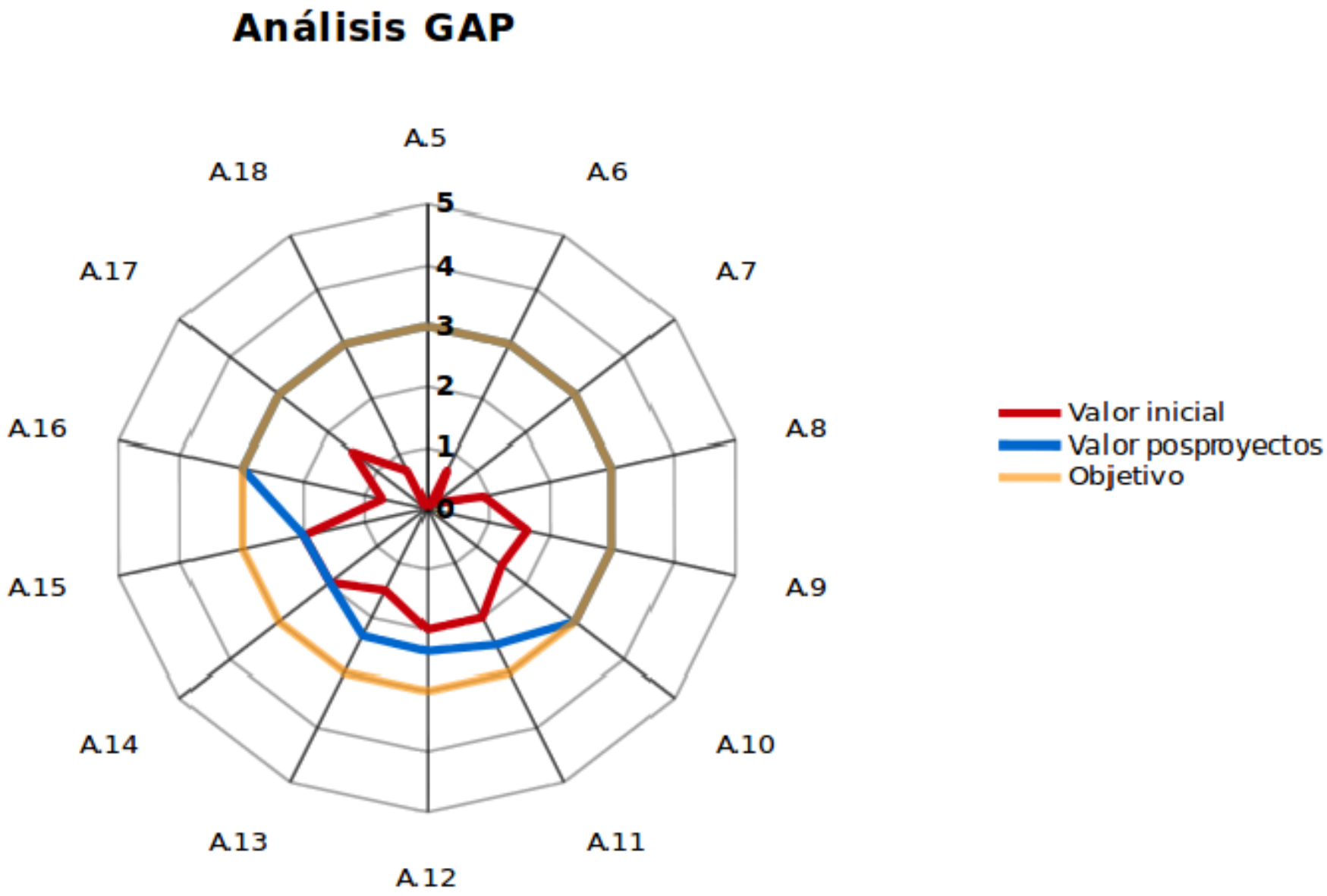
Evolución del riesgo



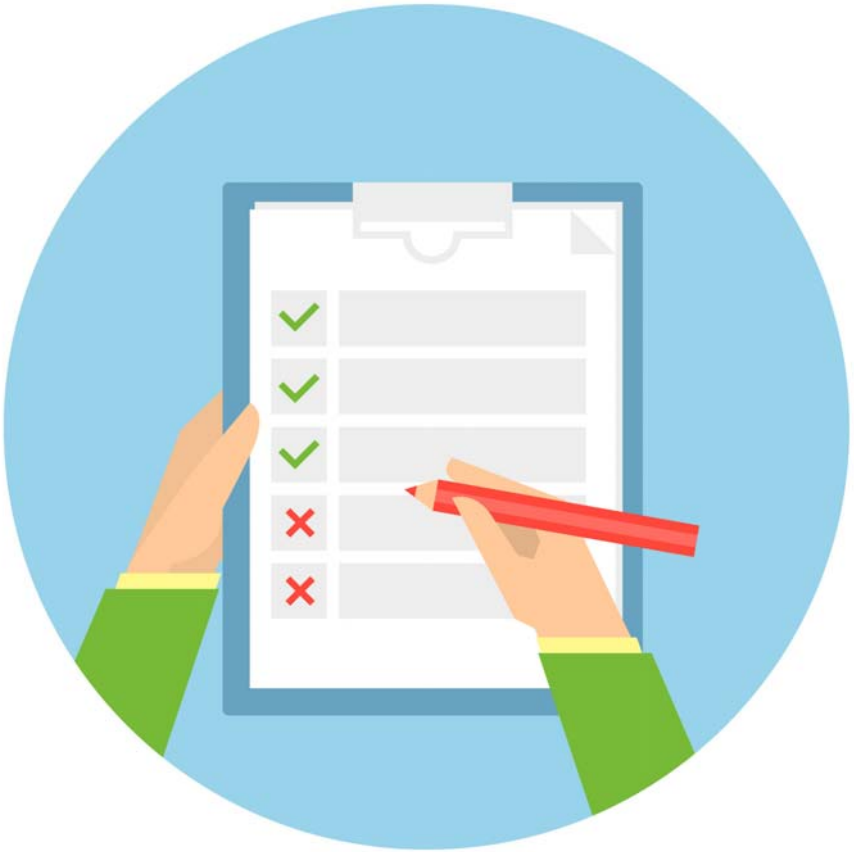
Cumplimiento ISO/IEC 27002

Capítulo	Valoración inicial	Valoración posproyectos
5 Políticas de seguridad de la información	0 %	90 %
6 Organización de la seguridad de la información	14,5 %	90 %
7 Seguridad relativa a los recursos humanos	1,7 %	90 %
8 Gestión de activos	16,7 %	90 %
9 Control de acceso	38 %	90 %
10 Criptografía	30 %	90 %
11 Seguridad física y del entorno	50 %	70 %
12 Seguridad de las operaciones	55,4 %	68,57 %
13 Seguridad de las comunicaciones	37,5 %	67,1 %
14 Adquisición, desarrollo y mantenimiento de los sistemas de información	48,3 %	48,3 %
15 Relación con proveedores	50 %	50 %
16 Gestión de incidentes de seguridad de la información	7,1 %	90 %
17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	30 %	90 %
18 Cumplimiento	13 %	90 %

Cumplimiento ISO/IEC 27002



- Fase 5 -
Auditoria de cumplimiento



Método para comprobar y valorar si el SGSI está conforme a la normativa de referencia

Las auditorias están integradas en el método PDCA o Ciclo de Deming

Esto permite analizar como evoluciona el SGSI y detectar anomalías

Los objetivos principales son:

- **Evaluar la efectividad de los controles, políticas, normas y procedimientos**
- **Verificar que la gestión de los riesgos se realiza correctamente**
- **Detectar No Conformidades en el SGSI y proponer recomendaciones de mejora**

Plan de Auditoria ejecutado

01/04/2022 – Reunión inicial y recogida de documentación.

04/04/2022 al 22/04/2022 – Auditoria documental.

25/04/2022 al 29/04/2022 – Auditoria *in situ*:

Fecha	Auditoría *in situ*	Objeto de auditoria	Representantes de la entidad
25/04/2022	Instalaciones del auditado	Departamentos de Dirección y Administración	La Dirección y el responsable de Administración
26/04/2022	Instalaciones del auditado	Departamento Comercial y Recursos Humanos	Responsable de RRHH y del dpto. Comercial
27/04/2022	Instalaciones del auditado	Departamento TIC	Responsable del dpto. TIC y sus trabajadores
28/04/2022	Puestos de teletrabajo	Departamento TIC	Trabajadores afectados
29/04/2022	Puestos de teletrabajo	Departamento TIC	Trabajadores afectados

Resultado de la Auditoria

Resultado	Encontradas	Plazo de corrección
No Conformidades Mayores	4	Entre 1 y 3 meses
No Conformidades Menores	2	6 meses
Observaciones	3	1 año

Conclusiones de la Auditoría

Se incumplen ciertas políticas internas y algunos controles de la norma ISO/IEC 27002:2013. Por lo que es necesario aplicar las medidas correctivas recomendadas en el informe de Auditoría

- Fase 6 -
Presentación de resultados y conclusiones del Proyecto

Con esta presentación y la entrega de los informes a la Dirección se llega al final del camino de este Proyecto

Puntos clave en la implantación del SGSI:

- La participación de la Dirección
- Identificar y valorar correctamente los riesgos en el AARR
- Escoger la metodología para la gestión de riesgos adecuada a la empresa
- Establecer metas alcanzables en el Plan Director de Seguridad
- Las auditorías son imprescindibles para la mejora contínua del SGSI

Conclusiones del Proyecto:

- **Los objetivos generales y la planificación de las fases han sido completadas de forma satisfactoria**
- **El nivel de madurez del sistema de gestión de la seguridad ha mejorado de forma sustancial**
- **TurisTech Balear a conseguido establecer una cultura de la seguridad en toda la organización**

- **Ahora es un empresa menos vulnerable ante los riesgos que amenazan sus activos de información**

- **Lo incidentes son inevitables al 100%, pero en caso de producirse hay más capacidad de reacción**

- **La imagen externa de la empresa se ha visto mejorada, es más profesional y aporta más confianza a sus clientes**

Líneas futuras:

- **Definir un nuevo Plan Director de Seguridad para los controles ISO/IEC 27002 que no han alcanzado el nivel L3 CMM.**

- **Analizar si seguir usando MAGERIT o buscar otras metodologías para el AARR**

- **Desarrollar nuevos servicios a entidades públicas. Certificación ENS y ENI**

GRACIAS

Imágenes de distribución libre recogidas de la fuente:

"https://www.freepik.es/fotos-vectores-gratis/fondo"

Autores de las fotos de fondo:
Senivpetro, Freepik, jcomp, Blossomstar, tirachardz, Creativeart, v.ivash, mindandi, Pressfoto, studiogstock,