Universitat Oberta de Catalunya

Plan Director de Seguridad en la Administración Local

bajo la perspectiva de la calidad del dato

Estudiante: Ramón Asensio Palao
Programa: Máster Univ. en Ciberseg. y Privacidad
Centro: Universitat Oberta de Catalunya
Consultor: Antonio José Segovia Henares
Profesor resp. TFM: Carles Garrigues Olivella

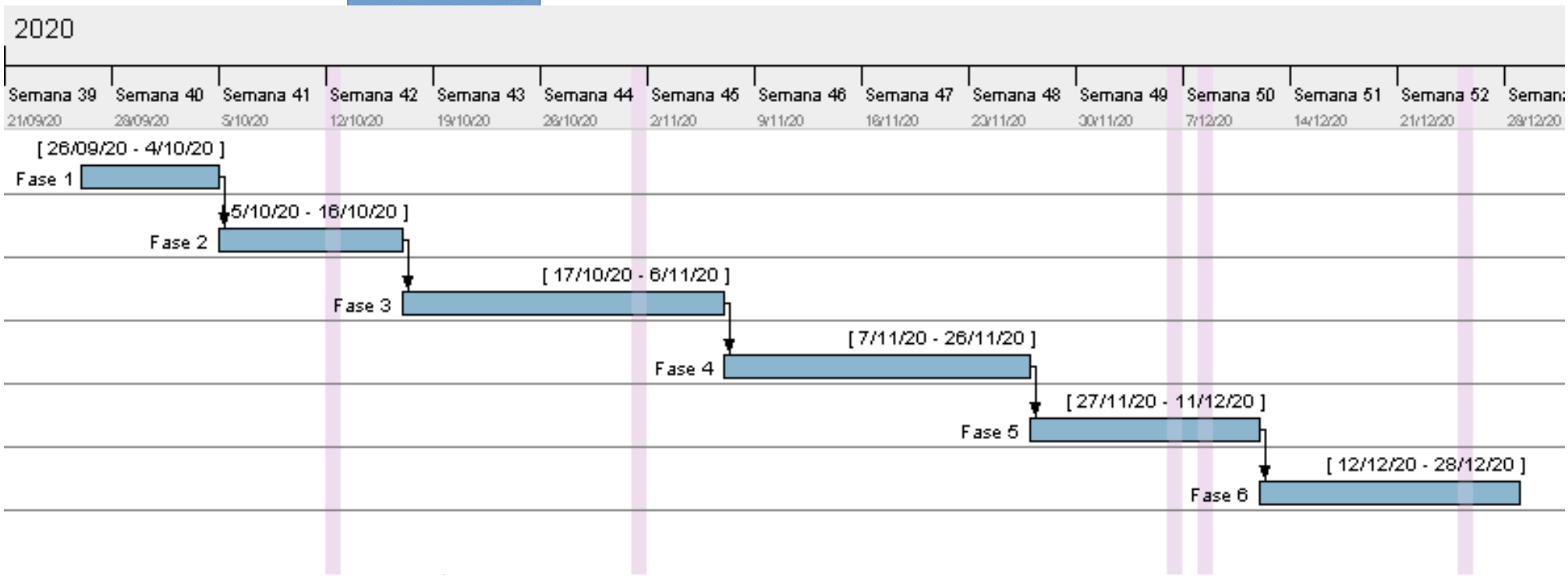
1. Introducción

1. Introducción - Objetivos

- Mejorar la seguridad del sistema integral de gestión de información en la administración pública local.
- Dar cumplimiento a las normativas de Esquema Nacional de Seguridad y Esquema Nacional de Interoperabilidad.
- Implementar buenas prácticas en los SGSI acordes a ISO/IEC 27001 e ISO/IEC 27002.
- Establecer nexos de unión entre seguridad y calidad del dato.
- Acercar el gobierno del dato al ciudadano.
- Convertir este TFM en una guía práctica de cumplimiento de ENS y Calidad del Dato aplicable a la Administración Local.

1. Introducción - Metodología

Fase 1. Contextualización, objetivos y Análisis Diferencial



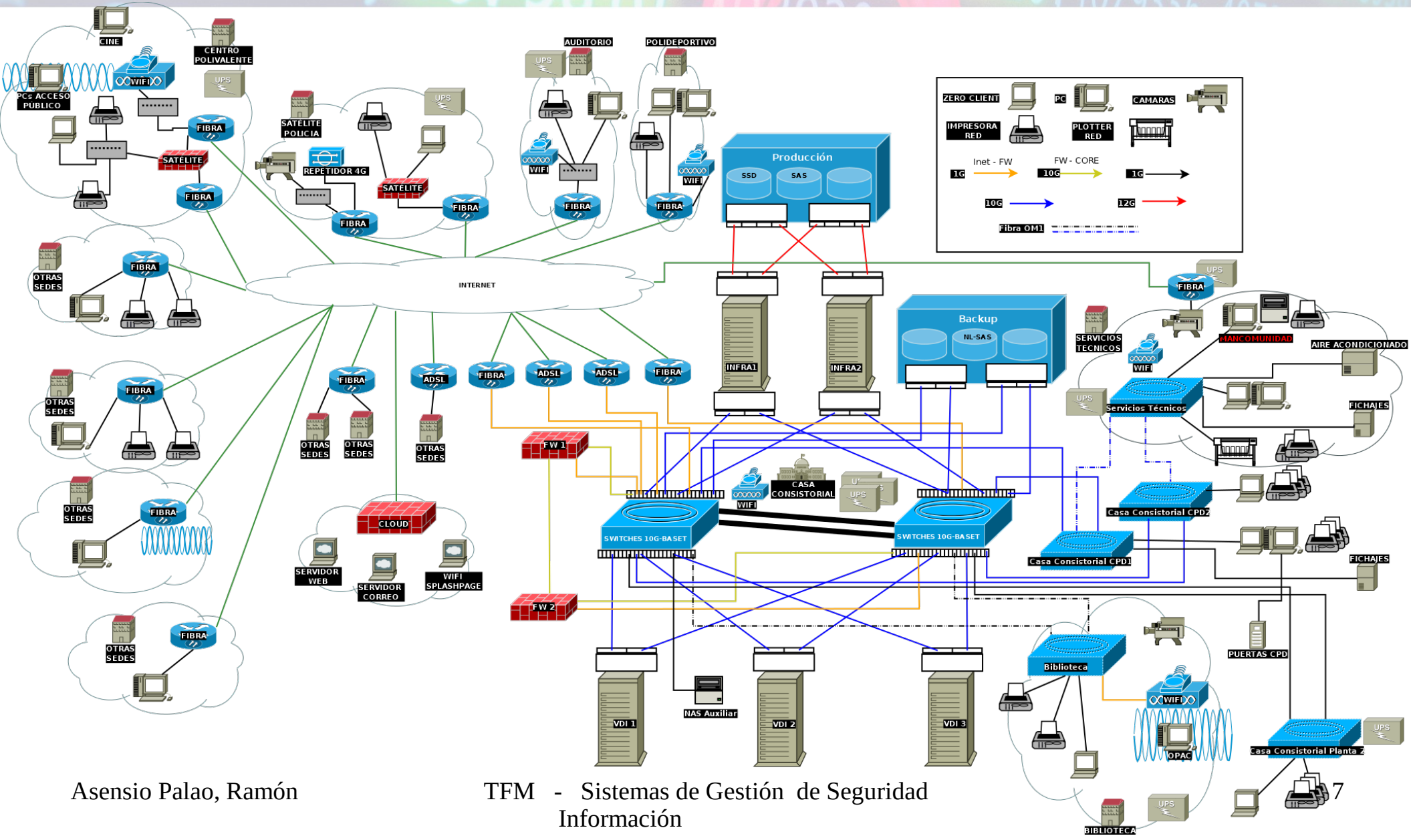
Fase 6. Presentación de Resultados

2. Contextualización, Objetivos y Análisis Diferencial

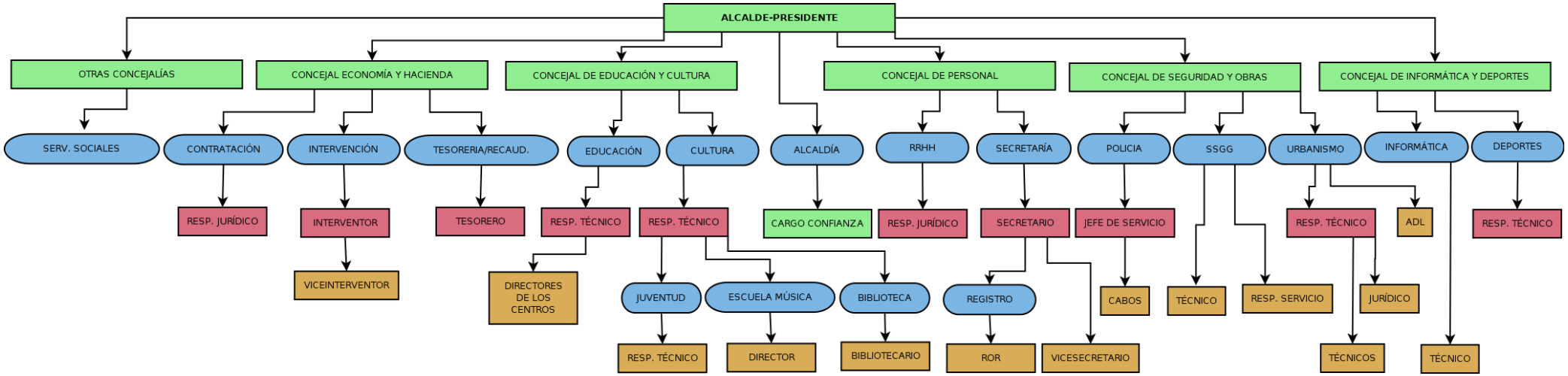
2. Contextualización, Objetivos y Análisis Diferencial

- Administración local de 20.000 habitantes aprox.
- 16 millones de € aprox. de presupuesto anual
- 18 sedes con acceso a datos (9 propias)

2. Contextualización, Objetivos y Análisis Diferencial

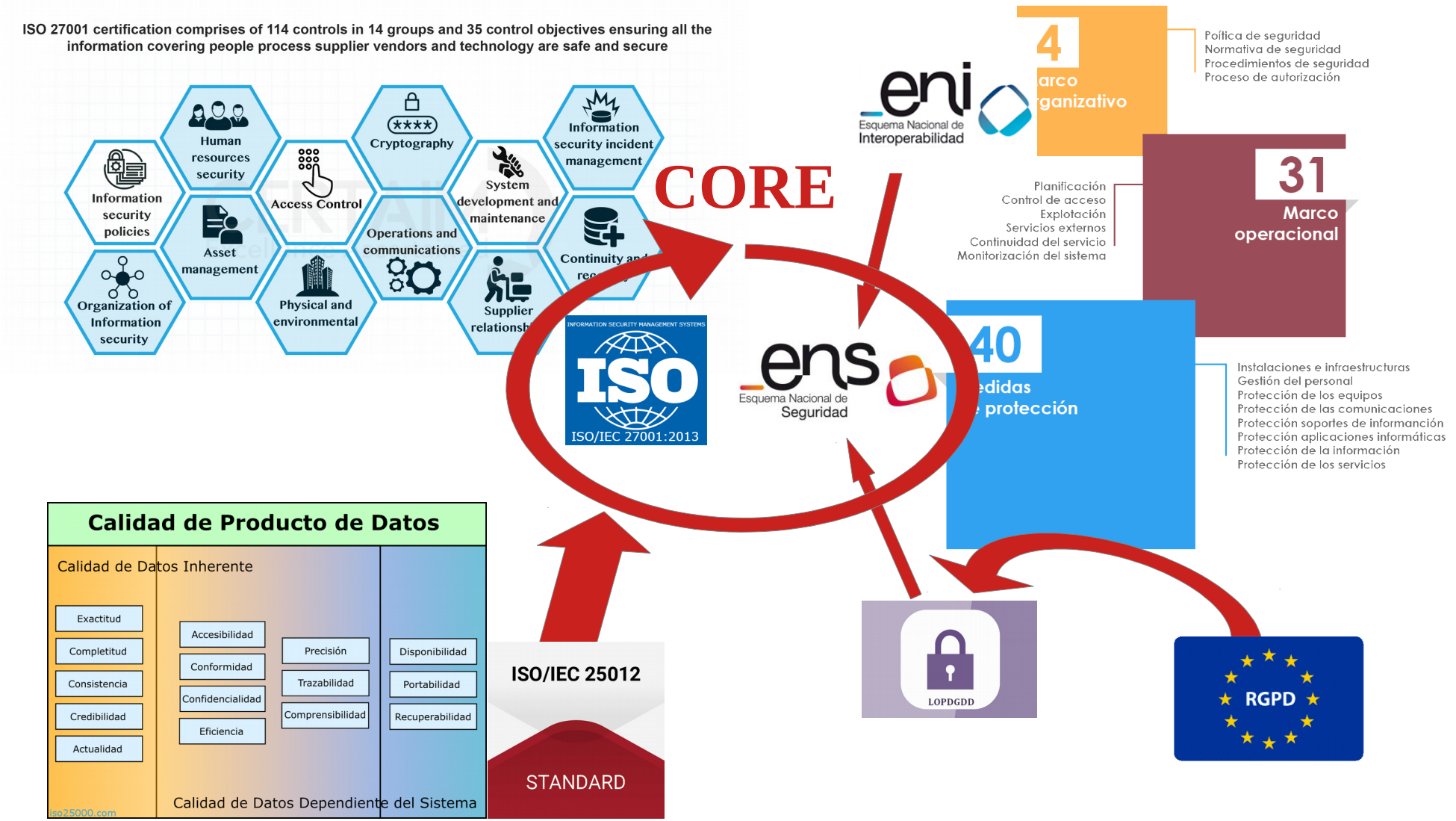


2. Contextualización, Objetivos y Análisis Diferencial



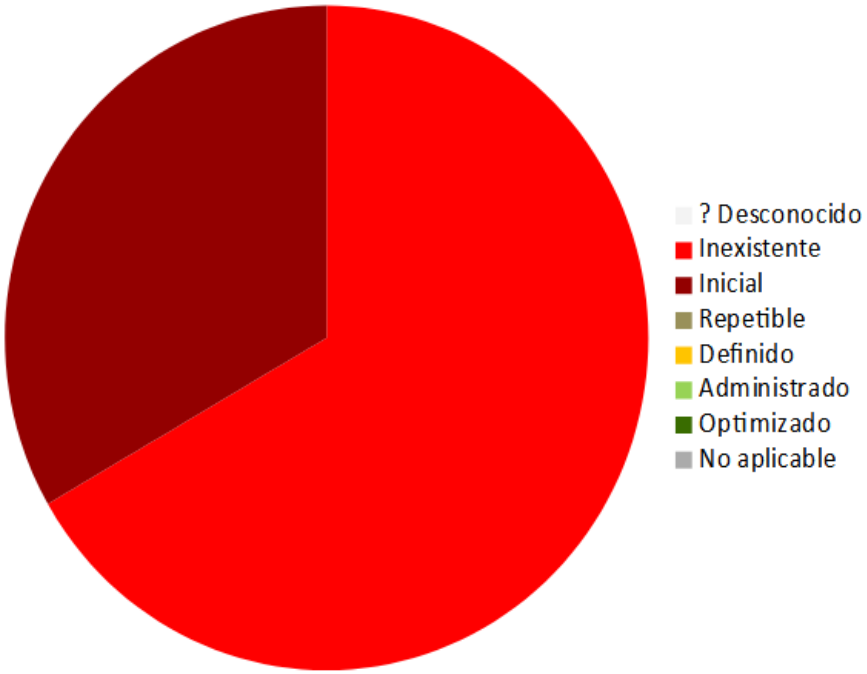
90 empleados aprox. con acceso de sistemas de información
1 Ingeniero técnico de Sistemas
1 FP de microinformática

2. Contextualización, Objetivos y Análisis Diferencial

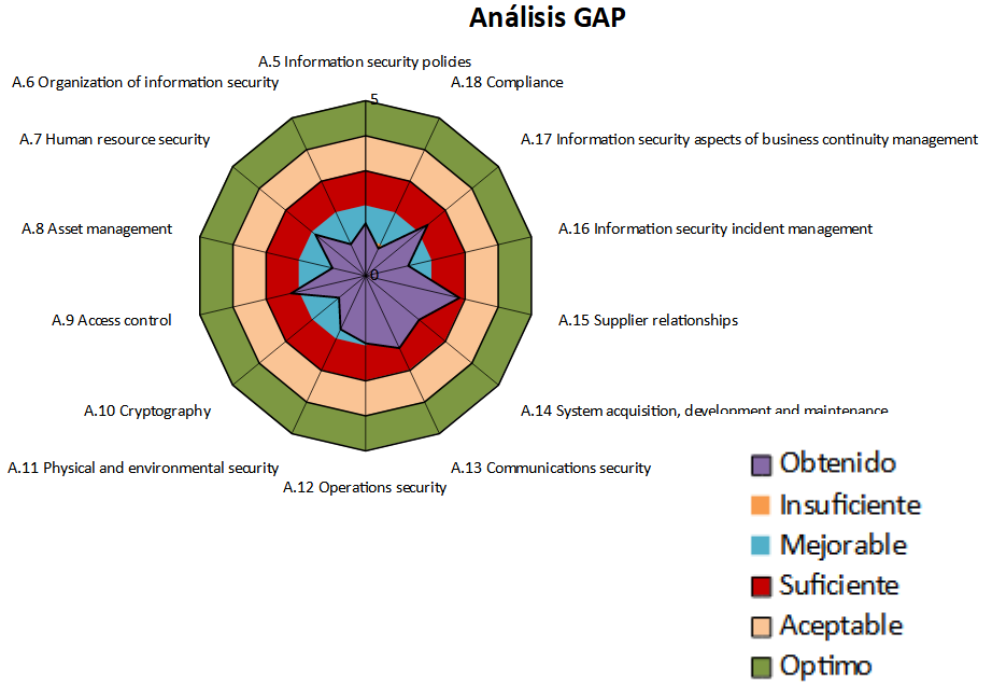


2. Contextualización, Objetivos y Análisis Diferencial

ISO/IEC 27001:2013



ISO/IEC 27002:2013



2. Contextualización, Objetivos y Análisis Diferencial

ENS

Proceso de gestión de derechos de acceso	(80%)
Mecanismos de autenticación	(51,25%)
Acceso local	(60,86%)
Configuración de seguridad	(62,28%)
Gestión de cambios	(100%)
Protección frente a código dañino	(100%)
Registro de actividad de los usuarios	(100%)
Protección de los registros de actividad	(100%)
Bloqueo de puesto de trabajo	(70%)
Protección de equipos informáticos	(100%)
Protección de la auten. y de la integridad	(66,67%)

ENI

Interop. organizativa:	Cumplimiento Medio
Interop. semántica:	Cumplimiento Medio
Interop. técnica:	Cumplimiento Medio-Alto
Infraestruc. y servicios comunes:	Cumplimiento Alto
Comunicaciones de las AAPP:	Cumplimiento Alto
Firma electrónica y certificados:	Cumplimiento alto
Recup. y conservación del Doc. Elec.	Cumplimiento insuf.
Normas de conformidad:	Cumplimiento insuficiente

3. Sistema de Gestión Documental

3. Sistema de Gestión Documental

1) Plan de Adecuación al ENS

2) Política de Seguridad

3) Procedimiento de Auditorías Internas

4) Gestión de Indicadores

5) Procedimiento de revisión por Dirección

6) Roles y responsabilidades

7) Metodología de Análisis de Riesgos

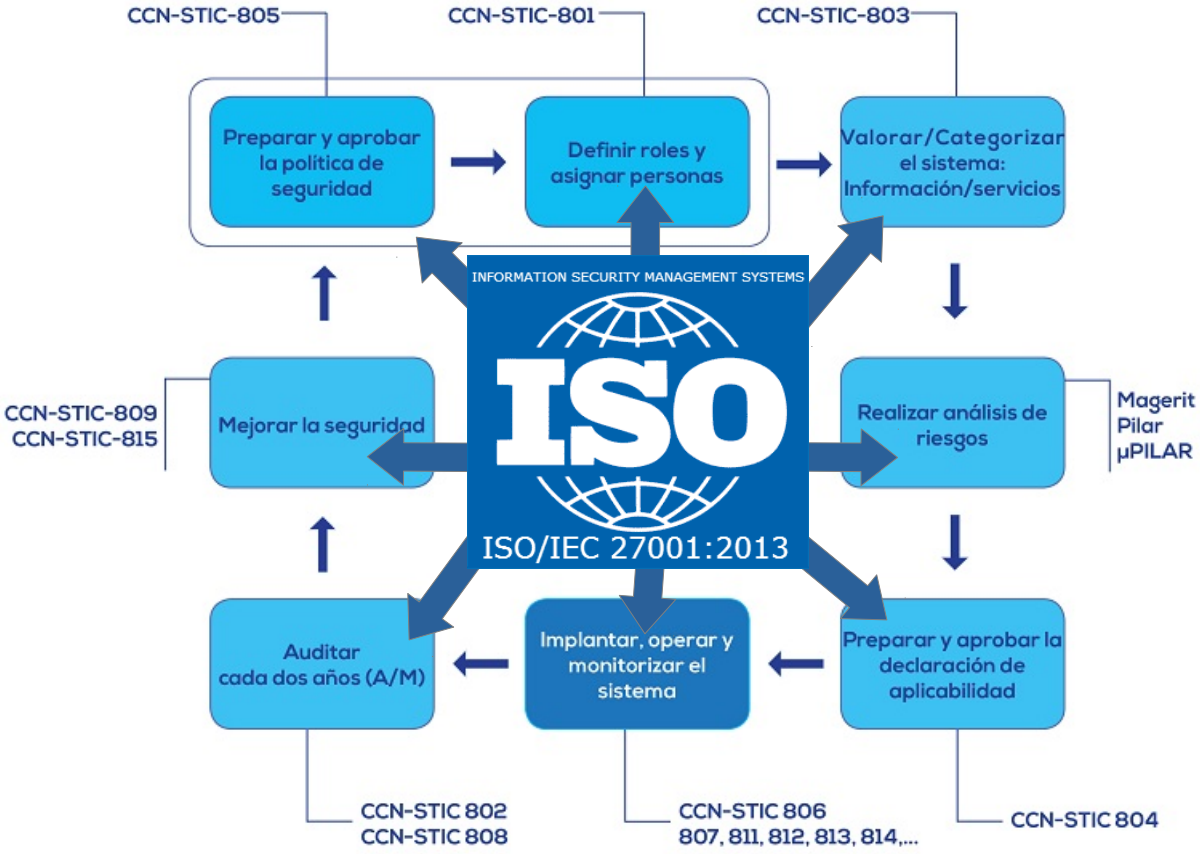
8) Declaración de Aplicabilidad

9) Plan de mejora de la seguridad

10) Plan de modelado de Calidad del Dato

3. Sistema de Gestión Documental

1) Plan de Adecuación al ENS



Trabajaremos desde la base del ENS hacía ISO/IEC 27001

3. Sistema de Gestión Documental

2) Política de Seguridad: propósito general de nuestro SGSI

- Misión
- Alcance
- Marco Normativo: Ley 39/2015, Ley 40/2015, RD 3/2010
- Cumplimiento: ISO/IEC 27001, ISO/IEC 27002 y ENS
- Organización de la seguridad: roles, comité de seguridad de la información, responsabilidades, funciones, etc.
- Datos de carácter personal: LOPGDD y RGPD
- Terceras partes

3. Sistema de Gestión Documental

3) Procedimiento de Auditorías Internas

- Objetivo de la Auditoría
- Alcance
- Roles y responsabilidades: ISMR, Responsable del programa de auditoría, Equipo auditor
- Procedimiento: planificación preliminar, reunión de inicio, ejecución, presentación de hallazgos, reunión de fin.
- Programación de auditorías
- Seguimiento y cierre

3. Sistema de Gestión Documental

4) Gestión de Indicadores: definir métricas de madurez para el cumplimiento.

5) Procedimiento de revisión por Dirección: revisar los problemas y los riesgos, tomar decisiones estratégicas para garantizar los objetivos del SGSI y la calidad de los datos.

6) Roles y responsabilidades: definir de Responsable de Información, Responsable de los Servicios, Responsable de Seguridad (CISO), Responsable del Sistema (CIO), DPD.

3. Sistema de Gestión Documental

7) Metodología de Análisis de Riesgos:

Metodología: magerit v.3.0

Herramienta: CCN-CERT /pilar>

Compatible con: ISO/IEC 27001:2013 | ens Esquema Nacional de Seguridad | LOPDGDD | RGPD

3. Sistema de Gestión Documental

8) Declaración de aplicabilidad: seleccionamos los controles ENS necesarios, establecemos equivalencia con los controles ISO/IEC 27002:2013. *

* Para la certificación en ISO/IEC 27001:2013 será necesario escribir una nueva declaración de aplicabilidad basada en esta atendiendo a los objetivos propios de la normativa.

9) Plan de mejora de la seguridad: contiene un informe de insuficiencias y nos muestra el camino a la hora de priorizar tareas de mejora de la seguridad para el ENS.

3. Sistema de Gestión Documental

10) Plan de modelado de Calidad del Dato: establecer los criterios para determinar si es mejor sustituir un activo antes que invertir en su seguridad.

- Requisitos de evaluación: confidencialidad, trazabilidad, disponibilidad, conformidad y recuperabilidad.

4. Análisis de Riesgos

4. Análisis de Riesgos

1) Análisis de Riesgos

2) Categorización del Sistema de acuerdo con el ENS

3) Calidad del Dato

4. Análisis de Riesgos

1) Análisis de riesgos: con metodología MAGERIT y la herramienta PILAR llevaremos a cabo las siguientes acciones:

- Inventariamos los activos.
- Establecemos dependencias entre ellos.
- Valoramos los activos.
- Evaluamos las amenazas que pueden producirse y el impacto que ocasionarían.
- Calculamos todos los tipos de riesgo: riesgo actual, riesgo aceptable aprobado por la dirección y riesgo residual.

4. Análisis de Riesgos

2) Categorización del sistema de acuerdo con el ENS: nos permite categorizar el sistema como de nivel MEDIO

- Identificar e inventariar los servicios y la información.
- Valorar los servicios y la información.
- Categorizar el sistema.
- Adicionalmente relacionamos los activos del Análisis de Riesgos con los activos encontrados en la categorización del sistema de modo que sea más sencillo relacionar su actividad.

4. Análisis de Riesgos

3) Calidad del dato: identificamos activos que no cumplan con la calidad del dato para no asignarlos en las propuestas de mejora de la seguridad y crear proyectos exclusivos de renovación que los traten.

- Identificación de activos evaluables: datos y servicios.
- Valoración de los activos.
- Nivel de calidad del dato aceptable aprobada por la dirección.
- El software financiero y de RRHH no pasa la evaluación.

5. Propuesta de Proyectos

5. Propuesta de Proyectos

1) Proyectos Prioritarios

2) Proyectos de mejora de la Calidad del Dato

3) Cuantificación económica

4) Cuantificación temporal

5) Impacto de los proyectos sobre la seguridad

5. Propuesta de Proyectos

1) Proyectos prioritarios: se tienen que acometer a corto plazo.

Plan de formación en seguridad	RSEG y CSI
Procedimiento de gestión de seguridad con terceros	CSI
Procedimiento de Protección frente a código dañino	RSIS y RSEG
Procedimiento de segmentación de redes	RSIS
Procedimiento de control de acceso	RSIS
Política de acceso a la información	RSIS y CSI
Instrucciones técnicas de configuración segura	RSIS
Gestión y configuración de las copias de seguridad	RSIS
Mejora de la Ciberseguridad	RSEG
Mejora de la seguridad del CPD	RSIS
Procedimiento de captura de registros de actividad	RSIS
Puesta en marcha de entornos de prueba/producción	RSIS
Seguridad en mecanismos de autenticación	RSIS

5. Propuesta de Proyectos

2) Proyectos de mejora de la Calidad del Dato: tienen que acometerse después de los prioritarios

- Proyecto para renovar los servicios económicos del Ayuntamiento, activos sustituidos: software de contabilidad, software de recaudación, bases de datos asociadas.

- Proyecto para renovar la plataforma del empleado, activos sustituidos: software de intranet, software de fichaje, bases de datos asociadas.

5. Propuesta de Proyectos

3) Cuantificación económica:

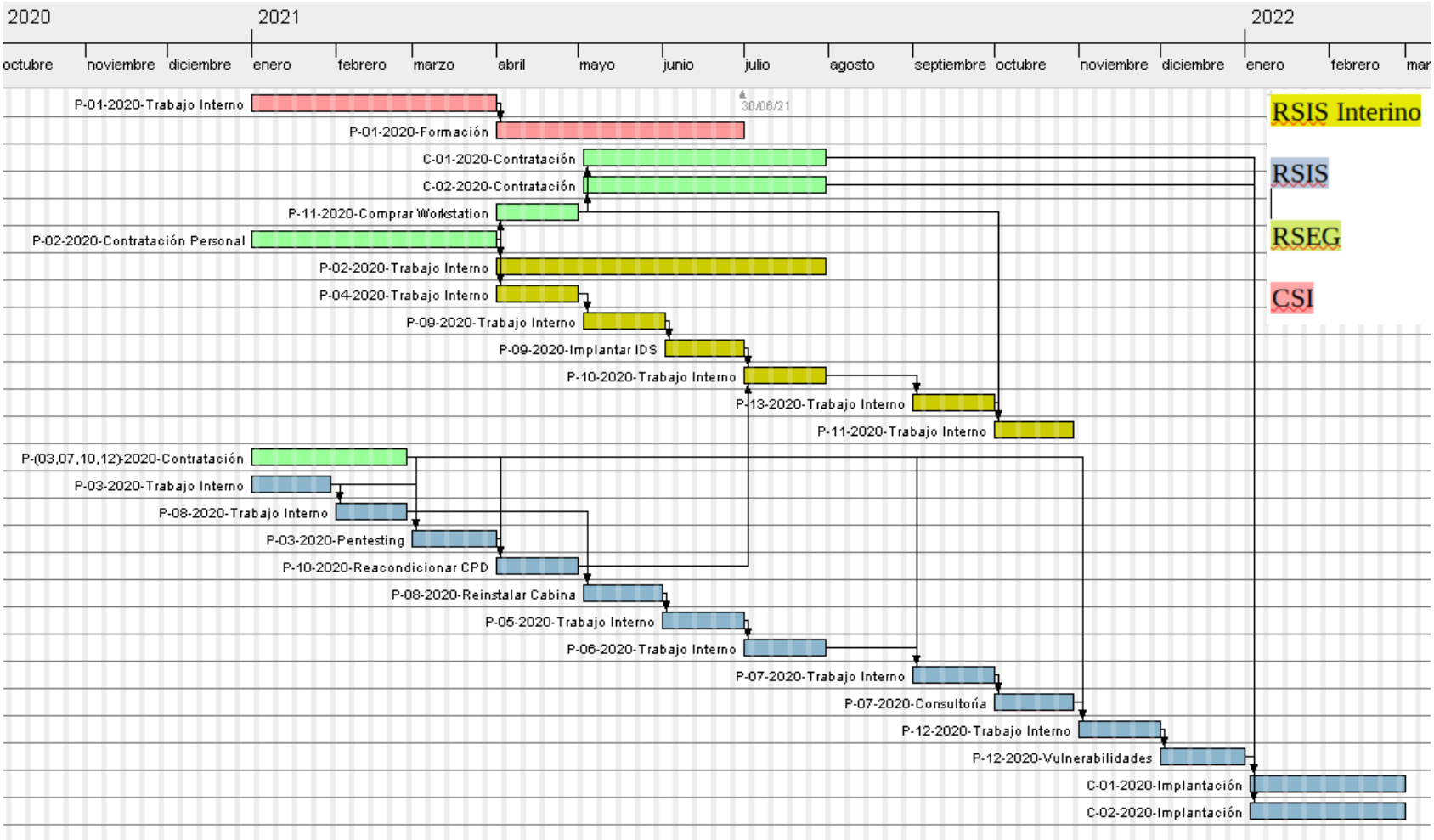
CONTRATACIÓN
Plataforma de Contratación del Sector Público

TOTAL: 130.000 € IVA inc. (+20%)

Empresa de formación	3.500 € IVA incluido
Técnico Interino Informático	35.000 € brutos
Servicio de Pentesting	3.000 € IVA incluido
Servicio de Consultoría	3.500 € IVA incluido
Reinstalación de la cabina de backup	2.000 € IVA incluido
Implantar IDS de red	10.000 € IVA incluido
Reacondicionamiento CPD	20.000 € IVA incluido
Workstation para instalar GLORIA y LUCIA	1.500 € IVA incluido
Servicio de consultoría en intrusión y vulnerabilidades	3.500 € IVA incluido
Renovación Servicios económicos del Ayuntamiento	40.000 € IVA incluido
Renovación Plataforma para el Empleado del Ayto.	8.000 € IVA incluido

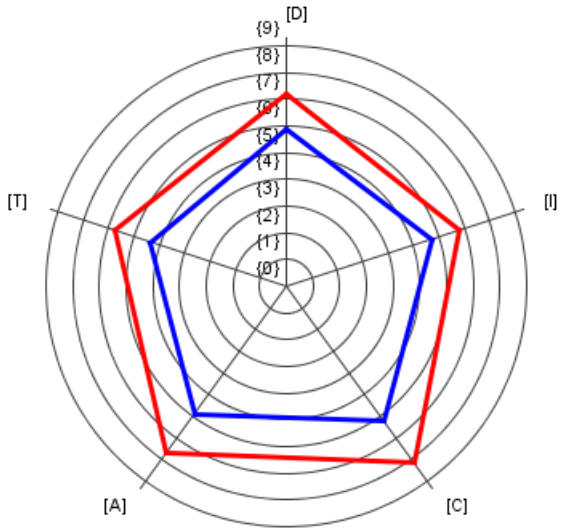
5. Propuesta de Proyectos

4) Cuantificación temporal.



5. Propuesta de Proyectos

5) Impacto esperado de los proyectos sobre la seguridad: mejora del riesgo acumulado una vez aplicados los proyectos.



[D]isponibilidad
[T]razabilidad
[C]onfidencialidad
[I]ntegridad
[A]utenticidad

ANTES
DESPUÉS

6. Auditoría de Cumplimiento

6. Auditoría de Cumplimiento

1) Evaluación de los controles y la madurez

2) Evaluación de nivel de cumplimiento ENS

3) Evaluación de nivel de cumplimiento ISO/IEC 27002:2013

4) Hallazgos ENS

5) Hallazgos ISO/IEC 27002:2013

6. Auditoría de Cumplimiento

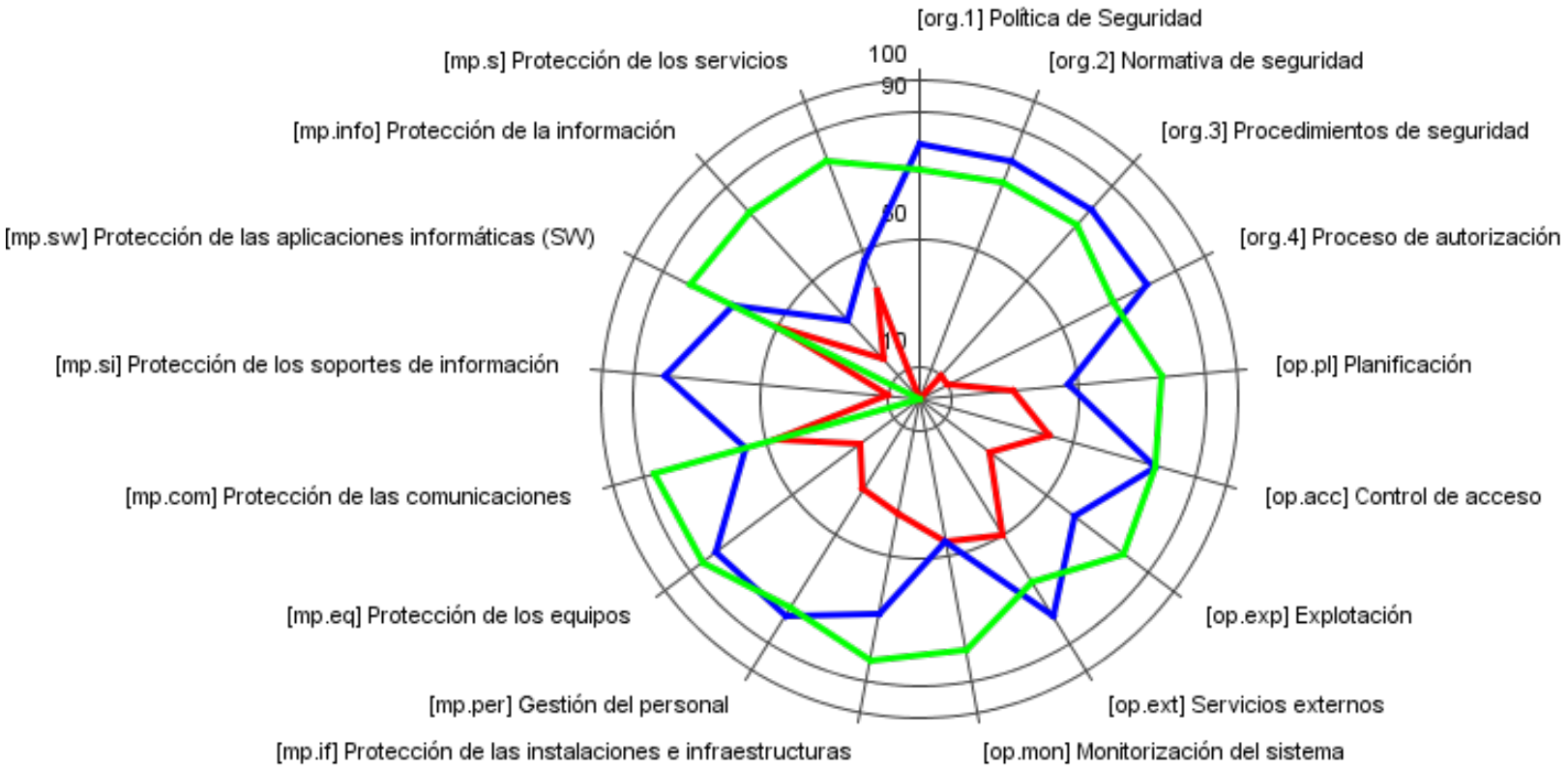
1) Evaluación de los controles y la madurez.

- ISO/IEC 27002:2013. Se analizarán un total de 114 controles o salvaguardas, descritas en la norma organizadas en 14 dominios y 35 objetivos de control.
- ENS. Se analizarán los controles o salvaguardas de los distintos marcos organizativos (org, op, mp) atendiendo a la categoría media del sistema.
- Modelo de madurez de la Capacidad:

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

6. Auditoría de Cumplimiento

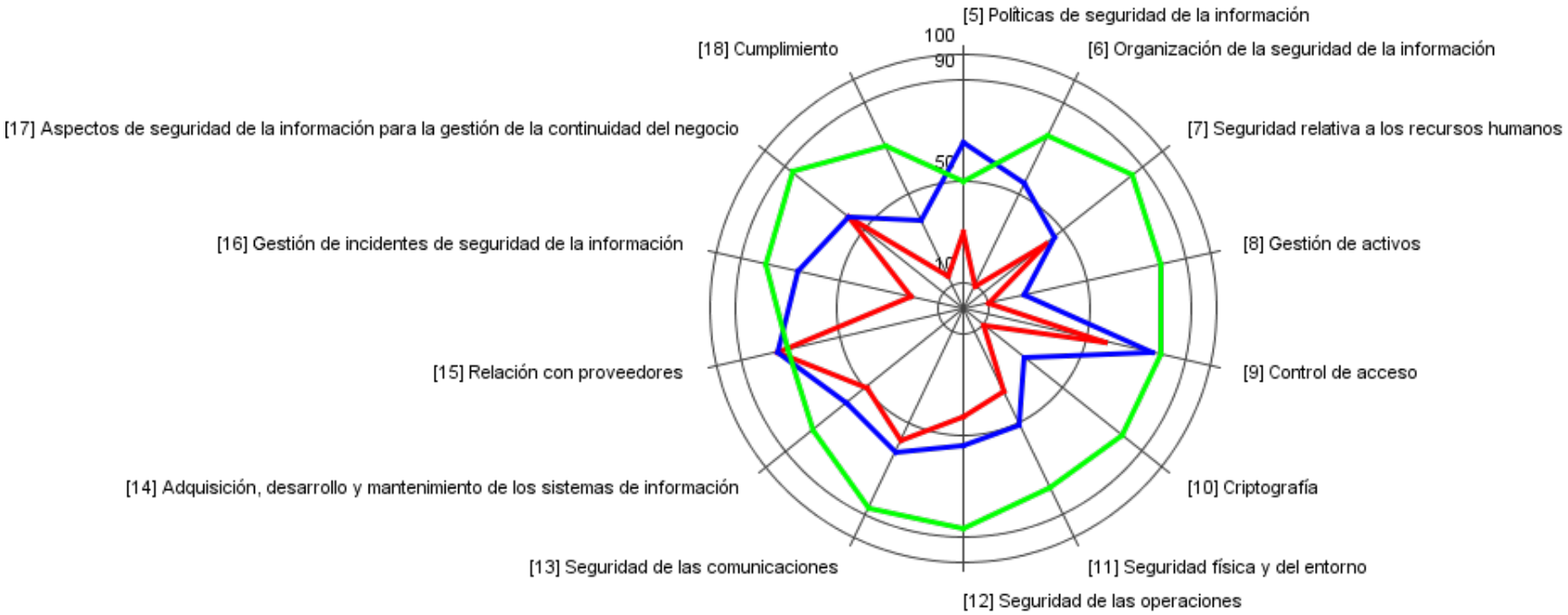
2) Evaluación de nivel de cumplimiento ENS.



En rojo la situación “Anterior”, en azul la situación “Actual” y se añade en verde la recomendación de cumplimiento hecha por la herramienta PILAR.

6. Auditoría de Cumplimiento

3) Evaluación de cumplimiento de ISO/IEC 27002:2013.



En rojo la situación “Anterior”, en azul la situación “Actual” y se añade en verde la recomendación de cumplimiento hecha por la herramienta PILAR

6. Auditoría de Cumplimiento

4) Hallazgos ENS

TIPO	NÚMERO
No conformidad MAYOR	8
No conformidad MENOR	9
Observaciones	11
Posibilidad de Mejora	2

5) Hallazgos ISO/IEC 27002:2013

TIPO	NÚMERO
No conformidad MAYOR	18
No conformidad MENOR	35
Observaciones	14
Posibilidad de Mejora	0

7. Conclusiones

7. Conclusiones

"Caminamos a hombros de gigantes"

7. Conclusiones

- Para poder implantar un Plan Director de Seguridad es necesario involucrar a toda la organización, especialmente a la Dirección.
- La figura del Responsable de Seguridad o CISO se vuelve imprescindible, cayendo sobre él la responsabilidad y el liderazgo a la hora de implantar un Plan Director de Seguridad.
- En cada ciclo Deming hacia la mejora de la SI es mejor centrarse en un único estándar (ISO 27001 o ENS).
- Las Administraciones Públicas deben empezar adecuándose al ENS aunque es recomendable tomar algunas acciones alineadas con ISO 27001 que faciliten su posterior certificación.
- La Calidad del Dato nos permitirá ahorrar esfuerzos e implantar más rápido nuestro Plan Director de Seguridad.

7. Conclusiones – Objetivos logrados

- Todos los objetivos de nuestro TFM han tenido un cierto grado de éxito a excepción de uno que ha fracasado totalmente:

"Convertir este TFM en una guía práctica de cumplimiento de ENS y Calidad del Dato aplicable a la Administración Local."

Aún queda mucho trabajo por hacer.

7. Conclusiones – Líneas de trabajo futuro

- Estudiar cómo deben llevarse a cabo los siguientes ciclos Deming ¿seguimos con el ENS o priorizamos ISO 27001?
- Realizar un Plan Director de Seguridad incluyendo los activos de telefonía (móvil y fija) y de teletrabajo.
- Desarrollar modelos para el punto 3.11 de la memoria del TFM.
- Profundizar en el uso de ISO 25012 analizando más datos.
- Estudiar como avanza en su cumplimiento ENI, RGPD y LOPDGDD al implantar ENS o ISO 27001.
- Estudiar como unificar el Plan Director de Seguridad con el Plan Estratégico de Sistemas de Información y el Plan de Actuación Municipal, aplicar un framework de gobernabilidad (Val IT).

Imagen de fondo: blogtrepreneur.com/tech

https://flic.kr/p/MhztwS Attribution 2.0 Generic (CC BY 2.0)

Plantilla LibreOffice: William Moreno Reyes

[CC-BY-SA](https://creativecommons.org/licenses/by-sa/3.0/)
[fedora-server-slideshow-template](https://fedoraproject.org/wiki/Templates_for_Presentations)

Imágenes de dominio público empleadas en esta presentación con fines docentes y de estudio

Transparencia 4:
https://upload.wikimedia.org/wikipedia/commons/thumb/7/7a/PDCA_Cycle.svg/600px-PDCA_Cycle.svg.png
Transparencia 9: https://www.emailvendorselection.com/data-security-marketing-automation-software-iso27001/
Transparencia 9 y siguientes: https://static.isms.online/wp-content/uploads/2017/07/iso-iec-27001-2013.png
Transparencia 9 y siguientes: https://www.ccn-cert.cni.es/ens.html
Transparencia 9 y siguientes: https://store.pecb.com/products/isoiec-25012-data-quality-model
Transparencia 9 y siguientes:
https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2020/Enero/Noticia-2020-01-08-10-a-os-del-Esquema-Nacional-de-Interoperabilidad.html#.X-cHFBZ7lPY
Transparencia 14:
https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia/2-uncategorised/48-adecuacion-al-ens-y-seguimiento-del-progreso.html
Transparencia 18:
https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii-jornadas-stic-ccn-cert/3440-m32-03-enfoque-unificado-para-el-analisis-de-riestos-multinorma/file.html
Transparencia 29 (imágenes de uso libre):
https://pxhere.com/en/photo/1441915
https://www.pexels.com/photo/accountant-business-calculate-chart-1808924/
Transparencia 40:
https://commons.wikimedia.org/wiki/File:Orion_aveugle_cherchant_le_soleil.jpg