Máster Universitario en Ciberseguridad y Privacidad (MUCIP)

RESUMEN EJECUTIVO

Universitat Oberta de Catalunya

Natividad García Lacárcel

INDICE

1. INTRODUCCIÓN 4
2. OBJETIVOS 4
3. ALCANCE 4
4. RESULTADOS
    4.1 ANÁLISIS DIFERENCIAL 5
    4.2 SISTEMA DE GESTIÓN DOCUMENTAL 7
    4.3 ANÁLISIS DE RIESGOS 8
    4.4 PROPUESTA DE PROYECTOS 9
    4.5 AUDITORÍA DE CUMPLIMIENTO 9
    5. CONCLUSIONES 11

1. INTRODUCCIÓN

La información junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una empresa. Las organizaciones y sus sistemas están expuestos a un gran número de amenazas, que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. Se trata de los tres pilares básicos de la seguridad de la información y sin los cuales no existe nada seguro.

Con la finalidad de proteger adecuadamente la información, se evalúa el estado actual de los procesos relacionados con la seguridad, clasificando y valorando los activos, elaborando un análisis de los riesgos e identificando las amenazas, así como los proyectos que será necesario llevar a cabo para conseguir el estado al que la organización quiere llegar.

2. OBJETIVOS

Los objetivos principales del **Plan Director de Seguridad de la Información** serán los siguientes:

- Involucrar a la alta dirección en el desarrollo e implantación del SGSI. Así como a toda la organización en conjunto para garantizar una correcta ejecución del SGSI.
- Establecer los canales adecuados para poder garantizar la seguridad de la información en todas las fases.
- Generar confianza a la dirección, trabajadores, empresas externas en los sistemas de información.
- Asegurar la confidencialidad, seguridad y correcto uso de los sistemas de la organización.
- Evaluar el nivel de cumplimiento, por medio del análisis diferencial respecto a las normas estándar ISO/IEC 27001 e ISO/IEC 27002.
- Detectar y valorar los riesgos; priorizándolos para implantar los controles que se consideren adecuados.
- Efectuar seguimiento sobre las propuestas y mejoras realizadas.
- Asegurar el cumplimiento de la legislación aplicable.

3. ALCANCE

El alcance del proyecto incluye la totalidad de los procesos y tratamientos de la información que se efectúa en la empresa. Afectará a todo el sistema, las instalaciones y el personal, así como a la información que pueda procesarse en la empresa, tanto si pertenece a ella como a terceros.

Por lo tanto, en este proceso se procurará la gestión de la seguridad en todos los niveles y capas de la organización. Procurando alinear los objetivos de seguridad con el negocio. Implicando a la alta dirección y procurando la concienciación del personal para que efectuar un correcto tratamiento de la información. Incluyendo la gestión de la seguridad tanto de los soportes físicos como lógicos de la seguridad. Así como el acceso a la información de forma remota o localmente.

4. RESULTADOS

4.1 ANÁLISIS DIFERENCIAL

En este apartado se realizará un análisis diferencial de las medidas de seguridad y la normativa de la organización en relación a la Seguridad de la Información para establecer su estado antes de iniciar las acciones de implementación del SGSI. Será el punto de partida para determinar la situación de la organización y de esta manera poder valorar los avances que a lo largo del proyecto se realicen.

El análisis diferencial se realizará con respecto la norma ISO/IEC 27001 y las mejores prácticas descritas en ISO/IEC 27002, y nos permitirá evaluar la capacidad actual y realizar las recomendaciones y oportunidades de mejora.

El análisis se ha efectuado empleando para la valoración CMM

	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "best practice", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporciona mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "ad hoc" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

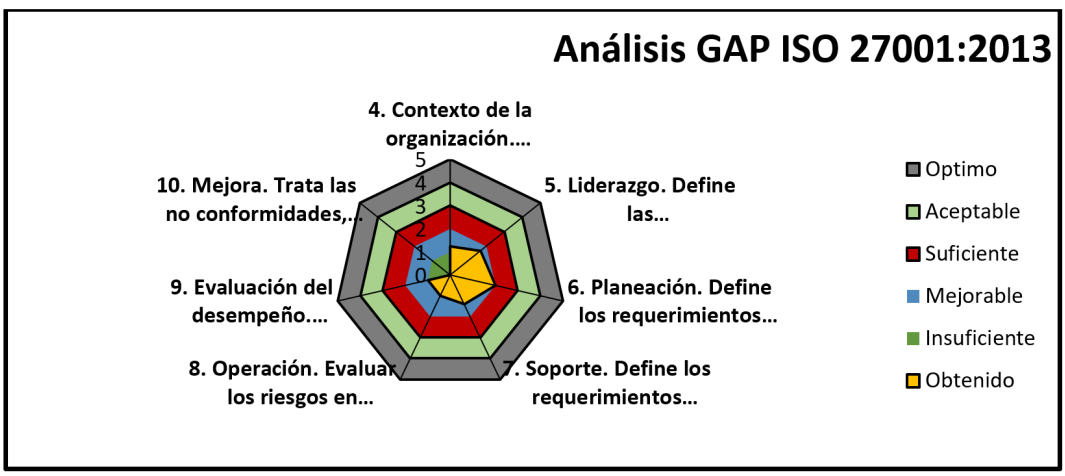
El nivel de cumplimiento de cada uno de los controles con el siguiente baremo:

MENOR 1.65	NO CUMPLE
ENTRE 1.66 Y 3.25	CUMPLE PARCIALMENTE
MAYOR 3.26	CUMPLE REQUISITOS NORMA

En la siguiente tabla se muestra el nivel de madurez de la norma ISO/IEC-27001:2013

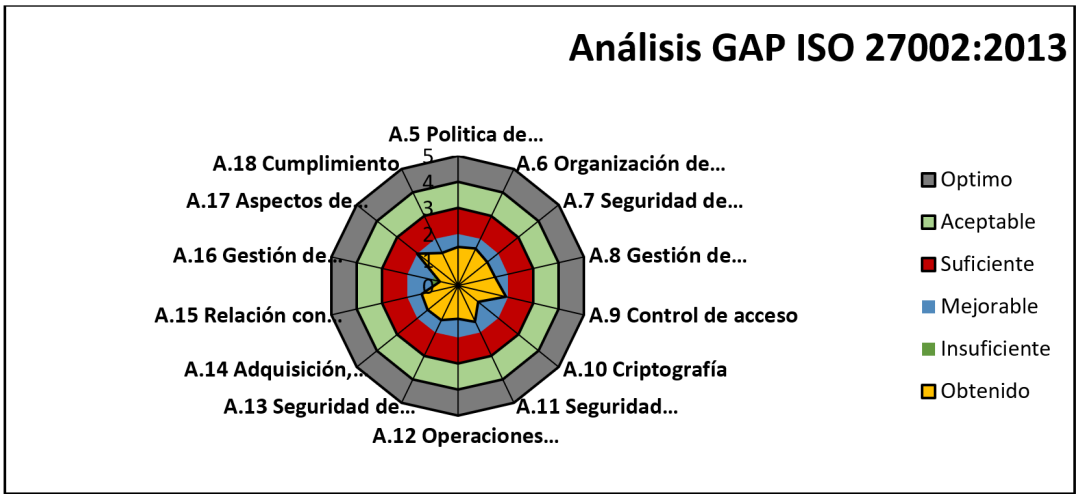
	VALOR	CUMPLIMIENTO
4. Contexto de la organización.	1,25	NO CUMPLE
5. Liderazgo.	1,666666667	CUMPLE PARCIALMENTE
6. Planeación.	2	CUMPLE PARCIALMENTE
7. Soporte	1,4	NO CUMPLE
8. Operación.	1	NO CUMPLE
9. Evaluación del desempeño.	1	NO CUMPLE
10. Mejora.	0	NO CUMPLE

Mediante la gráfica en forma de "diagrama de araña" se pueden observar las deficiencias de seguridad.



Por otra parte, la siguiente tabla muestra el nivel de madurez general de cada una de las secciones del anexo A de la norma ISO 27001:2013

CONTROL	VALOR	CUMPLIMIENTO
A.5 Política de seguridad de la información	1,5	NO CUMPLE
A.6 Organización de la seguridad de la información	1,6	NO CUMPLE
A.7 Seguridad de recursos humanos	1,44	NO CUMPLE
A.8 Gestión de activos	1,47	NO CUMPLE
A.9 Control de acceso	1,92	CUMPLE PARCIALMENTE
A.10 Criptografía	1	NO CUMPLE
A.11 Seguridad física y del entorno	1,56	NO CUMPLE
A.12 Operaciones de seguridad	1,26	NO CUMPLE
A.13 Seguridad de las comunicaciones	1,46	NO CUMPLE
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	1,48	NO CUMPLE
A.15 Relación con proveedores	1,42	NO CUMPLE
A.16 Gestión de incidentes de seguridad de la información	0,71	NO CUMPLE
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio	2	CUMPLE PARCIALMENTE
A.18 Cumplimiento	1,4	NO CUMPLE



Debería producirse una mejora general en todas las áreas relacionadas con la gestión de la seguridad de la información. Solamente dos áreas cumplen parcialmente con los requerimientos de la norma, control de acceso y aspectos de seguridad de la información de la gestión de la continuidad del negocio. De forma que el objetivo tras la implantación de los proyectos que se propondrán será conseguir el estado Aceptable u Óptimo.

4.2 SISTEMA DE GESTIÓN DOCUMENTAL

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que el Sistema de Gestión de Seguridad de la Información debe tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001. Estos documentos básicos son los siguientes:

- **Política de Seguridad de la Información:** Se trata de la normativa interna de la organización y de conocimiento y cumplimiento por parte del personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información.

- **Procedimiento de auditorías Internas:** Documento sobre la planificación de las auditorías que se efectuarán durante la vigencia de la certificación. La ISO/IEC 27001:2013 establece en su apartado 9.2 la necesidad de llevar a cabo auditorías internas con el objeto de verificar que el Sistema de Gestión de Seguridad de la Información cumple con los requisitos propios de la organización y con los requisitos de la norma indicada.

- **Gestión de Indicadores:** Deben definirse los indicadores para medir la eficacia de los controles de seguridad implantados, así como el sistema de medición.

- **Gestión de Roles y Responsabilidades:** El Sistema de Gestión de la Seguridad de la Información debe contar con un equipo que se encargue de crear, mantener, supervisar y mejorar el sistema. Debe disponer personal técnico y de dirección, para que se puedan tomar decisiones consensuadas con la dirección.

- **Procedimiento de Revisión por la dirección:** La dirección debe efectuar revisiones sobre las cuestiones más importantes que han sucedido en relación a Sistema de Gestión de la Información.

- **Metodología de Análisis de Riesgos:** Establece el método para calcular el riesgo, incluyendo la identificación y valoración de los activos, amenazas y vulnerabilidades.

- **Declaración de Aplicabilidad:** Documento que incluye todos los controles de seguridad establecidos en la Organización, con el detalle de su aplicabilidad, su estado actual y documentación relacionada.

4.3 ANÁLISIS DE RIESGOS

El primer paso del análisis de riesgos consiste en identificar los activos de seguridad de la información de la empresa. Se efectúa el inventario de los activos, clasificándolos en función de su tipología, asignándoles un valor y evaluando las dimensiones de seguridad (Autenticidad, Confidencialidad, Integridad, Disponibilidad, Trazabilidad).

Seguidamente, se analizan las amenazas a las que está expuesto cada uno de los tipos de activos de la organización y se calcula el impacto que pueden tener estas amenazas sobre los activos, así como la frecuencia estimada con la que pueden producirse las amenazas.

A continuación, en base a la información anterior se puede calcular el nivel de riesgo al que están expuestos cada uno de los activos de la organización.

La agrupación de los activos permite estudiar de forma más clara el grado de riesgo en que se encuentra cada activo.

Se observa un gran número de ellos en estado de riesgo tolerable y aceptable. Sin embargo, los catalogados como críticos o de alto riesgo demandan un tratamiento adecuado. Para ello se gestionará un plan de acción e implementarán los proyectos posteriores con el objeto de procurar minimizar el riesgo.

TRATAMIENTO DEL RIESGO CRÍTICO	
[SW-07]	Servidores
[D-01]	Bases de datos

TRATAMIENTO DEL RIESGO IMPORTANTE	
[SW-01]	Sistemas operativos
[SW-04]	Software de desarrollo
[SW-05]	Software de contabilidad
[D-04]	Backups (copias de seguridad)
[D-06]	Logs de servidores y clientes
[D-7]	Credenciales y datos de control de acceso.
[SER-06]	Servicio aplicaciones
[SER-07]	Servicio ficheros
[P-05]	Director Sistemas TI
[P-06]	Responsable seguridad de la información.

TRATAMIENTO DEL RIESGO MODERADO	
[SW-03]	Antivirus
[SW-06]	Email
[SER-05]	Servicio web

TRATAMIENTO DEL RIESGO TOLERABLE	
[SW-02]	Paquete ofimático
[SER-01]	Acceso remoto
[SER-03]	Acceso a internet
[SER-04]	Correo electrónico
[P-01]	Director General
[P-02]	Director comercial
[P-03]	Director de proyectos
[P-04]	Director financiero
[P-07]	Key Account Manager
[P-08]	Técnicos de sistemas
[P-09]	Personal del departamento comercial
[P-10]	Personal del departamento de proyectos

4.4 PROPUESTA DE PROYECTOS

Con la finalidad de reducir el riesgo de la organización, a unos niveles aceptables por parte de ella y según los aspectos descritos en el Plan Director, se propone la implantación de los siguientes proyectos:

PROYECTOS
Proyecto 1 – Definir políticas de seguridad de la información
Proyecto 2 – Mejora del CPD
Proyecto 3 – Control de acceso
Proyecto 4 – Plan de contingencia de datos – Backups y Restores
Proyecto 5 – Monitoreo SGSI
Proyecto 6 – Concienciación sobre la importancia de la información
Proyecto 7 – Criptografía
Proyecto 8 – Plan de clasificación de la información y tratamiento del mismo.
Proyecto 9 – Mantenimiento, control y protección equipos informáticos
Proyecto 10 – Proyecto Desarrollo de software
Proyecto 11 – Plan de contingencia y continuidad de negocio
Proyecto 12 – Procedimiento Gestión de incidentes

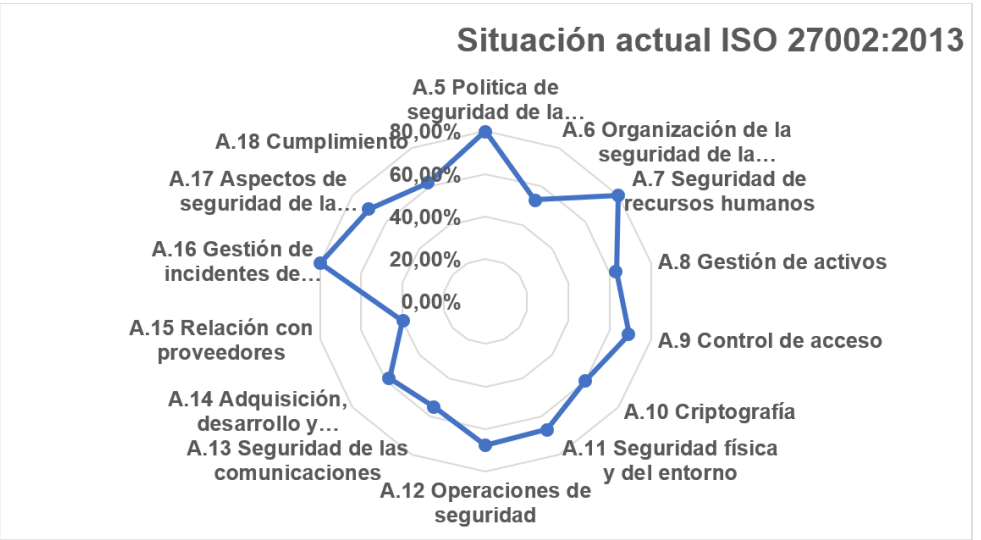
4.5 AUDITORÍA DE CUMPLIMIENTO

La auditoría de cumplimiento analiza la evolución y estado de la seguridad de la información. En esta fase se realizará nuevamente un análisis del estado de la empresa, en relación, a los distintos controles de la ISO/IEC 27002:2013 para poder comprobar si efectivamente tras la consecución de los distintos proyectos realizados y los controles que se han añadido, han producido efectos en el SGSI. La estimación se realizará según la tabla del Modelo de Madurez de la Capacidad (CMM).

Se han producido importantes mejoras en la situación de la seguridad de la información de la organización. Se ha definido la política de seguridad de la información, se han

CONTROL	Situación actual	Objetivo	Óptimo
A.5 Política de seguridad de la información	80%	100%	100%
A.6 Organización de la seguridad de la información	53%	60%	100%
A.7 Seguridad de recursos humanos	80%	80%	100%
A.8 Gestión de activos	63%	80%	100%
A.9 Control de acceso	69,33%	80%	100%
A.10 Criptografía	60%	90%	100%
A.11 Seguridad física y del entorno	66,83%	80%	100%
A.12 Operaciones de seguridad	67,76%	80%	100%
A.13 Seguridad de las comunicaciones	55,33%	80%	100%
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	57,85%	80%	100%
A.15 Relación con proveedores	40%	60%	100%
A.16 Gestión de incidentes de seguridad de la información	80%	90%	100%
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio	70%	80%	100%
A.18 Cumplimiento	62%	80%	100%

documentado normas y procedimientos y se han establecido procedimientos de medición que permiten detectar desviaciones frente a la evolución prevista. Por otra parte, ningún control de la norma figura en un nivel de madurez calificado como "0 – Inexistente".



A pesar de las mejoras, se han detectado diversas No conformidades y Observaciones que deberían ser tratadas y solucionadas.

Dominio A.6. Organización de la seguridad de la información
6.1.4 (L2) No conformidad menor
6.2.2 (L2) No conformidad menor

Dominio A.8. Gestión de activos
8.3.1 (L1) No conformidad menor

Dominio A.11. Seguridad física y del entorno
A.11.1.5(L1) No conformidad menor
A.11.1.6(L2) No conformidad menor
A.11.2.7(L2) Observación

Dominio A.12.Operaciones de seguridad
A.12.6.1(L1) No conformidad menor

Dominio A.13.Seguridad de las comunicaciones
A.13.1.1(L2) No conformidad menor

Dominio A.14.Adquisición, desarrollo y mantenimiento de los sistemas de información.
A.14.1.3(L2) No conformidad menor
A.14.2.4(L2) Observación
A.14.2.5(L1) Observación

Dominio A.15.Relación con proveedores
A.15.1.1(L2) No conformidad menor
A.15.1.2(L2) No conformidad menor
A.15.1.3(L2) No conformidad menor
A.15.2.1(L2) No conformidad menor
A.15.2.2(L2) No conformidad menor

Dominio A.16.Gestión de incidentes de seguridad de la información
A.16.1.6(L2) No conformidad menor

Dominio A.18.Cumplimiento
A.18.1.1(L2) Observación
A.18.1.2(L2) Observación
A.18.1.3(L2) Observación
A.18.1.4(L2) Observación

5. CONCLUSIONES

La ejecución del presente proyecto supone una mejora en el nivel de madurez de seguridad de la información en la organización. Se ha tomado conciencia sobre la importancia de los sistemas de gestión de la seguridad. Mediante su implementación se ha conseguido:

- Reducir los riesgos asociados a la seguridad de la información.
- Garantizar el tratamiento y seguridad de la información.
- Hacer la empresa más competitiva tanto a nivel nacional como internacional.
- Cumplir con la normativa legal vigente en materia de protección de datos personales.
- Ofrecer una imagen de buenas prácticas a clientes y proveedores.
- Asegurar la continuidad del negocio, reduciendo los tiempos de recuperación de los sistemas, ante posibles incidentes.

Por último, mediante la mejora continua se seguirá trabajando para mantener el nivel de madurez en aquellos dominios que cumplen con los requisitos de la norma y alcanzar un nivel de madurez lo más óptimo posible del resto.