POSGRADO EN GESTIÓN Y AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN

Posgrado en gestión y auditoría de la seguridad de la información

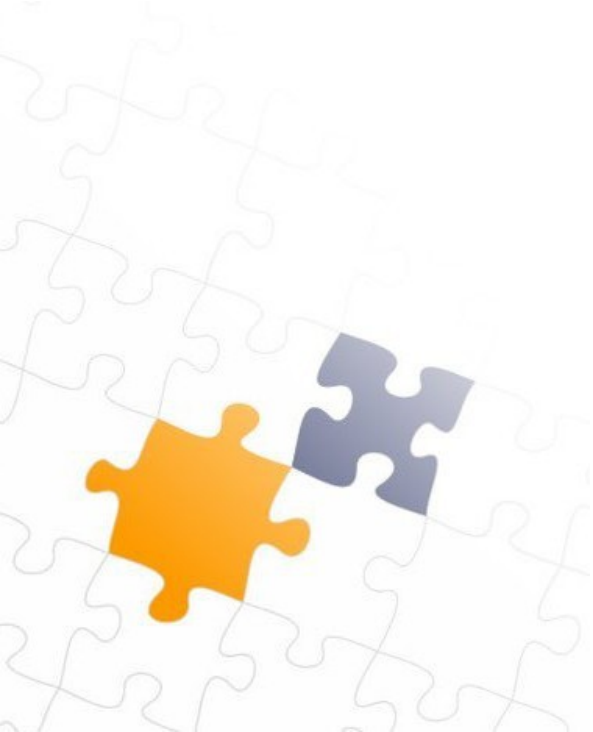
PLAN DIRECTOR DE SEGURIDAD DEL AYUNTAMIENTO DE BUENAS MANERAS

DIRECTOR: Carles Garrigues
CONSULTOR: Arsenio Tortajada
ALUMNO: Jennifer Gil

PRESENTACIÓN (JUNIO 2017)

UOC
Universitat Oberta de Catalunya
www.uoc.edu

ÍNDICE



1. INTRODUCCIÓN

LA INFORMACIÓN EN LAS AA.PP.

- Responsabilidades legales(Llei 15/1999, ENS, …)
- Funciones operativas y de gestión
- Estado de derecho
- Responsabilidades de custodia de la información
- Servicios al ciudadano

1. INTRODUCCIÓN

LA INFORMACIÓN EN LES AA.PP.

Importancia máxima en seguridad del Ayuntamiento:

- La **DISPONIBILIDATD** (Acceso a la información)
- La **INTEGRIDAD** (Contenido correcto y exacto)
- La **CONFIDENCIALIDAD** (Privacidad de los datos)
- La **AUTENTICIDAD** (Para asegurar la auditoría)
- La **TRAZABILIDAD** (Realización de seguimiento)

1. INTRODUCCIÓN

LA INFORMACIÓN EN LES AA.PP.

Posibles amenazas:

- Inundación en Centro de Protección de Datos
- Robo de información confidencial

  Falta de implicación de la dirección
- Error de maquinaria
- Uso malintencionado de algún elemento de las TIC
- ...

1. INTRODUCCIÓN

LA INFORMACIÓ EN LES AA.PP.

Problemas de la Seguridad de la Información:

- Complejidad de la organización
- Falta de planificación y visión global
- Falta de formación del personal
- Viabilidad económica
- ...

1. INTRODUCCIÓN

PLAN DE SEGURIDAD, ¿POR QUÉ?

- Análisis de la situación actual
- Organización de roles y responsabilidades
- Adaptación a las normativas
- (ISO 27001:2005 – Establiment d'un SGSI)
- Detección de posibles problemas y amenazas
- Definición de objetivos y mejoras en el sistema
- Seguimiento y control del ciclo (Ciclo PDCA)

2. PLAN DE SEGURIDAD

ÁMBITO:

- Infraestructuras y redes:

  Salas, cableados, (CPD).

- Aplicaciones y servicios

  Gestión de padrón, contabilidad, registro, expedientes, etc.

- Datos

  Padrón, contabilidad anual, convenios y contratos, documentos, ...

- Recursos humanos relacionados con las TIC

  Cualquier trabajador afectado por el uso de las tecnologías de la información

2. PLAN DE SEGURIDAD

OBJETIVOS:

- Mejora de la Seguridad de la Información.
- Facilitar el cumplimiento de las leyes actuales(LOPD, ENS, ...).
- Conocimiento del estado actual de la organización.
- Propuesta de mejoras para mejorar la seguridad
- Control periódico de las medidas aplicadas
- Ahorro económico en caso de accidente

2. PLAN DE SEGURIDAD

FASES:

- **FASE 1:** Situación actual (contexto, objetivos y análisis diferencial ISO)
- **FASE 2:** Sistema de Gestión Documental
- **FASE 3:** Análisis de riesgos (metodología MAGERIT)
- **FASE 4:** Propuestas de proyectos
- **FASE 5:** Auditoría de cumplimiento (respecto ISO 27001)
- **FASE 6:** Presentación de resultados y conclusiones

2. PLAN DE SEGURIDAD

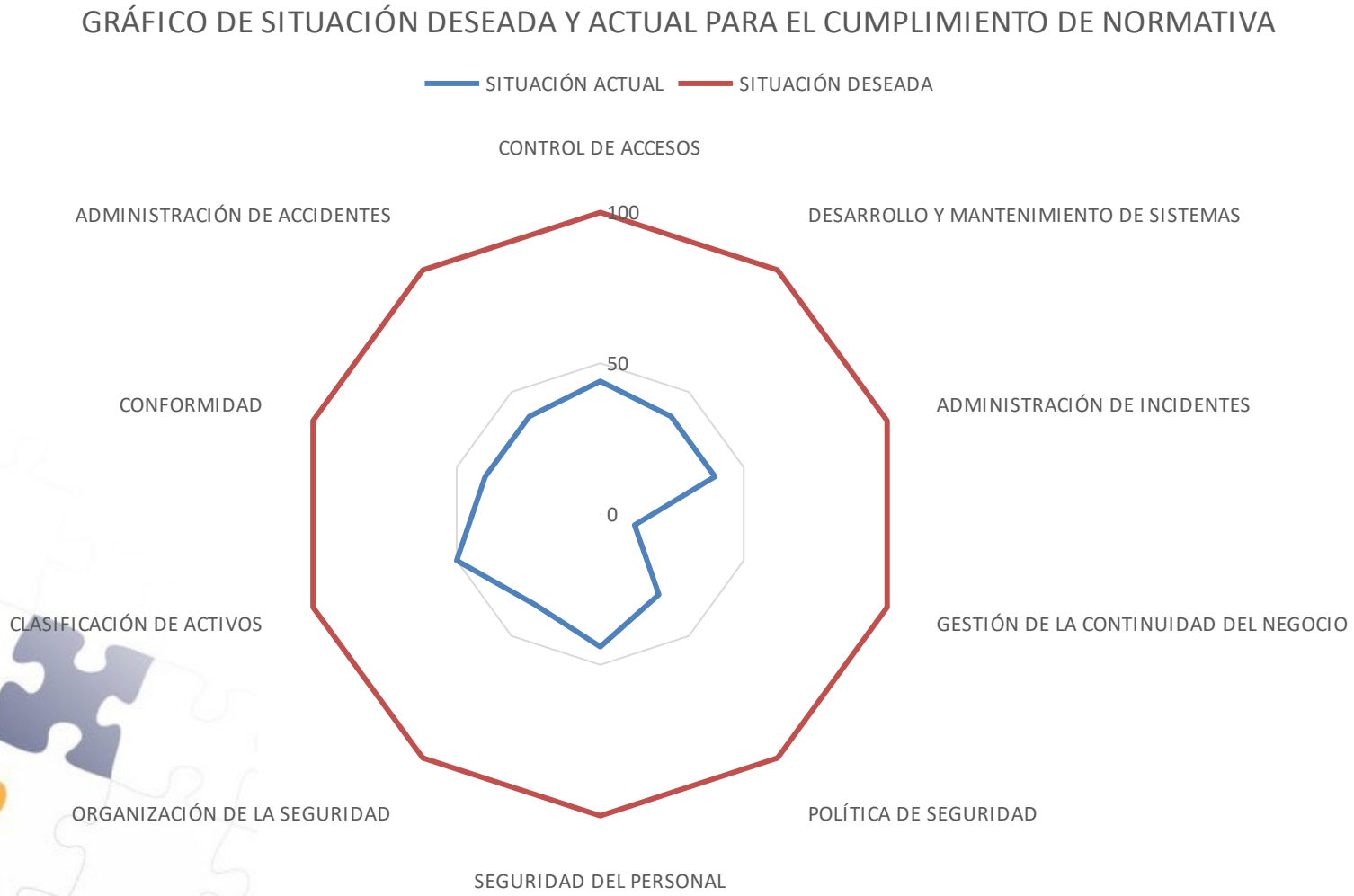
ISO 27001

5. Política de seguridad (1 objetivo, 2 controles)
6. Organización de la seguridad de la información (2 objetivos, 11 controles)
7. Gestión de activos (2 objetivos, 5 controles)
8. Seguridad relativa al personal (3 objetivos, 9 controles)
9. Seguridad física y del entorno (2 objetivos, 13 controles)
10. Gestión de comunicaciones y operaciones (10 objetivos y 32 controles)
11. Control de acceso (7 objetivos y 25 controles)
12. Seguridad en la adquisición, en el desarrollo y en el mantenimiento de SI (5 objetivos, 14 controles)
13. Gestión de incidencias (2 objetivos, 5 controles)
15. Conformidad (3 objetivos, 10 controles)

11 Dominios, 39 objetivos de control y 133 controles.

3. ANÁLISI DE RESULTADOS

SITUACIÓN ACTUAL – Análisis diferencial



3. ANÁLISIS DE RESULTADOS

ANÁLISIS DE RIESGOS

METODOLOGÍA: MAGERIT

- Valoración de activos
- Clasificación
- Análisis de amenazas
- Impacto potencial
- Cálculo de riesgo

3. ANÁLISIS DE RESULTADOS

Objetivo análisis de resultados

- Determinar los activos relevantes para el ayuntamiento, su interrelación y su valor en el caso de degradación y perjuicios asociados.
- Determinar cuáles salvaguardas están disponibles y su eficacia.
- Estimar el impacto, definido como el perjuicio sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de frecuencia (o expectativa de materialización) de la amenaza.

4. PROPUESTA DE PROYECTOS

OBJETIVOS:

- **Reducir el riesgo de determinados activos**
- **Mejorar el nivel de cumplimiento de la ISO 27002**

  - Mayor optimización de los recursos
  - Mejoras en la gestión de procesos
  - Mejoras en las tecnologías utilizadas

4. PROPUESTA DE PROYECTOS

PROYECTOS PROPUESTOS

5. Política de seguridad.

6. Aspectos organizativos de la seguridad de la información.

8. Seguridad ligada a los recursos humanos.

12. Adquisición, desarrollo y mantenimiento de sistemas de información.

13. Gestión de incidentes en la seguridad de la información.

14. Gestión de la continuidad del negocio.

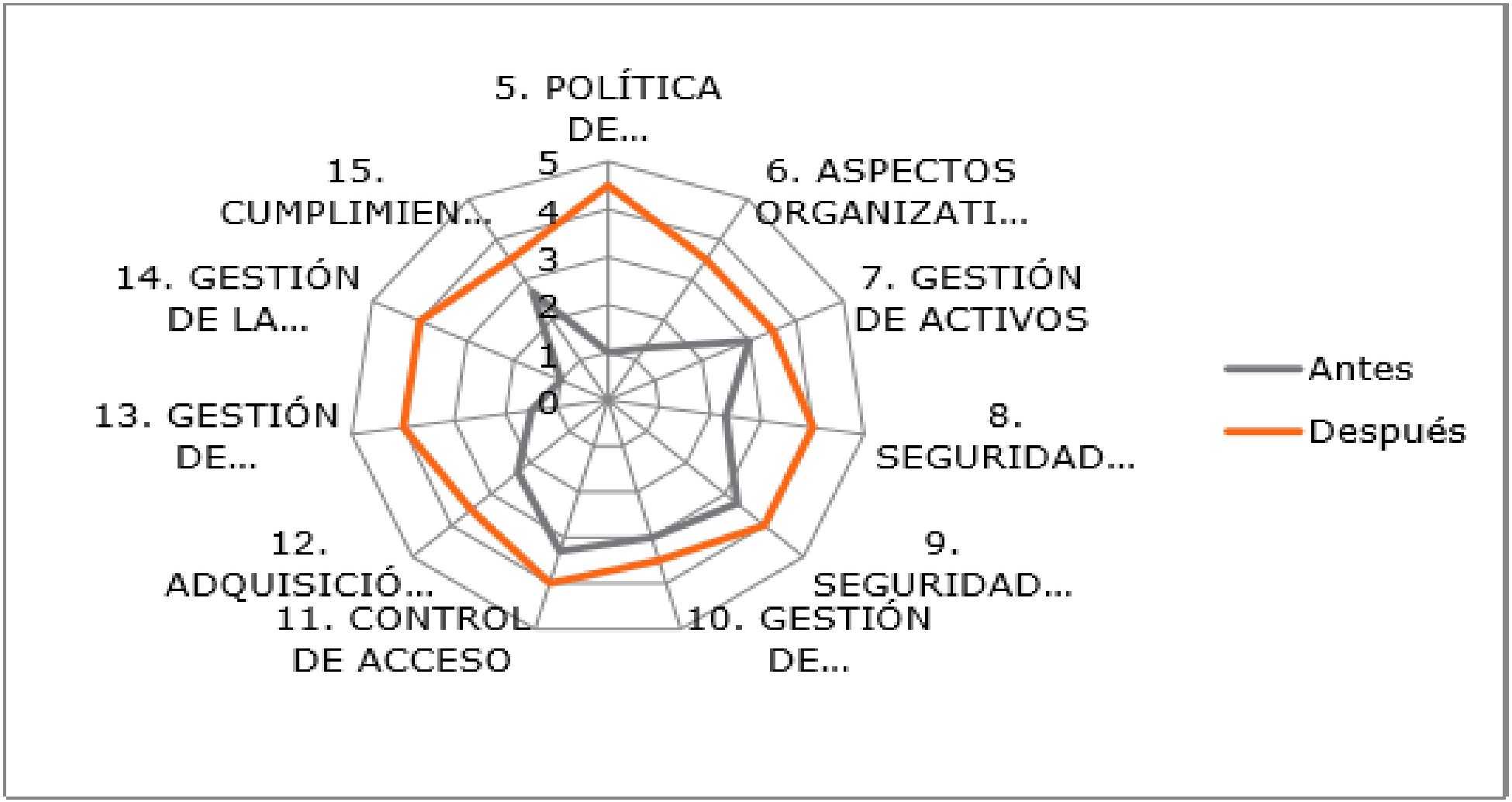
4. PROPUESTA DE PROYECTOS

IMPACTO

PROYECTO	% Reducción del impacto	Dificultad de implantación
1. Redefinición de la política de seguridad y aspectos organizativos	70%	Baja
2. Programa de formación y sensibilización en seguridad de la información	80%	Baja
3. Definición de política de controles criptográficos y procedimientos de control de cambios	60%	Media
4. Mejora en la gestión de incidentes de seguridad	50%	Media
5. Establecimiento de un plan de continuidad de negocio	65%	Alta

4. PROPUESTA DE PROYECTOS

IMPACTO



5. AUDITORÍA DE CUMPLIMIENTO

OBJECTIVOS

- Avaluación de la madurez de la seguridad

  (Modelo de madurez de la capacdad - CMM)

- Revisión detallada de los 133 controles de la ISO 27002
- Detección de no conformidades mayor y menor
- Anotación de las diferentes observaciones

5. AUDITORÍA DE CUMPLIMIENTO

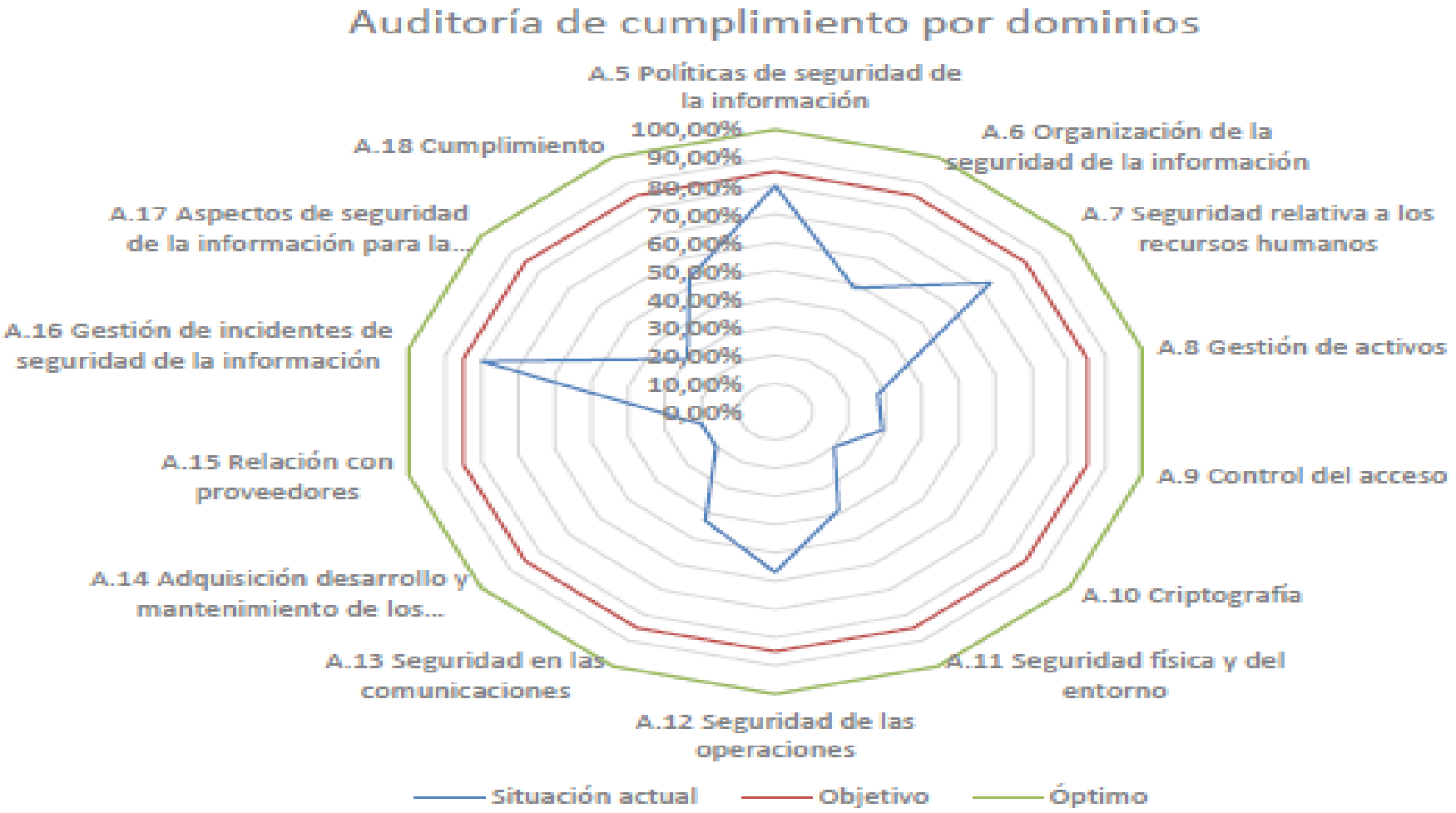
RESULTADOS

Han mejorado los siguientes dominios:

- Políticas de seguridad de la Inf.
- Gestión de incidentes de la Información

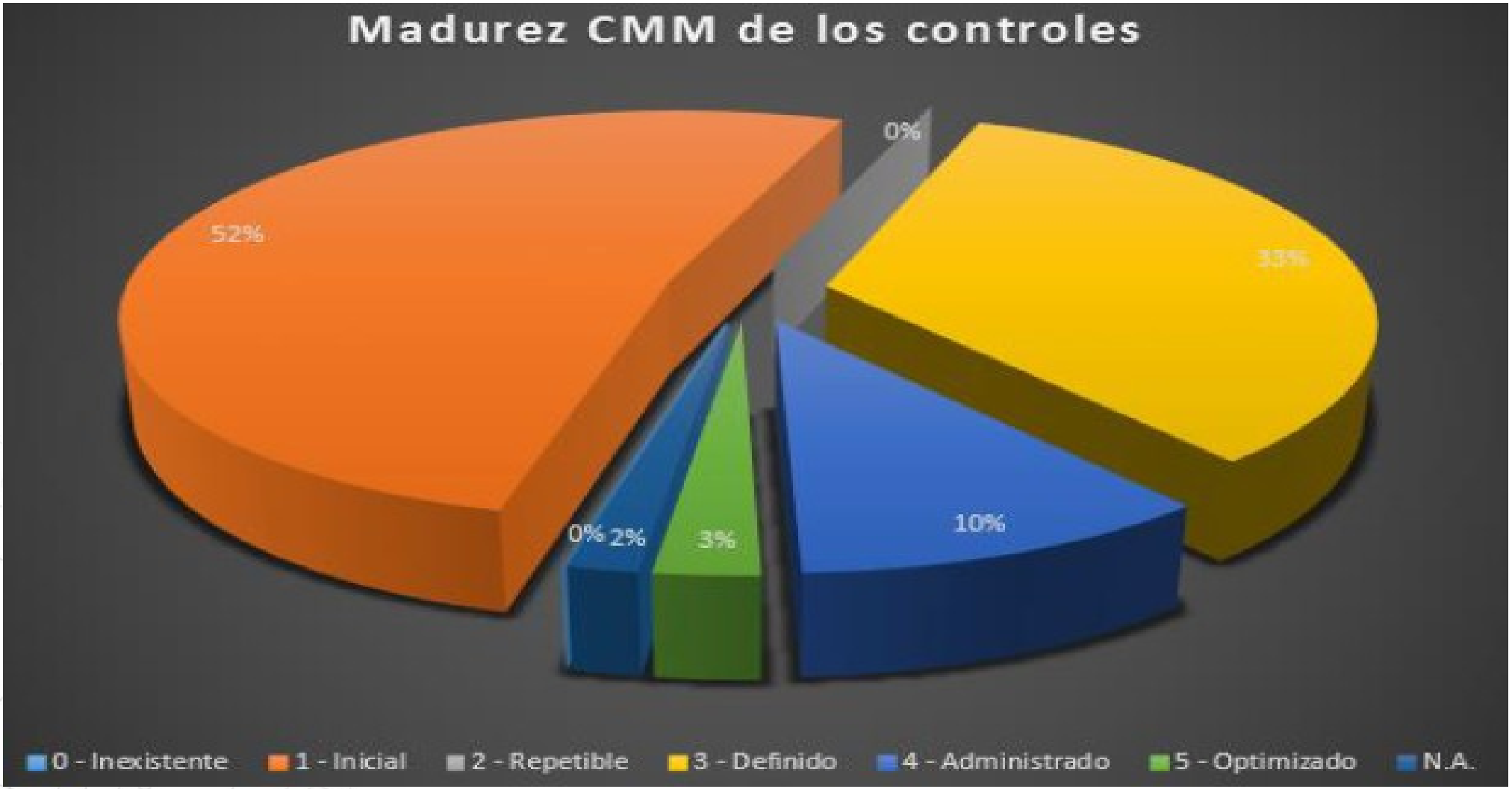
5. AUDITORÍA DE CUMPLIMIENTO

RESULTADOS



5. AUDITORÍA DE CUMPLIMIENTO

RESULTADOS



6. CONCLUSIONES

PLAN DE SEGURIDAD – AYUNTAMIENTO DE BUENAS MANERAS

- Se ha definido el alcance y los objetivos del plan de seguridad.
- Se ha evaluado la situación actual de la seguridad.
- Se ha realizado el análisis de riesgos (MAGERIT)
- Se han propuesto proyectos de mejora
- Se ha realizado una auditoría de cumplimiento