Máster Universitario de Investigación en Ingeniería de Software y Sistemas Informáticos

Itinerario de Investigación en Ingeniería de Software - 31105128

Desarrollo de un marco de gestión de proyectos para el desarrollo seguro en entornos industriales de infraestructuras críticas

Alumno: Félix Antonio Barrio Juárez

Directora: Magdalena Arcilla Cobián

Curso 2015/2016 – Convocatoria Septiembre 2016

RESUMEN **5**
EXECUTIVE SUMMARY **5**
1. INTRODUCCIÓN. OBJETIVOS DEL TFM **6**
1.1 CONTEXTO E IMPORTANCIA DE LAS INFRAESTRUCTURAS CRÍTICAS 6
1.2 LAS TI Y LOS SISTEMAS DE CONTROL EN LAS ORGANIZACIONES INDUSTRIALES ESPAÑOLAS 9
1.2.1 Sistemas ICS *12*
1.3 LA SEGURIDAD DE LAS TI EN LOS ENTORNOS INDUSTRIALES DE IICC 13
1.4 INICIATIVAS Y SOLUCIONES DE SEGURIDAD TI EN IICC 18
1.5 OBJETIVOS DEL TRABAJO DE FIN DE MASTER 21
1.6 ESTRUCTURA DEL TRABAJO FIN DE MASTER 22
1.6.1 Metodología empleada *23*
2. ESTADO DE LA CUESTIÓN **24**
2.1 MARCOS, MODELOS Y NORMAS PARA LA ADMINISTRACIÓN DE PROYECTOS SEGURA PARA IICC 24
2.1.1 La gobernanza TI en infraestructuras críticas *25*
2.1.1.1 Marco regulatorio gubernamental: compliance y gobernanza TI en IICC 25
2.1.1.2 ENS 27
2.1.1.3 Programa CSSP 28
2.1.1.4 MAGERIT 28
2.1.1.5 Modelos generalistas: ISO/IEC 38500 y COBIT 29
2.1.1.6 Estudio comparativo de guías de gobernanza en entornos de IICC 29
2.1.2 Gestión de servicios TI en IICC *31*
2.1.2.1 Framework de Ciberseguridad del NIST 31
2.1.2.2 TSP Best practices 33
2.1.2.3 Modelos generalistas: ISO/IEC 20000 e ITIL 33
2.1.2.4 Estudio comparativo de guías de gestión de servicios en IICC 35
2.1.3 Mejora de procesos *37*
2.1.3.1 Programa de Evaluación CSEP 37
2.1.3.2 CMMI 38
2.1.3.3 ISO/IEC 15504 39
2.1.3.4 Estudio comparativo de guías de ciclo de mejora de procesos en IICC 39
2.1.4 Gestión de Proyectos *40*
2.1.4.1 Métodos Generalistas: PMBOK O PRINCE 41
2.1.4.2 MÉTRICA V3 42
2.1.4.3 Metodologías Predictivas 42
2.1.4.4 Metodologías Adaptativas 43
2.1.4.5 Estudio comparativo de guías de gestión de proyectos 44
2.1.5 Gestión de Seguridad *45*
2.1.5.1 NERC CIP 46
2.1.5.2 NRC - RG 5.71 48
2.1.5.3 CFATS 50
2.1.5.4 PCI DSS 53
2.1.5.5 ISA/IEC 62443 54
2.1.5.6 Industrial Control System (ICS) Cyber Security: Recommended Best Practices 55
2.1.5.7 ISREC Catalogue 56
2.1.5.8 CSPN 56
2.1.5.9 ISO/IEC 27000 56
2.1.5.10 Security by Design with CMMI-DEV 58
2.1.5.11 ISO/IEC15408 / Common Criteria 58
2.1.5.12 Metodologías de Análisis de Riesgo 58
2.1.5.13 Estudio comparativo de guías de seguridad 59
2.2 REVISIÓN SISTEMÁTICA 63
2.2.1 Objetivos de la revisión *63*
2.2.2 Resumen de resultados *65*

2.2.3 Consideraciones finales de la revisión sistemática *69*
2.3 RESULTADOS DEL ESTADO DEL ARTE 70
3. PLANTEAMIENTO DEL PROBLEMA E HIPÓTESIS DE TRABAJO 73
3.1 VISIÓN GENERAL DEL PROBLEMA 73
3.2 APROXIMACIÓN A LA SOLUCIÓN 74
3.3 HIPÓTESIS DEL TRABAJO 75
4 RESOLUCIÓN 77
4.1 INTRODUCCIÓN 77
4.2 RESOLUCIÓN DEL PROBLEMA 77
4.2.1 Estandarización y definición del modelo. *78*
4.2.2 Modelo estándar de proceso para la administración segura de proyectos de tecnologías de la información en IICC *79*
4.2.1.1 Fase I. Inicio y Dirección 80
4.2.1.1.1 I. A1. Declaración de la política de seguridad 80
4.2.1.1.2 I. A2. Definición de prerrequisitos de seguridad 82
4.2.1.1.3 I. A3. Planificación y comunicación 83
4.2.1.2 Fase II. Definición de Requisitos de Seguridad 84
4.2.1.2.1 II. A1. Clasificación de activos 84
4.2.1.2.2 II. A2 Definición del catálogo de requisitos de seguridad 85
4.2.1.2.3 II. A3 Definición de requisitos de monitorización del catálogo 87
4.2.1.3 Fase III. Definición de Requisitos de Seguridad 88
4.2.1.3.1 III. A1. Gestión de Riesgos TI 88
4.2.1.3.2 III. A2. Implementación de la Solución 89
4.2.1.3.3 III. A3. Diseño del procedimiento de monitorización de la solución 90
4.2.1.4 Fase IV. Monitorización 91
4.2.1.4.1 IV. A1. Definición del procedimiento de monitorización y recuperación 91
4.2.1.4.2 IV. A2. Revisión de los activos de seguridad 92
4.2.1.4.3 IV. A3. Emisión de informes 93
4.2.1.5 Fase V. Revisión y Mejora 94
4.2.1.5.1 V. A1. Revisión del estado actual 94
4.2.1.5.2 V. A2. Planificar y comunicar el plan de mejora 95
5. EXPERIMENTO 96
5.1 METODOLOGÍA EXPERIMENTAL. 96
5.2 CASO DE ESTUDIO 96
5.3.1 Contexto de caso *96*
5.3.2 Establecimiento de la línea base *98*
5.3.2.1 Resultados Línea Base Inicial 100
5.3.2.2 Conclusiones Línea Base 101
5.3.3 Definición del patrón del proyecto *103*
5.3.3.1 Inicio y Dirección *105*
5.3.3.2 Definición de requisitos de seguridad *106*
5.3.3.3 Diseño e Implantación de la Solución de Seguridad *110*
5.3.3.4 Monitorización de los Activos de Seguridad *112*
5.3.3.5 Mejora Continua del Proyecto de TI seguros *114*
5.3.4 Resultados de la línea final *116*
5.3.6 Comparación resultados líneas inicial y final *119*
5.3.7 Conclusiones *120*
6. APORTACIONES, CONCLUSIONES Y LÍNEAS FUTURAS 121
6.1 INTRODUCCIÓN 121
6.2 CONCLUSIONES 121
6.3 LÍNEAS FUTURAS DE TRABAJO 122

ANEXO I. PREGUNTAS VALIDACIÓN INICIAL Y FINAL **124**
ANEXO II. RESULTADOS DE VALIDACIÓN INICIAL Y FINAL **135**
II.I CUESTIONARIO INICIAL LABORATORIO DE IICC 135
II.II CUESTIONARIO FINAL LABORATORIO DE IICC 138
ANEXO III. POLLTLCA DE SEGURIDAD DOCUMENTO **143**
ANEXO IV. MANUAL DE SEGURIDAD **145**
ANEXO V. ORGANIGRAMA DEL LABORATORIO IICC **153**
ANEXO VI. CATÁLOGO DE ACTIVOS DE SEGURIDAD **157**
ANEXO VII. PLAN DE CONTINGENCIA Y DISPONIBILIDAD **161**
BIBLIOGRAFÍA **165**
ÍNDICE DE FIGURAS **173**
ÍNDICE DE TABLAS **174**

Resumen

Este Trabajo Fin de Master pretende diseñar, desarrollar e implantar un Modelo de Gestión de Seguridad Industrial en los proyectos de Tecnologías de la Información y Comunicaciones en entornos de infraestructuras críticas.

A partir del análisis del estado del arte referente a los sistemas de Gestión de Seguridad para entornos industriales, con especial atención en lo referente a protección de Infraestructuras Críticas, nuestro Trabajo de Fin de Master (TFM) pretende resolver la necesidad de crear un marco parcial de gestión de proyectos de desarrollo de servicios TIC que responda a los principales modelos y marcos normativos de calidad y seguridad.

La creciente exposición a vulnerabilidades y riesgos en el ámbito de la ciberseguridad, supone un alto riesgo para los responsables de estas organizaciones catalogadas como entornos industriales y de infraestructuras críticas, consideradas imprescindibles para el correcto funcionamiento de la sociedad y la economía de un país.

El primer objetivo de este TFM apuntar un marco versátil que oriente los proyectos para el desarrollo seguro y continuidad posterior de la seguridad de los servicios de TI en entornos industriales de infraestructuras críticas. El segundo objetivo es desarrollar un modelo de aplicación genérica que incluya prácticas generalizables y una catalogación de activos de seguridad que ayude a las organizaciones con infraestructuras críticas en las tareas de desarrollo seguro de proyectos de TI.

Executive Summary

This Master Thesis aims to design, develop and implement a management model for Industrial cyber security related to ICT projects in critical infrastructure companies and organizations.

Starting with the analysis of the state of the art concerning systems security management for industrial environments, with special attention regarding critical infrastructure protection, our Master Thesis aims to solve the need to create a partial framework for ICT project management developments to meet the main models and regulatory frameworks for quality and cyber security.

Increasing exposure to vulnerabilities and risks in the field of cyber security represents a high risk for those responsible at these organizations classified as industrial environments of critical infrastructure, considered essential for the proper functioning of the society and the economy of a country.

The first objective of this TFM is provide a versatile framework to guide projects for subsequent safe development and continuity of the security of IT services at critical infrastructure industrial environments. The second objective is to develop a generic model application that includes generalizable practices and to catalogue security assets to help organizations with critical infrastructure to develop IT projects in a securely approach.

1. Introducción. Objetivos del TFM

El tema que nos ocupa en este Trabajo Fin de Master es la gestión de la seguridad en los proyectos de Tecnología de la Información y Comunicaciones (TIC o TI), dentro del contexto de las Infraestructuras Críticas. Así, el objetivo de este primer capítulo es mostrar el contexto organizativo que nos ocupa, las TI en este tipo de instalaciones y los proyectos TI afrontados, y la problemática actual en cuanto a la capacidad de este tipo de organizaciones para abordar la gestión de la seguridad en sus proyectos TI, a nivel de los parámetros de confidencialidad, integridad y disponibilidad que necesitan la información y sus sistemas. conforme a un marco regulatorio que les exige una conformación específica de los mismos. El capítulo concluye exponiendo los objetivos del Trabajo Fin de Master y resumiendo la estructura de este Trabajo.

1.1 Contexto e importancia de las infraestructuras críticas

Las organizaciones que constituyen infraestructuras consideradas por la autoridad de un Estado o territorio como críticas pueden ser tanto empresas como instituciones, privadas como públicas, pasando a ser sometidas bajo una tutela que, además de fines de protección, conlleva un objetivo más profundo como es el de asegurar la continuidad de los servicios públicos que aseguran la normalidad en la vida cotidiana de una sociedad. La legislación viene definiendo en consecuencia que la protección y tutela alcanza el conjunto de activos, sistemas y redes (físicas o virtuales) vitales para un país o territorio, cuya incapacitación o destrucción debilitaría la seguridad en general, la seguridad económica, la salud nacional, y en general lo que la tradición anglosajona diferencia bajo los epígrafes de *security* y *safety*, entendiendo esta última en una dimensión de seguridad más "física". El objetivo es asegurar la continuidad de negocio en estas organizaciones asegurando la prestación de servicios y el mantenimiento de sus operaciones críticas, incluso en el caso de que se produzca un ciberataque, aunque no sólo en este caso (Sanders, 2012: p. 19), matiz que resulta muy importante porque estamos trascendiendo el concepto de defensa.

Las infraestructuras críticas (IICC o en terminología anglosajona CIKR-*Critical Infrastructure and Key Resources*[1]) se enmarcan dentro de un concepto más amplio que es el de las infraestructuras de interés estratégico para una sociedad o Estado, o simplemente infraestructuras estratégicas. Una clasificación típica de las denominadas infraestructuras estratégicas comprende tres grandes grupos o bloques (Álvarez Fernández, 2016):

1. Infraestructuras críticas: imprescindibles para la sociedad y la economía, sin posibilidad de reemplazo ni discontinuidad dado el riesgo de grave afectación social y económica.
2. Infraestructuras esenciales: aquellas cuya destrucción o interrupción pueden producir daños importantes a la sociedad.

[1] https://www.oig.dhs.gov/assets/Mgmt/OIG_09-95_Aug09.pdf

3. Infraestructuras complementarias: aquellas cuya destrucción o interrupción pueden producir daños moderados a la sociedad.

El carácter privado o público de estas infraestructuras varía según los países en los que se encuentren. En el caso español la mayoría son empresas privadas aunque fuertemente reguladas. Los sectores públicos y privados a los que pertenecen las infraestructuras críticas incluyen entre doce y dieciocho sectores agregados, establecidos en los diferentes marcos de regulación estatal. En el caso español, los doce sectores en los que se agrupan los denominados operadores estratégicos son doce (Dunn, & Abele-Wigert 2006; Álvarez Fernández, 2016):

- Administración
- Alimentación
- Energía
- Espacio
- Sistema Financiero y Tributario
- Agua
- Industria Nuclear
- Industria Química
- Instalaciones de Investigación
- Salud
- Tecnologías de la Información y las Comunicaciones
- Transporte

El Real Decreto 704/2011 que establece el Reglamento de Protección de Infraestructuras Críticas[2] considera que podrían ascender a más de 3.500 instalaciones.

En los Estados Unidos, los sectores se clasifican en dieciocho grupos, y añaden grupos como la minería o el desarrollo de software educacional. Se aprecia una sobrerrepresentación del sector energético, que representaría en torno al 23% del total de operadores norteamericanos a tenor del estudio realizado en 2013 por el *Sans Institute* (Luallen, 2013).

Cabe destacar que la sectorización no impide que una infraestructura crítica pueda pertenecer a más de un sector a la vez, ya que las propias instalaciones de la industria nuclear en gran medida se incluirían en el sector energético, mientras que el subsector tributario pertenece asimismo al sector Administración pública.

Debido al carácter confidencial que tienen este tipo de infraestructuras resulta difícil extraer datos exactos sobre el número y distribución de estas entidades, que pueden ser clasificadas como tales dependiendo del criterio del gobierno. Aun así no resulta difícil adivinar que dicha condición la comparten grandes infraestructuras como las instalaciones de producción energética, aeropuertos y grandes terminales de transportes,

[2] BOE núm. 121 de 21 de mayo de 2011.

sistemas de aprovisionamiento de agua, servicios sanitarios, financieros y diversos sectores industriales que proporcionan servicios de comunicaciones, de producción y distribución alimentaria o la industria química.

A la vista de la creciente preocupación por la seguridad de este tipo de infraestructuras, instalaciones y servicios, se deriva que durante los próximos años se va a generar un nuevo y creciente mercado global, a nivel de prestaciones de seguridad a servicios ya desarrollados así como para proteger infraestructuras que se consideran clave para la sociedad civil. De hecho, en este TFM se mostrará cómo en la última década la regulación y la aplicación de ingeniería de seguridad en entornos de infraestructuras críticas se ha desarrollado notablemente a nivel mundial, especialmente en lo que a seguridad física se refiere, mientras que los aspectos relacionados con la seguridad TI en estos entornos, se encuentra más rezagada.

Por otro lado, el hecho de que todavía resulte incipiente la experiencia del sector tecnológico en el planteamiento de proyectos de ingeniería en ciberseguridad en IICC se debe a dos motivos principales:

a) La regulación sobre política y estrategia en ciberseguridad en entornos de TI, como la que por ejemplo regula el Esquema Nacional de Seguridad en España se ha aplicado fundamentalmente en el sector público.

b) El Plan Nacional de Protección de Infraestructuras Críticas (PNPIC) y la EU's Internal Security Strategy (ISS) son aproximaciones a la protección de infraestructuras completamente nuevas en Europa y, por tanto, no existen antecedentes, y en ambas la regulación en materia de protección de las TI aún resulta más tímida e incipiente, en favor de la protección física.

En definitiva, se está generando una nueva demanda para la que además no existen históricos desde la ciberseguridad, como se constata en el estudio de mercado sobre "Tendencias en el mercado de ciberseguridad" desarrollado por INCIBE (2016), y que resume las principales tendencias tecnológicas a nivel mundial distribuidas en seis áreas. La primera de éstas corresponde al Sector Industrial y Medio Ambiente y contempla 3 tendencias de actualidad, relacionadas con el desarrollo de la ciberresiliencia en las IICC, en primer lugar, seguida de la *Ciberseguridad aplicada en los llamados Sistemas de Control* Industriales, particularmente relacionados con las tecnologías ICS y *SCADA*, así como la securización de las denominadas *Smart Grids.*

En consecuencia se que afectan al conjunto de la industria tanto en los operadores críticos como en la industria proveedora de servicios y soluciones de seguridad, como es la industria TIC, son las siguientes:

a) Desarrollar metodologías adaptadas a cada tipo de servicio y tipo de infraestructura.

b) Automatizar la prestación de seguridad, suprimiendo esfuerzos adaptativos para cada nuevo proyecto que surja.

c) Identificar "buenas prácticas de implantación".

d) Innovar en materia de prevención, investigación y combate respecto a las amenazas de seguridad en las IICC.

En definitiva se concluye que el entorno de las infraestructuras críticas industriales tendrá en los próximos años un importante protagonismo en el desarrollo de un mercado de ciberseguridad.

1.2 Las TI y los sistemas de control en las organizaciones industriales españolas

Para poder realizar una aproximación al estado del arte de las TI en entornos de IICC, necesitamos comprender la realidad de los sectores industriales estratégicos de la economía, ya que estas organizaciones comparten con el resto de la industria la situación de desarrollo tecnológico y exposición a riesgos que es común al conjunto del sector.

De acuerdo al Directorio Central de Empresas (DIRCE), que elabora anualmente el INE, el número total de empresas en España ha alcanzado en 2015 las 3.186.878, un 2,2% más que en el año 2014 (ONTSI, 2016). El sector de empresas industriales se sitúa como el sector con más representación dentro de las empresas con 10 o más empleados en España, un 21,3% y, se lo sumamos a los sectores de Transporte y almacenamiento y al de Informática, Telecomunicaciones y Audiovisuales, alcanza un total del 32,4% del total del sector empresarial español que no constituye las llamadas "microempresas" de menos de 10 empleados.

Resulta patente que el nivel de desarrollo tecnológico en las organizaciones industriales crece a un nivel exponencial, constituyendo una de las tendencias tecnológicas más pujantes, por efecto de la apertura de estos entornos a Internet y las nuevas tecnologías, en lo que se ha dado en llamar *Industria 4.0.* alusiva a la penetración digital en la industria (INCIBE, 2016).

Según datos del Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (ONTSI, 2016) perteneciente al Ministerio de Industria, Energía y Turismo, en su Informe "e-Pyme 2015-Análisis sectorial de implantación de las TIC en la empresa española", un análisis intersectorial de la implantación y uso de las TIC en los diferentes sectores empresariales, se analiza específicamente el grado de adopción de las herramientas y servicios tecnológicos utilizados por las empresas españolas. De este modo en 2015, considera que se puede hablar de universalización de la TI en el tejido empresarial e industrial español.

Sólo en el segmento de las microempresas (1-9 empleados) no existe el 100% de informatización empresarial, de extensión de telefonía móvil o acceso a Internet, con sectores como el transporte y almacenamiento donde sólo el 54,4% disponen de computadoras. En los teléfonos móviles, la universalización también es completa, aunque con una penetración menor, de nuevo, del 76,5% en el caso de las microempresas, y en el acceso a Internet, también se limita en este segmento al 68% de los casos. No obstante, a nivel general aún resulta incipiente la adopción de estrategias de ciberseguridad: el 37% de las pymes y grandes empresas y el 10,1% de las microempresas cuentan con política de seguridad TIC definida. El 65,8% de las primeras y el 61,2% de las segundas la han revisado en los últimos doce meses.

En lo relativo al sector industrial, los subsectores afectados por la clasificación de IICC se encuentran particularmente representados, aunque finalmente el número de operadores designados es mucho menor en términos unitarios, se van a corresponder sin embargo

con las grandes instalaciones energéticas, metalúrgicas, químicas, alimentarias y de transporte en un país. En la Figura 1.1. se aprecia la distribución por cada uno en España en la actualidad:

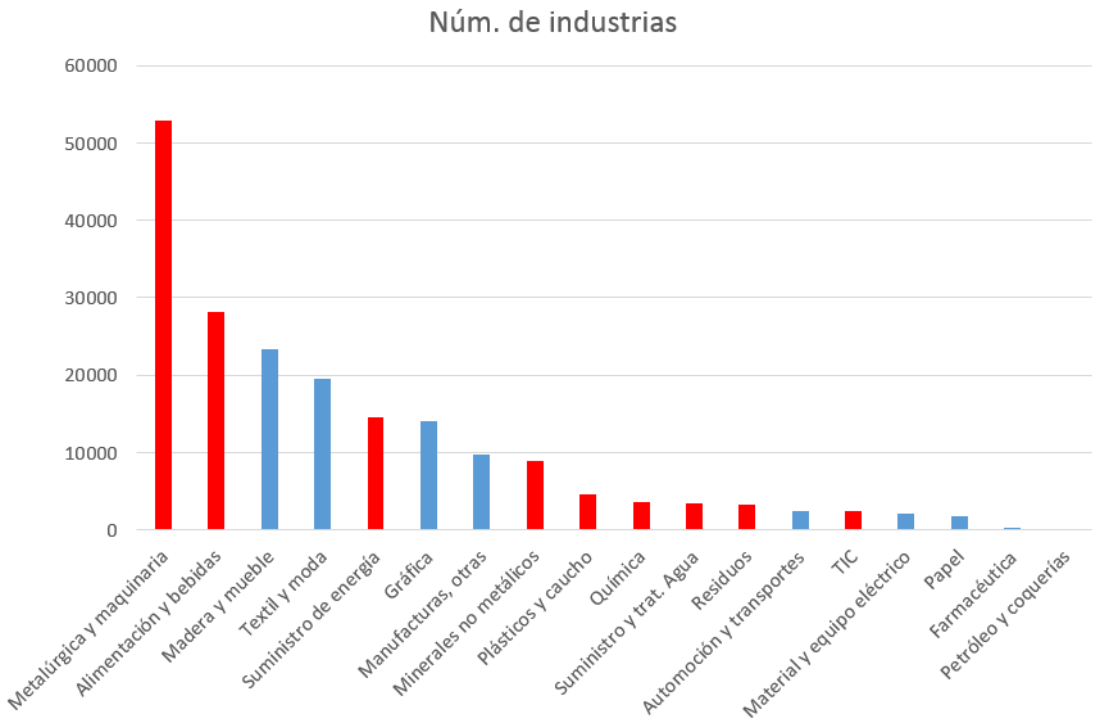


Figura 1.1. Número de empresas por subsector industrial en España, 2015. En rojo los 11 subsectores afectados por la clasificación de IICC en un grado significativo. Fuente: Elaboración propia en base a DIRCE 2015, INE (ONTSI, 2016)

Respecto a la penetración de Internet, tanto en las pymes como en las grandes empresas del sector industrial la penetración se mantiene estable, con porcentajes superiores al 97% ya en 2014, disponiendo de conexión a Internet cuenta con acceso de banda ancha fija o móvil en 2015 el 97,9%. El principal servicio ofrecido por las empresas a través de sus páginas web continúa siendo la presentación de la empresa (90,3% de las pymes y grandes empresas y el 75,7% de las de menos de diez trabajadores), seguida del cumplimiento de la legislación de privacidad y la certificación relacionada con la seguridad de la web (65,5%). En tercer lugar aparece el acceso a catálogos y listados de precios (37,7% en el caso de las micropymes y el 56,7% de las pymes y grandes empresas.

La universalización TI de los sectores industriales también se evidencia en la penetración de las tecnologías de movilidad: el porcentaje de pymes y grandes empresas que proporciona a sus empleados dispositivos portátiles con conexión a Internet para uso empresarial en el sector industrial sigue aumentando, pasando del 53,5% en 2014 al 64,6% de 2015. El 47,4% de las pymes y grandes empresas facilita a sus empleados dispositivos como portátiles, tabletas o netbooks y el 57,6% smartphones o PDA. Esto supone unos incrementos respecto a 2014 de 13,5 puntos y 9,2 puntos porcentuales, respectivamente. Por parte de las microempresas, su implantación es inferior, aunque en

2015 ha crecido el porcentaje de empresas que facilitaron dispositivos como las tabletas, portátiles o netbooks y las que facilitaron PDA o smartphones.

En el ámbito del software corporativo, el 44,5% de las compañías de 10 o más empleados dispone de herramientas informáticas ERP para gestionar sus procesos de negocio, un 36,7% dispone de herramientas CRM para gestionar información sobre clientes, y el uso de herramientas software de código abierto asciende al 64,7% de las microempresas y al 82,9% de las pymes y grandes empresas. Los principales tipos de software siguen siendo los navegadores de Internet y las aplicaciones ofimáticas.

También resulta destacable que se hayan universalizado los intercambios electrónicos vía trámites con la Administración en el sector industrial: el 91,8% de las pymes y grandes empresas y el 66,5% de las empresas de menos de diez trabajadores interactuaron en 2014 con la Administración a través de Internet.

En lo que a penetración de las redes sociales se refiere en estos ámbitos industriales, el 27,3% de las microempresas y el 33,9% de las pymes y grandes compañías las utilizaron en 2015. Los medios sociales en las compañías de 10 o más empleados cuentan con redes sociales (91,6%), websites que comparten contenido multimedia (40,7%), seguidas de los blogs (36,2%).

En 2015, solo el 13% de las compañías industriales de 10 o más empleados y el 2,2% de las de menos de 10 trabajadores han recurrido a algún servicio de cloud computing. Las soluciones más adquiridas entre las pymes y grandes empresas son los servicios de correo electrónico (66,9%), el almacenamiento de ficheros (61,8%) y servidores de bases de datos (52,7%). En menor medida se contratan capacidad de computación, aplicaciones de software financiero o contable y las aplicaciones para tratar información sobre clientes.

El 24% de las pymes y grandes empresas del sector realizó compras por medio del comercio electrónico en 2014, porcentaje que, entre las microempresas, se redujo al 10,3%, siendo los canales habituales las páginas web o aplicaciones móviles, utilizadas por el 23%. La compra a través de mensajes tipo EDI[3] la realizó el 3,1% de las pymes y grandes y el 1,5% de las microempresas.

Por último, en lo relativo a la formación en TIC en 2015 en el sector industrial, el 21,4% de las pymes y grandes empresas la proporcionaron a sus empleados. Entre las microempresas solo lo hicieron el 3,9%.

Se aprecia en el informe del Ministerio de Industria cómo son materias cada vez más importantes para la industria, en el desarrollo de las TIC, tanto la ciberseguridad como el establecimiento de políticas adecuadas que permitan asegurarla. El 35,2% de las pymes y grandes empresas y el 9% de las empresas de menos de 10 empleados disponen de este tipo de política, mientras que el 87,7% las pymes y grandes empresas que ya cuentan con una política de seguridad TIC definida, afirman haber tratado riesgos sobre destrucción de datos por ataque o incidentes inesperados, el 78,7% lo ha hecho sobre revelación de datos confidenciales y el 67% sobre la falta de disponibilidad de servicios TIC por ataques externos.

[3] Sistema automatizado de intercambio de información electrónica mediante "documentos electrónicos estructurados" conforme a un estándar predefinido y programable. Este sistema permite un flujo continuado de transacciones entre dos empresas.

1.2.1 Sistemas ICS

Los sistemas de control de proceso (*Process Control Systems* o PCS) son sistemas complejos que ejecutan tareas definidas como parte de un proceso de producción industrial y, en particular, son considerados como el entorno principal de control para otras infraestructuras críticas (Alcaraz, Fernández y Carvajal, 2012: 120). Estos sistemas monitorizan y supervisan sensores remotos desplegados junto a la infraestructura crítica, gestionando operaciones automatizadas y almacenando mediciones de datos sensibles. En la literatura existente existen tres tipos diferenciados de PCS, en función de su distribución topográfica (IBM, 2007):

- Sistema SCADA. Controlan la supervisión y toma de datos (*Supervisory Control and Data Acquisition*) y son una red distribuida en un área territorial amplia donde un conjunto de servicios de automatización industrial se despliegan para controlar el rendimiento y la continuidad de otras instalaciones tales como producción y distribución energéticas, suministradoras, potabilizadoras o depuradoras hídricas, gestión de basuras, químico-farmacéuticas, transportistas (NIST, 2008).
- Sistemas de Control Distribuido (*Distributed Control Systems* o DCS). El control en este caso está repartido geográficamente, ubicándose en diferentes instalaciones donde se encuentran desplegados los elementos controlados, a modo de un conjunto de sistemas SCADA locales, actuando como un único sistema de monitorización sin punto de control central.
- Sistemas basados en *Programmable Logic Controllers* (PLC). Controladores lógicos programables, son en esencia sistemas SCADA de tamaño y complejidad reducidos.

Para Rodríguez Penin (2007) un SCADA es cualquier sistema que monitoriza y/o gestiona de forma centralizada y en tiempo real un conjunto de dispositivos finales. La figura 1.2, muestra la disposición funcional elemental de un SCADA y se articula en combinaciones de bucles de control que actúan como sensores, transmisotes o motores, junto a interfaces hombre-máquina que permiten ejercer el control y monitorización y utilidades que permiten diagnosticar y mantener de forma remota la funcionalidad de los sistemas (Barrio y Ramos, 2012):

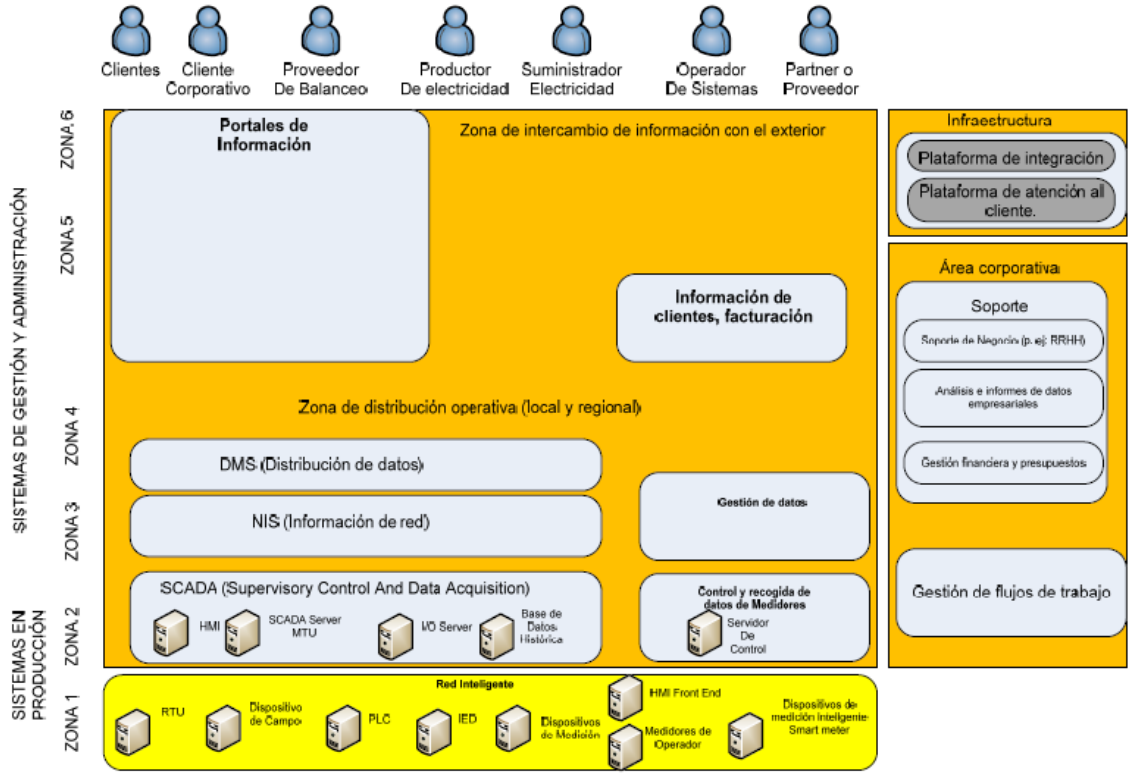


Figura 1.2. Esquema de funcionamiento de un sistema SCADA (Fuente: Barrio y Ramos, 2012)

Las tecnologías SCADA (Supervisory Control and Data Acquisition) son, por lo tanto, una pieza fundamental de los sistemas de control industrial empleados para la gestión de instalaciones que tienen la consideración de infraestructuras críticas y, por tanto, objetivo principal de los ciberataques, gracias también a la tendencia reciente de dotar a estos sistemas de mayores mecanismos de comunicación con otro tipo de sistemas, incluso a través de Internet.

1.3 La seguridad de las TI en los entornos industriales de IICC

Aunque la preocupación por la seguridad y la prevención de la discontinuidad de servicios de interés público como pueden ser los transportes, el abastecimiento alimentario, hídrico y energético, y diversos servicios básicos, han sido preocupaciones básicas para los responsables públicos desde los orígenes de las sociedades humanas, la aparición del concepto seguridad de la información (en adelante, SI) en las infraestructuras estratégicas se remonta a finales del siglo XX.

Es en 1982, durante el conflicto ruso-americano cuando se registra un primer episodio de ataque cibernético a una infraestructura crítica, mediante la creación de un troyano destinado a sabotear los sistemas informáticos de gestión de los gaseoductos soviéticos (Villalón, 2011: p.4). Pero es a finales de la década de 1990 cuando se conecta a Internet un amplio repertorio de sistemas informáticos que, hasta la fecha, habían permanecido aislados, el momento en que se comienzan a repetir intentos de penetración y ataque a los

mismos, dándose la situación de que pocos habían previsto las consecuencias de inseguridad derivadas de la conexión remota que ofrecía Internet. En el año 2000 se registra un ataque a una central de tratamiento de aguas residuales por parte de un ex-empleado que accede de modo inalámbrico al sistema (Villalón, 2011). En 2003 el gusano Slammer ocasiona el apagado de la central nuclear norteamericana de Davis-Besse (Poulsen, 2003).

El siguiente hito en las amenazas de malware en sistemas de control industrial se corresponde con el gusano Stuxnet, detectado en 2010 y documentado ampliamente en diversos estudios, que ataca sistemas software de la empresa alemana Siemens espiando y reprogramando controladores lógicos programables (Chien, 2010). Para la multinacional de seguridad Kaspersky, se trata del primer caso de guerra cibernética real y diferentes analistas consideran que esto explicaría el hecho de que el 60% de los terminales atacados se ubicasen en Irán, así como el posible boicot al programa nuclear iraní (Falliere et al., 2011).

En la actualidad, el registro de incidentes de ciberseguridad relacionados con infraestructuras críticas se produce prácticamente con carácter diario en cualquier economía desarrollada. El nivel de riesgo y criticidad de la exposición a amenazas se ha incrementado en la medida en que la exponencial aparición de usuarios malintencionados explotan las posibles vulnerabilidades de los sistemas TI de dichas infraestructuras. Así, a comienzos de mayo de 2016 una infección por ramsonware afectó a un proveedor local de agua y luz en el estado norteamericano de Michigan (Trendmicro, 2016), y ese mismo mes la central nuclear alemana de Gundremmingen detectaba varios equipos afectados por los virus W32.Ramnit y Conficker (BBC, 2016).

La ciberguerra también ha situado los ataques cibernéticos a infraestructuras críticas en la lista de prioridades en un ataque bélico, normalmente con carácter previo al despliegue de un ataque armado, o simplemente como represalias ante conflictos internacionales, como parece suceder en el caso del ataque mediante spear-phising que sufrió una factoría siderúrgica alemana en 2014, en plena crisis entre Rusia y la Unión Europea por el conflicto ucraniano, ataque que ocasionó un fallo en un termostato y cuyos enormes daños paralizaron la producción de acero en dicha factoría durante semanas (Paganini, 2014).

A diferencia de estos ataques, todavía son minoritarios los que se basan en el desarrollo de malware específicamente desarrollado para entornos de software particulares de Infraestructuras críticas. Un caso es el del malware Havex[4], empleado en el ataque identificado como “Dragonfly” o “Energetic Bear”, que disponía de una funcionalidad que le permitía buscar y encontrar sistemas de control industrial en distintos puertos de conexión, así como un módulo específico para comunicaciones OPC (Open Platform Communications) utilizadas habitualmente por este tipo de sistemas. En 2007 aparecía el denominado malware Blackenergy versión 2, que afectó a una central eléctrica ucraniana atacaba a los productos ELTIMA Serial to Ethernet Connector o ASEM Ubiquity, utilizados en sistemas de control industrial. Sobre esta inicial versión se han desarrollado nuevas versiones del malware.

La situación de estos entornos, desde el punto de vista del Instituto Nacional de Ciberseguridad (Firvida, 2016), estaría caracterizada por la dependencia de este tipo de

[4] https://scadahacker.com/resources/havex.html

entidades hacia sistemas IT tradicionales, así como por la poca visibilidad que tendrían las redes industriales dado su tradicional aislamiento, a nivel de los IDS o antivirus, ya que al estar desconectados de la red, en muchos casos no se reporta a los fabricantes la incidencia de modo que no es posible el análisis de falsos negativos que permitan identificar nuevas amenazas.

Además tradicionalmente el objetivo de los ciberdelincuentes se ha centrado en atacar grandes conjuntos de posibles víctimas, por lo que las infraestructuras industriales como tales no han sido la prioridad si exceptuamos los ciberterroristas o como objetivos militares. En este sentido, las estadísticas de incidentes nos revelan que el malware más frecuente se dirige al robo de datos con fines lucrativos ilícitos, principalmente datos bancarios o de medios electrónicos de pago, que son los preferidos del malware tipo ramsonware o de las redes botnet. Consecuentemente son los sistemas operativos más populares y extendidos como Windows o Android los asimismo elegidos por los desarrolladores de malware, mientras que sistemas operativos más frecuentes en los entornos de sistemas y redes industriales, tales como Unix o Linux, están infrarrepresentados en el ranking de sistemas operativos más atacados a nivel global.

En tercer lugar, según INCIBE la propia idiosincrasia de los sistemas de software de control industrial supone una dificultad adicional para los desarrolladores de malware, pues se requiere un cierto nivel de conocimiento sobre la ingeniería de software específica y sobre procedimientos de función del sistema industrial, de los cuales los atacantes suelen carecer en modo suficiente.

Cabría añadir que la minusvaloración por parte de los responsables TI de las organizaciones, de su nivel de exposición al riesgo, se refuerza precisamente por el tradicional aislamiento y lo incipiente del desarrollo de tecnologías y conectividad en los entornos de infraestructuras críticas.

En la actualidad se combina la mayor apertura de los sistemas de control industrial a las redes abiertas y la mayor conectividad de los dispositivos en un par de vectores de aceleración de la exposición a terceros posibles atacantes, pero multiplicando la exposición a vulnerabilidades y amenazas. En consecuencia, los desarrolladores de malware disponen de más incentivos para desarrollar productos específicos para los sistemas de control industrial.

En la conferencia *Black Hat Asia* de 2016, una investigación de la compañía *OpenSource Security* sobre un gusano diseñado para sistemas PLC de la gama Siemens S7-1200 mostró cómo el procedimiento de detección e infección de víctimas se ejecuta desde los propios PLC mediante la carga en origen del malware en un primer PLC, bien a través de un PC comprometido o distribuyendo un PLC manipulado, para posteriormente seguir una pauta de contagio a terceros PLC con la emulación de las órdenes del software TIA-Portal. Esta simulación mostró la vulnerabilidad específica de protección de escritura en el PLC y llevó a Siemens a poder desarrollar un parche ad hoc. Una segunda investigación desarrollada por la compañía FireEye en junio de 2016 y presentada en la conferencia S4xEurope mostró evidencias de un tipo de malware para sistemas de control industrial subido a *VirusTotal* en 2014 que en su momento había sido desapercibido por los fabricantes de antivirus. El malware tenía semejanzas con Stuxnet pero se había adaptado a entornos de simulación industrial, concretamente para Siemens PLCSIM, y su modus operandi permitía realizar ataques *man-in-the-middle* a procesos de entrada y salida de datos mediante el reemplazo de una librería de software por otra maliciosa, a la vez que

incorporaba técnicas para evasión de *sandboxing* de modo que no se pudiera detectar si se ejecutaba en entornos *VMWare* o con *Cuckoo*. El hecho de que los investigadores no detectaran la explotación de la vulnerabilidad en ningún producto Siemens les llevó a la conclusión de que podía tratarse de un ejercicio de prueba de concepto o de una investigación para desarrollar malware de ataque a sistemas de control industrial de otro tipo.

Para Firvida (2016) las recientes investigaciones sobre el malware específico en sistemas de control industrial muestran un nivel de complejidad tal que los asemeja a buena parte de las características de una APT. Requieren, en este sentido, una aplicación de recursos de investigación, conocimiento e interés por alcanzar objetivos muy concretos en el ataque, siendo la mayor diferencia que no persiguen como fin último el robo de información, manteniendo la impunidad y el desconocimiento de los atacados en lo posible, sino que su propósito es alterar el normal funcionamiento de objetivos industriales dañando la infraestructura de modo que el atacado perciba claramente la agresividad y potencial de su enemigo. Firvida presupone que se require el respaldo de una estructura o aparato de Estado detrás de este esfuerzo y lo alinea con una típica acción de ciberguerra, y considera inminente que las redes criminales comiencen a utilizar malware específico para ICS con fines de extorsión al estilo del uso de *ramsonware*.

Cabría añadir que las redes criminales podrían prestar sus capacidades delictivas a los Estados con fines de ciberguerra, por no mencionar que en los conflictos bélicos contemporáneos a menudo la estructura de aparatos de Estado es sustituida por movimientos políticos o sociales que desarrollan operaciones bélicas y terroristas, por lo que su análisis dual Estado/redes criminales no resulta útil para describir las cada vez más complejas tipologías de atacantes que pueden desarrollar o utilizar malware dirigido con infraestructuras críticas. En otras palabras, si bien es cierto que la complejidad de un ataque a ICS requiere de unos recursos y organización sofisticados de la que disponen los departamentos de ciberdefensa o ciberguerra, otras organizaciones criminales, activistas, terroristas o paramilitares pueden adquirir el conocimiento y la capacidad suficientes para intentar explotar las vulnerabilidades de los sistemas ICS con diferentes propósitos tales como la extorsión, el boicot o la exhibición de sus capacidades.

En un estudio realizado por el Sans Institute entre 700 empresas norteamericanas pertenecientes a alguno de los dieciocho sectores de IICC señalados en el U.S. National Infrastructure Protection Plan (NIPP), se constató que es creciente la conciencia entre las empresas respecto a los riesgos que pueden asumir los sistemas SCADAs , de modo que dos terceras partes lo califican como crítico o alto mientras que un tercio de las encuestadas sospechaban ser víctimas de incidentes de seguridad cibernética (Luallen, 2013):

En el tercer estudio de Sans Institute desarrollado en 2015 (Harp & Gregory-Brown, 2015), un 32% de los 314 operadores encuestados afirmó que sus activos o redes del sistema de control habían sido víctimas de una infiltración y un 34% habrían sufrido alguna brecha de seguridad en los últimos 12 meses, y un 44% de estos reconocieron ser incapaces de identificar la fuente de la infiltración.

En consecuencia, la demanda de productos, servicios y sistemas que mantengan sistemas de información (SSII) seguros y que contribuyan eficazmente a mantener la seguridad integral de las infraestructuras críticas es creciente. Para ello las organizaciones deben aplicar un enfoque con el máximo rigor que le permita gestionar, evaluar y mejorar la

seguridad de los proyectos TI a abordar y obtener, con ellos, productos y servicios con la garantía y seguridad adaptada a las necesidades de la propia infraestructura crítica.

En este marco van a surgir los SGSI o sistemas que permiten la gestión de la SI. Para las IICC, disponer de estos sistemas de gestión evita la improvisación en la adopción de prácticas.

La securización en los sistemas industriales estarán condicionadas por su entorno y deberán adaptarse a la legislación sobre protección de IICC en cada caso, precisando de equipos robustos y de la redundancia o duplicidad de sus elementos críticos, de forma que si el elemento original sufre un fallo de funcionamiento, el sustituto pueda realizar las funciones.

En el plano de las TIC, la seguridad física aún tiene un grado de dependencia funcional media de las mismas, pero los avances en control perimetral, de accesos y monitorización, así como la generalización de los sistemas de conexión inalámbricos la han desarrollado exponencialmente.

Se advierten más disparidades entre los distintos sectores de IICC, aunque se ha popularizado el cifrado de las comunicaciones y la estrategia de capas de protección tanto en el área de equipos de campo, telemétricos como de acceso y control remotos tal que posibiliten por ejemplo informar de la interrupción del suministro eléctrico en un tramo de ferrocarril, o la detección y alerta sobre objetos extraños en una vía de tráfico terrestre. En la *Figura 1.3* Solomon diferencia los grados de dependencia de las TIC según el tipo de sector IICC.

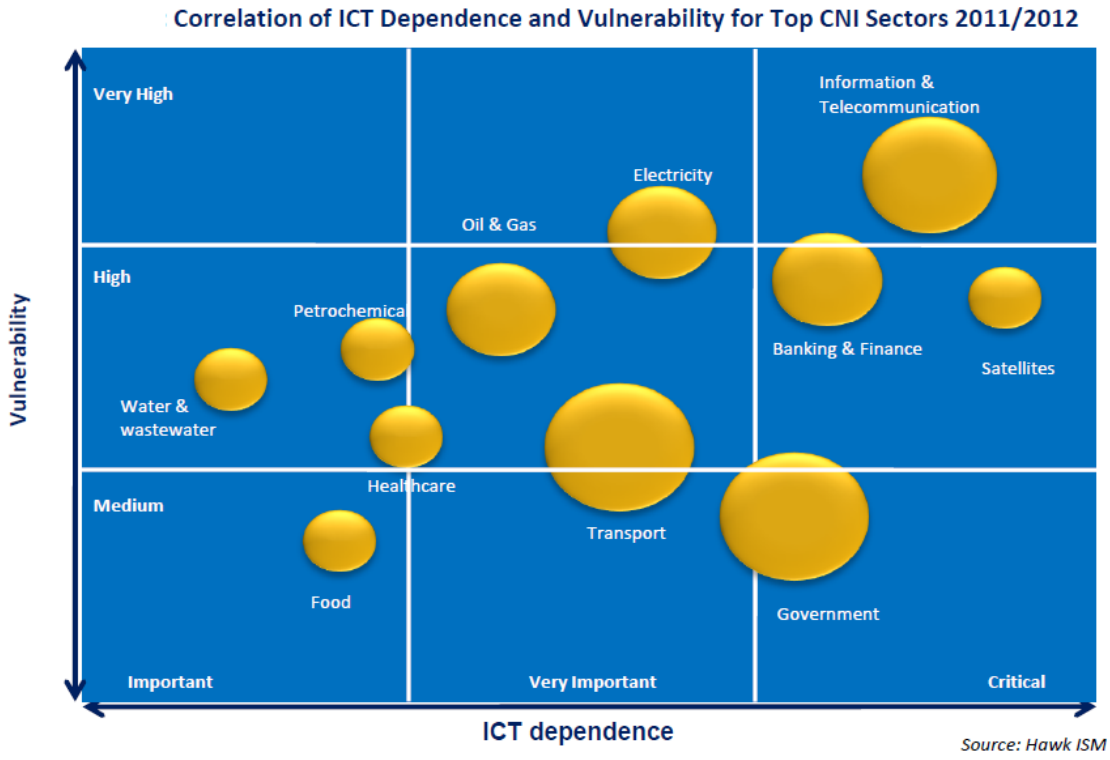


Figura 1.3. Correlación entre la dependencia de las TIC y la vulnerabilidad mostrada por los principales sectores de IICC 2011-2012 (Fuente: Solomon, 2011)

Para un mayor detalle sobre sistema de securización de entornos SCADA conforme al marco legal de securización de las IICC, en el caso español aplica la reglamentación específica desarrollada para cada sector en el marco del Plan Nacional de protección de IICC. En Barrio y Ramos (2012, pp. 176-207) se incluye una descripción de la aplicación de medidas de securización en sistemas SCADA aplicable a un modelo común.

En el presente Trabajo Fin de Master analizaremos sintéticamente algunos marcos y estándares reconocidos internacionalmente y que, desde diferentes perspectivas, permiten a las IICC la adopción y gestión de sus respectivos SGSI.

1.4 Iniciativas y soluciones de seguridad TI en IICC

En el ámbito de Europa, el ataque terrorista de Madrid en marzo de 2004 llevó al Consejo Europeo dos meses después a solicitar a la Comisión Europea que preparase una estrategia sobre protección de infraestructuras críticas. El 20 de octubre de 2004 la Comisión emitía la *Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo*, proponiendo mejoras en la prevención, preparación y respuesta frente a ataques terroristas. En diciembre el Consejo ponía en marcha el PEPIC (Programa europeo de protección de infraestructuras críticas) y una red de alerta en IICC (*Critical Infrastructures Warning Information Network*-CIWIN), y la Directiva comunitaria 2008/114/CE conminaba a elaborar una norma nacional que en España constituiría el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) como órgano de asistencia al Secretario de Estado de Seguridad y responsable de la coordinación del sistema.

España se alineaba con el marco normativo europeo aprobando la Ley 8/2011, de 28 de abril[5], por la que se establecen medidas para la protección de las infraestructuras críticas y del Reglamento para la Protección de Infraestructuras Críticas. La Ley 8/2011, el Esquema Nacional de Seguridad, así como la EU's Internal Security Strategy (ISS) son por lo tanto los exponentes de una estrategia española y europea común para la protección de servicios e infraestructuras estratégicos, alineada con estos otros elementos reguladores:

- La suscripción española del Convenio Internacional sobre Cibercrimen del Consejo de Europa[6].
- Los Esquemas Nacionales de Seguridad y de Interoperabilidad para las administraciones públicas.
- La Agenda Digital para Europa que establece la estrategia europea para la economía digital de cara al año 2020[7], y que es una de las siete iniciativas para el desarrollo económico de la UE, mediante la articulación de políticas públicas que permitan crear un mercado digital único, aumentar la interoperabilidad, impulsar

[5] http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630

[6] http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm

[7] https://ec.europa.eu/digital-single-market/en/europe-2020-strategy

la confianza y la seguridad en internet, y otros objetivos planteados hasta el año 2020.

- La Agenda Digital para España, que refleja la estrategia de la Agenda Digital europea planteando una estrategia general aplicada al ámbito nacional, bajo liderazgo del MINETUR[8].
- El desarrollo de la Estrategia Española de Seguridad, de la cual se deriva la Estrategia Española de Ciberseguridad Nacional, liderada por el Ministerio de Presidencia[9].

La Ley 8/2011 considera **operador crítico** las organizaciones que detentan, son propietarias o asumen la operatividad cotidiana de una infraestructura considerada crítica. Estos tienen la obligación de diseñar y aplicar Planes de Seguridad del Operador y otros de Protección Específicos, así como reportarlos al CNPIC cada dos años o cada vez que sufran cambios significativos. La norma cataloga las IICC y articula un Plan Nacional de Protección bajo coordinación del Ministerio del Interior.

En general, se puede concluir que el desarrollo reglamentario de indicaciones para diseñar y establecer planes específicos de protección para cada sector estratégico de la industria está claramente enfocado a dar solución a la gestión integral de seguridad.

Pero para poder cumplir con las disposiciones reglamentarias, es preciso disponer de guías y protocolos de actuación que faciliten la implantación concreta de medidas de protección a nivel de gestión integral y de TI.

Estas reglamentaciones constituyen una hoja de ruta estándar a la que las organizaciones pueden ajustarse razonablemente, y se basan en marcos, estándares y guías, de referencia internacional, entre las que se incluirían las siguientes principales:

- La familia de estándares de seguridad TI ISO 27000.
- Los estándares, y marcos de gobierno y gestión de servicios TI como ISO 38500, ISO 20000, COSO, NIST, COBIT, GAISP o la guía de buenas prácticas para la gestión de servicios de ITIL.
- Los marcos de mejora de procesos como CMMI o SPICE (ISO/IEC15504-7, 2008), o la guía de gestión de proyectos de seguridad descrita por la Carnegie Mellon University (SEI, 2013) y modelos generalistas de gestión de proyectos como los de PMI.
- Modelos como el desarrollado por el SEI (Siemens, 2013), que y su marco de trabajo "Security by Design" cuyo objetivo es la mejora de los procesos que generan productos y servicios TI seguros.

Además, la necesidad de recurrir a SCADA en los entornos industriales va a condicionar especialmente el recurso a estándares específicos. En el estudio del Sans Institute se obtuvo como resultado que las normas más comúnmente usadas por los operadores críticos en Estados Unidos (Luallen, 2013) incluyen la guía del NIST *Guide to SCADA*

[8] http://www.agendadigital.gob.es/Paginas/Index.aspx

[9] http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

and Industrial Control Systems Security [10] (40%), seguida del modelo 20 Critical Security Controls[11] (34%) y del NERC CIP12 (30%), tal como se muestra en la *figura 1.4.*

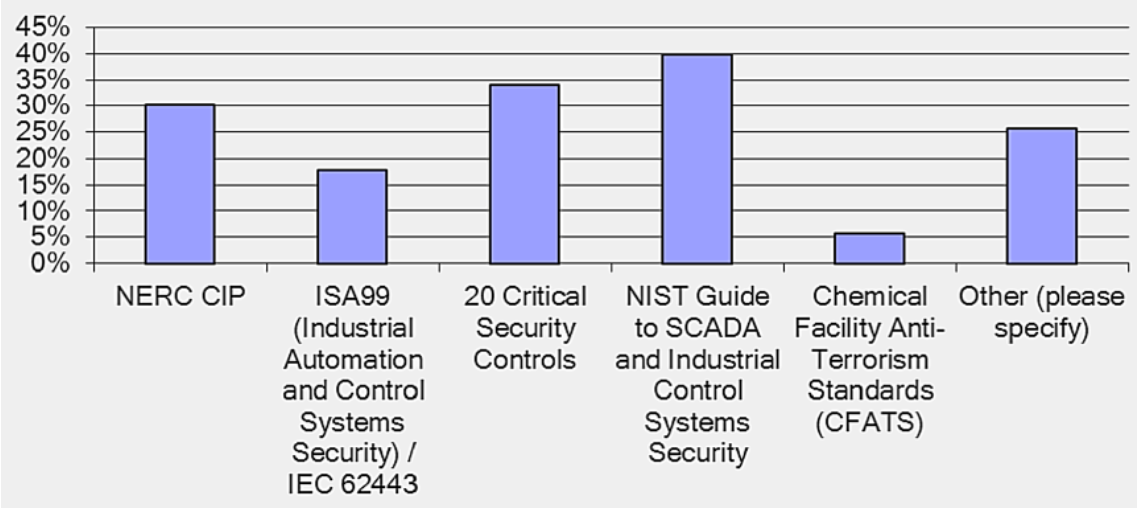


Figura 1.4. Principales estándares utilizados por los operadores de IICC en Estados Unidos (Fuente: Luellen, 2013: p. 11)

Sin embargo, en el contexto de las de las infraestructuras críticas, todos ellos son muy difíciles de implantar, requiriendo por lo habitual una inversión especialmente alta, por lo que encontraremos disparidad de grados de implantación. En sectores como el TIC, el nuclear o el financiero, la normativa y la experiencia desarrollada durante décadas permite disponer de completos y eficaces SGSIs, mientras que, opuestamente, podemos encontrar organizaciones de sectores como el transporte o la salud que tienen una más reciente trayectoria de desarrollo de SGSIs normalizados. Mientras que los operadores que son oriundos del sector TIC tienden a tener muy desarrollada en su cultura de negocio la gestión TI, ya que están familiarizados con la ciberseguridad, sin embargo la mayoría de los operadores estratégicos, que incorporan mecanismos de control industrial, tradicionalmente han centrado su mayor preocupación en la seguridad física, y se encuentran una fase de preparación progresiva para acometer suficientemente la seguridad lógica.

La práctica totalidad de los marcos normativos y guías de protección sólo proponen las actividades a realizar y no aportan detalles de cómo deben ser aplicadas. Esto se debe, en parte, a la necesidad de que tengan un carácter genérico que permita homogeneizar las prácticas a desarrollar entre organizaciones y sectores de IICC muy diferentes entre sí, por lo que el legislador y los organismos reguladores establecen guías de buenas prácticas que no descienden a casos de uso detallados.

Por todo lo anterior, en el capítulo 2 de este trabajo de fin de master se revisarán modelos y guías de mejores prácticas propuestas específicamente para la gestión de seguridad en los SSII y sus proyectos en infraestructuras críticas. Se analizarán las aportaciones en

[10] http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[11] http://www.sans.org/critical-security-controls/

[12] www.nerc.com/page.php?cid=2%7C20

relación a la gestión de seguridad de estos marcos y se reflejarán las carencias más importantes en el contexto de las IICC.

1.5 Objetivos del Trabajo de Fin de Master

Como se ha mostrado en el apartado anterior, a pesar de los numerosos marcos, estándares y guías, reconocidas internacionalmente, que abordan la gestión de la SI oganizativamente, la realidad demuestra que, para las IICC aún supone un reto el poder alcanzar un nivel óptimo en todos y cada uno de los doce sectores que las componen, debido principalmente a los siguientes factores:

- Muchos de los entornos organizaciones de IICC han permanecido tradicionalmente aislados de las redes de comunicación o con una relativamente baja implantación de TI en sus procesos.

- El relativo aislamiento ha podido facilitar en los responsables de seguridad de las IICC una minusvaloración de la creciente exposición a riesgo que suponen los avances tecnológicos.

- Muchas de las organizaciones consideradas como IICC requieren de una inversión que en ocasiones puede resultar difícil de acometer.

- La propia especificidad de la seguridad TI de las IICC hace que sea especialmente difícil mantener actualizadas las medidas de protección sin una correcta adopción de un SGSI.

- El desarrollo normativo impulsado por las autoridades gubernamentales a nivel internacional y dentro de cada país resulta desigual y no siempre se dispone de guías de actuación suficientemente adaptadas y detalladas a los requerimientos de seguridad TI que se necesitan en cada sector de IICC.

Dada la amplitud que requiere la gestión de la seguridad en las IICC, este Trabajo Fin de Master considera las áreas de proceso establecidas en el marco descrito por Siemens (2013). La investigación se centra en definir prácticas de seguridad en los proyectos y cómo “Definir las actividades y las técnicas relacionadas con proyectos de desarrollo de seguro en entornos industriales de infraestructuras críticas”. Los objetivos secundarios planteados son:

1. Realizar un estudio del estado actual de la gestión de la SI en las IICC a través del análisis de los marcos, modelos, metodologías, estándares y guías de mejores prácticas actuales de gestión de la SI y (b) la revisión sistemática de la literatura en relación con las experiencias llevadas a cabo en IICC y que analicen la implantación e influencia de los marcos, modelos y estándares de gestión de SI en la mejora de los procesos.

2. Establecer una base de activos para el proceso de administración de SI en los proyectos de donde se obtendrán los distintos componentes del proceso a aplicar.

3. Definir un patrón para administrar SI en procesos TI y que incluya una guía que ayude a seleccionar los activos adecuados para la gestión y estructurarlos en el proceso a través del patrón definido.

4. Validar el marco propuesto a través de la aplicación de un conjunto selectivo de buenas prácticas en proyectos sobre IICC e identificar las oportunidades de mejora.

1.6 Estructura del Trabajo Fin de Master

En primer lugar, se realiza un análisis sobre los requerimientos de la Gobernanza TI en entornos de IICC y cómo la función de *compliance* condiciona la adopción de modelos de gestión de seguridad industrial.

En segundo lugar y de modo general, se revisa el panorama normativo y científico sobre los modelos de gestión de Seguridad Industrial a nivel internacional nos permite extraer buenas prácticas y experiencias sobre las que plantear una solución al desarrollo seguro en dichos entornos.

En tercer lugar, analizaremos de modo específico los Modelos Sectoriales utilizados en los Estados Unidos para regular la protección de las infraestructuras de las organizaciones en materia de Ciberseguridad y que son los siguientes:

- De modo preliminar, y a partir del trabajo de De la Cámara (2016) sobre factores relativos a la administración de proyectos de SI, en los siguientes sub-apartados se hace una introducción de los estándares y marcos más representativos en gestión segura de la TI, que asimismo son los más extendidos en el conjunto del mundo empresarial y de las organizaciones, por supuesto también las de carácter industrial y las IICC.
- En segundo lugar, se hará referencia al estándar NERC CIP, que el Gobierno Federal ha establecido de obligado cumplimiento, para las compañías relacionadas con el subsector eléctrico de la alta tensión.
- El Modelo NRC - RG 5.71, utilizado por la comisión que regula los aspectos nucleares, como requisito para poder operar las plantas nucleares en USA.
- El estándar CFATS, que tiene el objetivo de identificar y proteger las instalaciones químicas de alto riesgo que se consideran posibles objetivos de un ataque terrorista.
- En quinto lugar se analizará un modelo considerado relevante, de entorno diferente al industrial, como es el estándar de seguridad PCI-DSS, de obligado cumplimiento para las entidades que disponen de sistemas que almacenan, procesan o transmiten datos de tarjetas de pago.
- En sexto lugar, se analizará el alcance del Framework de Ciberseguridad definido recientemente por el NIST.
- Por último se parte de las prácticas propuestas de Seguridad por Diseño (Siemens, 2013), para la gestión proyectos de desarrollo aplicable en IICC.

Posteriormente, para la validación del marco se ha elegido un entorno experimental de infraestructura crítica.

1.6.1 Metodología empleada

Siguiendo a Arnold (1998) y el hecho de que toda observación científica significa una forma de comparación de similitudes y aspectos diferentes para la interpretación de una realidad, se marca en este TFM el objetivo de recabar terceras perspectivas sobre modelos y marcos de administración de la SI en las IICC.

Hay que resaltar que mientras que desde un enfoque tradicional el objeto a estudiar sería la seguridad en la gestión del desarrollo, desde la perspectiva sistémico/constructivista interesan las terceras visiones.

En conclusión, este Trabajo Fin de Master se encuentra organizado en un conjunto de siete capítulos cuyos contenidos se describen brevemente a continuaciónn

Tabla 1.1 Estructura del Trabajo Fin de Master

CAPÍTULO	**DESCRIPCIÓN**
1. Introducción	Se describe el contexto de las IICC y la problemática actual de este tipo de organizaciones en relación con la administración de proyectos de desarrollo seguros de TI.
2. Estado de la cuestión	Ser realizan una descripción y análisis de los marcos, guías, metodologías, y estándares actuales, más relevantes y relativos al proceso de administración de la SI en IICC, así como una revisión de la literatura científica.
3. Planteamiento del problema e hipótesis de trabajo	Se plantea el problema detectado de los estudios anteriores. Se introduce el proceso de solución propuesta y las hipótesis de trabajo.
4. Resolución	En este capítulo se detalla un marco de prácticas para la administración de proyectos de desarrollo seguro en las IICC. Se describen las actividades, las técnicas y la guía de implantación para facilitar el proceso.
5. Experimentación	Se verifica la aplicación del marco sobre proyectos de IICC, analizando la mejora en administración de SI en proyectos en IICC, a través de la medición de indicadores de éxito, antes y después de la aplicación del marco,m en orden a aceptar/rechazar las hipótesis del TFM.
6. Conclusiones y Líneas Futuras de Investigación	Reflexiones arrojadas por el estudio y una propuesta de líneas de investigación derivadas de este Trabajo de Fin de Master.
7. Bibliografía	Bibliografía asociada a este Trabajo de Fin de Master.

2. Estado de la cuestión

Se describen los distintos marcos, modelos, metodologías y estándares actuales, más relevantes y relativos a la administración de la SI particularmente el estudio de la administración de proyectos segura en el entorno de las infraestructuras críticas (IICC).

2.1 Marcos, modelos y normas para la administración de proyectos segura para IICC

Se abordan los marcos y estándares de mejores prácticas, reconocidos internacionalmente, que desde los niveles de estrategia, táctica y de operaciones, facilitan la administración segura en proyectos en las IICC.

Nivel	**Perspectiva (factores de SI)**
Estratégico	Gobernanza: evaluación-dirección-monitorización
Táctico	Gestión y mejora de servicios (áreas de procesos y buenas prácticas)
Operativo	Gestión de proyectos (métodos, procesos y buenas prácticas) Gestión de seguridad

Tabla 2.1 Marcos y normas involucrados en la administración segura de proyectos de desarrollo

Para cada uno de los referidos marcos o estándares de mejores prácticas genéricas De la Cámara (2016) realiza una revisión de los factores relativos al desarrollo seguro, a partir de un análisis de los aspectos más relevantes, resaltando aquellos encaminados a la gestión de proyectos segura. Este conjunto de marcos, guías y modelos se identifican como modelos de referencia considerados relevantes para el objetivo de este trabajo, aunque específicamente no son referentes a la protección de las IICC y a los entornos industriales.

Por ello este Trabajo Fin de Master se centra específicamente con la revisión de los siguientes esquemas normativos desarrollados para entornos industriales de IICC:

1) Los Modelos Sectoriales utilizados en los Estados Unidos para regular la protección de las infraestructuras de las organizaciones en materia de Ciberseguridad, tales como el estándar NERC CIP, que el Gobierno Federal ha establecido de obligado cumplimiento, para las compañías relacionadas con el subsector eléctrico de la alta tensión; el Modelo NRC - RG 5.71, utilizado por la comisión que regula los aspectos nucleares, como requisito para poder operar las

plantas nucleares; el estándar CFATS, que tiene el objetivo de identificar y proteger las instalaciones químicas de alto riesgo que se consideran posibles objetivos de un ataque terrorista.

2) Un Modelo considerado relevante, de entorno diferente al industrial. En concreto, se trata del estándar de seguridad PCI-DSS, de obligado cumplimiento, para las entidades que disponen de sistemas que almacenan, procesan o transmiten datos de tarjetas de pago.
3) El Framework de Ciberseguridad definido recientemente por el NIST.

2.1.1 La gobernanza TI en infraestructuras críticas

La Gobernanza Corporativa es el conjunto de procesos por el que el órgano de gobierno de una organización garantiza la consecución de los fines corporativos, así como la seguridad de sus activos y valores para sus grupos de interesados (clientes, usuarios internos, accionistas, administraciones), quienes deben recibir información transparente de su administración y procedimientos de control (OCDE, 2004). Desde el punto de vista de los procesos de administración (management) la norma ISO/IEC 38500 define la Gobernanza como el *sistema de procesos y controles requerido para la consecución de los objetivos estratégicos establecidos por el cuerpo de gobierno de la organización* (ISO 2008).

En cuanto a la Gobernanza corporativa TI, es el sistema de utilización de las TI dirigiéndolas y controlándolas de modo que presten apoyo a la organización y se evalúe en todo momento su uso en orden a la consecución de los planes. Incluye la estrategia y políticas para utilizar TI dentro de la organización, la gestión del activo Información y TI en la organización y la gestión del riesgo asociado con TI.

La gobernanza TI forma parte de la Estrategia de la Gobernanza Corporativa y en los entornos de IICC viene especialmente determinada por las obligaciones normativas que establecen las autoridades gubernativas en cada país.

La necesidad de ajustar la gobernanza corporativa y de la TI en las infraestructuras críticas a la legislación y normativa gubernamental, ha provocado que la labor de conformidad con dicha normativa o "*compliance*" se integre en el código genético de la gobernanza de tales organizaciones.

En consecuencia se hace preciso revisar analíticamente las implicaciones de los marcos regulatorios que a nivel internacional y nacional aplican la gobernanza TI en entornos de IICC y la incidencia que tienen los modelos normativos y estándares más extendidos en el mundo industrial a nivel de gobernanza.

2.1.1.1 Marco regulatorio gubernamental: compliance y gobernanza TI en IICC

Los marcos gubernamentales más desarrollados en el ámbito de ciberseguridad e IICC corresponden a Estados Unidos y Europa, aunque cabe realizar alguna referencia a países específicamente avanzados en el punto de vista legal como Reino Unido o Canadá, a cuyos modelos normativos se hará posterior referencia en el análisis.

Estados Unidos

Como es tradicional en el ámbito del liderazgo tecnológico mundial que ha ejercido Estados Unidos, dicho país ha sido el pionero en abordar la gestión de las infraestructuras críticas. Primeramente identificadas como objetivo potencial terrorista en la *Presidential Decision Directive U. S. Policy on Counterterrorism"* en 1995, y en 1998 en las directivas "Combatting Terrorism" y "Protecting America's Critical Infrastructures", al referirse al soporte informático de las IICC.

En dependencia del Dpto. de Homeland Security destacan dos divisiones que trabajan en materia de protección de Infraestructuras Críticas:

- La división National Cyber Security Division (NCSD), responsable de mejorar la seguridad y la resiliencia de las infraestructuras tecnológicas y de las comunicaciones de los EEUU.
- La *Office Infraestructure Protection* (OIP), que dirige y coordina los programas y las políticas sobre la protección de IICC.

En este sentido, una de las funciones de la OIP ha sido definir el Plan Estratégico de Infraestructuras Críticas (National Infrastructure Protection Plan), que establece los sectores aplicables a las infraestructuras críticas, existiendo para cada uno de ellos un plan específico: químico, instalaciones comerciales, comunicaciones, manufacturas, defensa industrial, servicios de emergencia, energía, servicios financieros, alimentos y agricultura, gobierno, salud, tecnología, reactores nucleares, materiales y sector residuos.

Dentro de esta sectorización destacan:

- El sector energía, en el que la comisión Federal Energy Regulatory Commision (FERC) es el organismo que tiene la jurisdicción sobre los aspectos más importantes dentro del sector energético en USA: tarifas eléctricas, licencias hidroeléctricas, tasas de gas natural y oleoductos.
- El sector nuclear, en el que la comisión Nuclear Regulatory Commission (NRC) es el organismo encargado de otorgar las licencias para poder operar plantas nucleares en USA.
- El sector químico, en el que la oficina OIP es la responsable de identificar y proteger las instalaciones químicas de alto riesgo que se consideren posibles objetivos de un ataque terrorista.

Por último, existen distintas organizaciones u organismos no gubernamentales que destacan en materia de seguridad de las IICC y entornos industriales como la International Society of Automation (ISA), la International Electrotechnical Commission (IEC) para la normalización en los campos eléctrico y electrónico; y el ISA Security Compliance Institute (ISCI) que es un consorcio industrial formado a partir del Automation Standards Compliance Institute (ASCI), para desarrollar especificaciones y procesos de los productos de sistemas de control industrial.

Como referente legal de primer nivel cabe destacar *Federal Information Security Management Act (FISMA* (NIST, 2007), una ley de 2002 bajo el Título III de la Ley de Gobierno Electrónico, cuyo fin es proporcionar SI y de los sistemas que soportan los procesos de negocio y activos empresariales, incluyendo los proporcionados o

gestionados por otras agencias, proveedores, o cualquier otra fuente. La ley también encomendó al NIST crear las normas SP-800 a modo de marco para la gestión de la SI, obligatorio para las agencias gubernamentales, (NIST, 2010). En la guía se proporcionan recomendaciones técnicas de prácticas para el diseño, implementación, mantenimiento, pruebas de seguridad, y evaluar una posible vulnerabilidad o la verificación de políticas y prácticas (Scarfone, Souppaya, & Cody, 2008).

A nivel de investigación, cabe destacar como centro de referencia el *Center for Sensed Critical Infrastructure Research* (CenSCIR) de la Carnegie Mellon University[13].

Unión Europea

En el ámbito europeo, la Directiva 2008/114/CE del Consejo Europeo, de 8 de diciembre de 2008, estableció la designación de IICC en la UE, estableciendo la obligatoriedad de realizar una evaluación de sus necesidades de seguridad, por lo que, a través de su transposición, disponía las bases para que todos los Estados miembros habilitasen una regulación nacional en esta materia. La Agencia Europea para la Seguridad de la Información (ENISA)[14] establece en su *National Cyber Security Strategies* como objetivos estratégicos respecto a la regulación de la gobernanza en IICC (Falessi et al., 2012) la definición de un marco normativo en cada Estado miembro, consistente en políticas, planes y recursos, clasificación de las IICC, gestión de riesgos y concienciación pública sobre su importancia, así como la necesaria colaboración entre organismos a nivel intracomunitario.

Por su parte, el *Programa Europeo de Protección de Infraestructuras Críticas* (PEPIC) establece los procedimientos para identificar y designar las IICC, así comouna red de alerta –*Critical Infrastructures Warning Information Network* (CIWIN), y la creación de grupos de trabajo. También facilita nuevos medios de financiación comunitaria.

2.1.1.2 ENS

El Real Decreto 3/2010, de 8 de enero, regula inicialmente el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, constituyéndolo una obligación para todas las administraciones públicas que ofrezcan servicios electrónicos (e- Administración) en España. Esta implantación obligatoria de un conjunto de procedimientos, actuaciones técnicas, estándares y normativa que garanticen los servicios a ciudadanos y organizaciones se planteó siguiendo la familia de normas ISO 27000.

---

[13] http://www.ices.cmu.edu/censcir/

[14] La agencia European Network and Information Security Agency (ENISA) es la agencia que trata los aspectos en referencia con la seguridad de la información y las redes en la Unión Europea, y la conforman sus Estados Miembros y distintas organizaciones del sector privado. ENISA trabaja para desarrollar recomendaciones y buenas prácticas en seguridad de la información. Ayuda a los Estados Miembros de la Unión Europea en la aplicación de la legislación pertinente y trabaja para mejorar la seguridad de las Infraestructura Críticas Europeas: https://www.enisa.europa.eu/

Sus elementos principales son los requisitos mínimos de SI en las AAPP, categorizando sus activos y estableciendo 75 medidas de seguridad distribuidas en cuatro para el ámbito organizativo, 31 para el operacional (31) y otrtas 40 medidas de protección específica.

El ENS establece asimismo instrucciones sobre auditorías de cumplimiento.

2.1.1.3 Programa CSSP

El NCSD ha creado el *Control System Security Program* (CSSP), que tiene el objetivo de orientar y reducir el riesgo en los sistemas de control industrial, coordinando conjuntamente a las áreas del gobierno y a las empresas privadas, siempre bajo coordinación de la estrategia nacional estadounidense para protección de IICC coordinada por el DHS, el *National Infrastructure Protection Plan* (NIPP).

CSSP proporciona guías pero también permite reducir el riesgo en los sistemas de control de IICC mediante las siguientes funciones:

- Conducir la Estrategia de Aseguramiento de los Sistemas de control como parte de la misión general para coordinar y liderar el ciclo de mejora continua.
- Gestionar y operar el Grupo de Trabajo en Sistemas de Control Industrial (Industrial Control Systems Joint Working Group -ICSJWG) para proporcionar un mecanismo formal y promover la coordinación entre agentes gubernamentales y privados.
- Operar el Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) en coordinación con el United States Computer Emergency Readiness Team (US-CERT) para el control de incidentes relacionados con sistemas de control y en actividades de concienciación sobre incidentes y ciberseguridad.
- Mantiene un centro de soporte técnico para orientar y evaluar componentes y sistemas de control disponibles comercialmente.
- Desarrollar actividades de formación y capacitación en la comunidad de sistemas de control.
- Crear herramientas y soluciones informativas para ayudar a proveedores y operadores.
- Proporcionar recomendaciones estratégicas para la comunidad de I+D de cara al desarrollo y evaluación de la próxima generación de sistemas de control seguro.

2.1.1.4 MAGERIT

MAGERIT es una metodología de análisis de riesgo que define asimismo un conjunto de recomendaciones apropiadas para controlar estos riesgos, sirviendo de apoyo al ENS y ayudando a las organizaciones a través de un conjunto de actividades estructuradas en tres etapas (CSAE, 2012).

2.1.1.5 Modelos generalistas: ISO/IEC 38500 y COBIT

En este grupo cabe referirse al muy extendido estándar ISO/IEC 38500 "*Corporate Governance of Information Technology*" (ISO/IEC38500, 2008) que se basa en la norma australiana AS8015:2005 (Standards-Australia, 2005) y pretende ayudar a la alta dirección de las organizaciones a comprender sus obligaciones legales, regulatorias y éticas en relación al uso de las TI.

En segundo lugar, otra de las metodologías generalistas y una de las primeras experiencias de gobernanza de TI es el marco "Control Objectives for Information and related Technology (COBIT). Esta norma está promovida y gestionada por el IT Governance Institute (ITGI) y es un conjunto de controles de cumplimiento de objetivos para las TI y, en su versión COBIT 5 (ITGI, 2012), recoge los conceptos básicos y recomendaciones de SI y auditorías IT, dadas en IT Assurance Framework (ITAF) (ISACA, 2014).

La Gobernanza de TI asegura que los requerimientos del negocio están vinculados a los servicios de TI. En este sentido, la TI se mide con base en el desempeño del servicio, incluidas las medidas de rendimiento para la creación de servicios nuevos o modificados a través de proyectos.

2.1.1.6 Estudio comparativo de guías de gobernanza en entornos de IICC

A la hora de abordar un estudio comparativo de los marcos presentadas en este enfoque de gobernanza de TI desde la perspectiva de las IICC, se ha definido un conjunto de elementos de SI para su estudio, relativos a la admninistración de proyectos de desarrollo seguro. en base a las actividades descritas por el modelo del SEI Security by Design (SbD) y los marcos elegidos en cada perspectiva (Siemens, 2008).

De este modo se pretenden mostrar los aportes y limitaciones de cada modelo y norma en cuanto a la administración de proyectos de desarrollo seguro en entornos industriales de IICC.

Para cada área de proceso de SbD y para cada una de sus prácticas específicas se definen uno o más factores de seguridad a partir de las respectivas sub-prácticas de cada práctica específica, examinándose cada factor de seguridad en cada marco: {GB, de Gobierno; Gestión de Servicios de SVM; PI, Mejora Continua; PM, Administración de Proyectos; y Gestión de SI SM},:

- Carencia del elemento o actividad en el modelo o norma estudiados: ○
- Elemento parcialmente considerado en el modelo o estándar estudiado. El icono que lo representa refleja que la guía considera nominalmente el elemento, pero sin definirlo o concretarlo de forma aplicada: ◗
- Descripción completa del elemento en el modelo o norma estudiada: ●

En este apartado se analiza el grado de presencia de un conjunto de acciones encaminadas al control de los riesgos asociados a la administración de la seguridad en los proyectos de TI. Así, los factores estudiados y los resultados de este enfoque serían los siguientes:

Tabla 2.2. Elementos de estudio para el análisis de las guías, normas y modelos de la gobernanza TI en IICC

CÓDIGO	Factor a estudiar	CSSP	MAGERIT	MODELOS GENERALISTAS ISO/IEC 38500 Y COBIT 5
GB_01	Proporciona guías y técnicas para definir políticas de gestión de seguridad para los proyectos TI abordados en la IICC	●	◗	◗
GB_02	Define directrices para crear un catálogo estándar de activos de seguridad para una IICC con departamento de TI	●	○	○
GB_03	Define los factores que aseguran una gestión de proyectos TI que genere productos seguros TI	●	○	○
GB_04	Proporciona guía para parametrizar los proyectos de TI	●	○	○
GB_05	Proporciona directrices para evaluar la seguridad de la gestión de proyectos de TI	●	◗	◗
GB_06	Proporciona directrices sobre el resultado de la evaluación de la seguridad de los productos TI	●	◗	◗
GB_07	Proporciona directrices de competencias y formación en seguridad	●	◗	◗
GB_08	Proporciona directrices en cuanto a las políticas de proveedores	●	◗	◗
GB_09	Establece directivas de integración de estándares, normas y regulaciones de seguridad	●	○	◗
GB_10	Proporciona guías para planificación de la seguridad de programas TI	●	○	○
GB_11	Proporciona guías sobre su aplicación en organizaciones empresariales	◗	◗	◗
GB_12	Proporciona guías sobre su aplicación en IICC	◗	○	○

2.1.2 Gestión de servicios TI en IICC

El *lifecycle* o ciclo del servicio se puede considerar como un proyecto que comienza con la necesidad del usuario y acaba con una solución satisfactoria a esa necesidad, bajo un principio de control. Las infraestructuras críticas constituyen por definición servicios imprescindibles para la sociedad y la economía de un territorio, por lo que la continuidad de servicio es un objetivo primordial en la protección de las mismas. De este modo, la aplicabilidad de modelos de gestión de servicios TI está extremadamente condicionada por la normativa aplicada.

El marco pionero en la administración de servicios de tecnologías de la información en IICC lo estableció el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) cuando lanzó su Framework de Cibseseguridad, paraa reducir los riesgos de seguridad en la gestión de las IICC.

En segundo lugar, mencionaremos un marco de referencia para gestión de seguridad de servicios de tecnologías de información que, pese a estar centrado en la gestión de la seguridad, resulta un ejemplo de guía de recomendaciones para proveedores de servicios de telecomunicaciones (Telecommunication Service Providers) y que está desarrollado por el canadiense *Canadian Security Telecommunications Advisory Committee* (CSTAC), un organismo asesor formado por expertos y creado por el gobierno de ese país para asesorar en materia estratégica a la National Strategy for Critical Infrastructure y la Canada's Cyber Security Strategy.

Por último, nos referiremos a los modelos generalistas ITIL, ISO/IEC 20000 y CMMI *for Services* del SEI (2013).

2.1.2.1 Framework de Ciberseguridad del NIST

El Framework del NIST establece cinco funciones para implementar la seguridad en las Infraestructuras:

1) Identificar: Realizar un entendimiento de la situación de la organización a través de la gestión del riesgo y teniendo en cuenta los activos, información, sistemas y controles de la Infraestructura.
2) Proteger: Desarrollar e implementar los controles adecuados, priorizados por el proceso de gestión del riesgo, para garantizar la seguridad de la Infraestructura.
3) Detectar: Desarrollar e implementar las medidas necesarias para identificar los eventos de ciberseguridad.
4) Responder: Gestionar las medidas a tomar ante posibles eventos de ciberseguridad.
5) Recuperar: Restaurar las capacidades o servicios de la Infraestructura ante posibles eventos de ciberseguridad.

Estas cinco Funciones descritas anteriormente están divididas en categorías y a su vez en subcategorías. El propio Framework muestra un mapeo de los controles establecidos con las buenas prácticas en seguridad. Cada uno de los controles mapea con uno o más de los siguientes estándares reconocidos internacionalmente:

- COBIT
- ISO/IEC 27001
- NIST SP 800-53
- ISA 99.02.01

El Framework proporciona una herramienta, que llama "*Profile Framework*", para que las organizaciones puedan establecer una hoja de ruta para reducción de los riesgos de SI.

La herramienta contempla los posibles objetivos de la organización y del sector, considera los requisitos legales o regulatorios y las mejores prácticas de la industria, y refleja las prioridades de gestión de riesgos.

A través de la herramienta, las organizaciones pueden conocer el estado de madurez actual en cuanto a ciberseguridad, además de identificar el GAP que deben abordar para cumplir los objetivos, en función del estado objetivo futuro que se marque la organización.

Proceso de Implantación del Framework

El Framework establece los mecanismos para su implementación, en el que se describen los flujos de la información y las decisiones dentro de una organización. En el Framework se diferencian los siguientes niveles: Ejecutivo, Proceso y Aplicación:

- El nivel Ejecutivo comunica al nivel Proceso las prioridades para alcanzar los objetivos, los recursos disponibles para ello y la tolerancia al riesgo a nivel global.
- El nivel Proceso utiliza la información proporcionada por el nivel Ejecutivo, para crear un "Profile Framework" en colaboración con el nivel Aplicación, reportando el resultado al nivel Ejecutivo.
- El nivel de Aplicación realiza el detalle del "Profile Framework".

En el Framework se establecen cuatro niveles de implantación de los controles, en los que se tienen en cuenta la madurez, en cuanto a: los procesos para gestionar los riesgos de ciberseguridad, la concienciación y los procesos existentes para relacionarse con otras organizaciones.

Los cuatro niveles de implantación de los controles son:

1) Tier 1 (Parcial): Este nivel se asocia a organizaciones que realizan iniciativas *ad hoc* pero no están formalizadas.
2) Tier 2 (Riesgo-Informado): Existe una mayor madurez que en el nivel 1, existiendo una mayor cultura en ciberseguridad, pero sin llegar a tener los procesos formalizados.
3) Tier 3: (Riesgo-Informado y Repetible): Nivel que se asocia a organizaciones que disponen de los procesos totalmente formalizados.

4) Tier 4 (Adaptado): Máximo nivel de madurez, existiendo una mejora continua de los procesos, que se adaptan a los posibles cambios.

Adecuación al sector Financiero

En 2015 el Banco Central Europeo inició un proceso de evaluación del nivel de madurez en materia de ciberseguridad en las entidades financieras supervisadas por dicho organismo a nivel europeo, de forma previa a comenzar a supervisar este entorno en el sector. El nivel de evaluación y detalle exigido está directamente relacionado con el framework de ciberseguridad del NIST.

2.1.2.2 TSP Best practices

El *Canadian Security Telecommunications Advisory Committee* (CSTAC) ha definido las Canadian Telecommunications Service Providers' (TSP) Security Best Practices, principalmente recomendaciones sobre seguridad, diseñadas para orientar a los Telecommunications Service Providers (TSP) en el robustecimiento de sus Infraestructuras Críticas, pudiendo ser utilizadas en otros sectores.

Las Best Practices están organizadas en seis áreas de seguridad, que se componen de once dominios de seguridad, que están compuestos por objetivos de control, y que a su vez se conforman de controles. Comprende recomendaciones en las siguientes áreas de seguridad:

- Protección del Servicio de Infraestructuras Críticas de Proveedores, prestando especial atención a su diseño y arquitectura de red y a securizar los denominados equipos *core.*
- Detección y Monitorización de las redes.
- Respuesta a Incidentes de Seguridad y los procedimientos de respuesta al cliente para la remediación y mitigación.
- Protección de la Infraestructura Crítica en el intercambio de información, definiendo los mecanismos para compartir dicha información.
- Admnistración de la Seguridad de los Proveedores.
- Controles para asegurar la Privacidad.

Las TSP canadienses se centran en las buenas prácticas de protección, respuesta y gestión de incidentes de seguridad, para lo cual desarrollan especialmente el proceso de gestión de incidentes.

2.1.2.3 Modelos generalistas: ISO/IEC 20000 e ITIL

La norma internacional ISO/IEC 20000-1 es una adaptación de la versión norma anterior desarrollada por la *British Standards Institution* (BSI) BS 150000-1. Aborda los requisitos necesarios de una organización para proveer servicios TI con calidad aceptable:

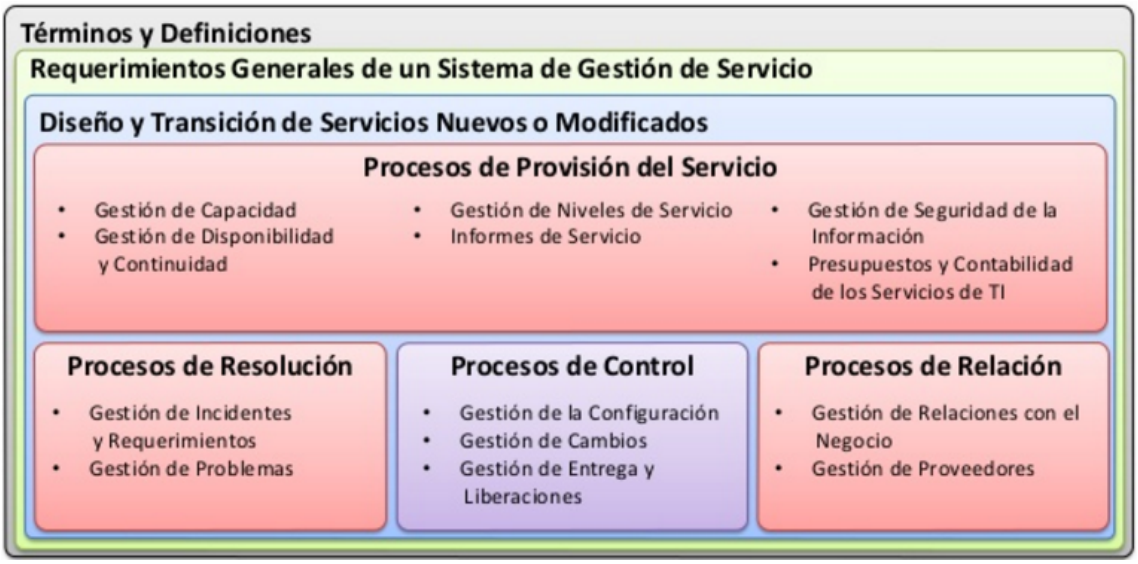


Figura 2.1 ISO/IEC 20.000. Estructura de Procesos.

En la categoría de provisión de servicio se incluyen los siguientes procesos relacionados con la seguridad:

- **Continuidad y disponibilidad del servicio**. Su objetivo es asegurar el cumplimiento de los objetivos relativos a la continuidad de negocio y la disponibilidad de los servicios acordados con los usuarios. En el caso de las IICC el nivel de *compliance* exigible condiciona los planes de negocio, así como los ANS (Acuerdos de Nivel de Servicio entre proveedor y cliente para establecer los niveles de calidad aceptables por éste) y las evaluaciones del riesgo, e incluyen los controles de acceso, los lapsos de respuesta y la disponibilidad de los activos.
- **Seguridad de la información (SI)**. Toma como referencia las normas ISO/IEC 27001 e ISO/IEC 17799 como las mejores para cumplir sus requisitos de seguridad. Analizaremos el esquema normativo ISO/IEC 27000 en el apartado correspondiente a los modelos específicos de Gestión de la Seguridad.

ISO/IEC 20000 comparte orígenes con la librería de mejores prácticas de gestión de TI, ITIL.

Además de incluir los procesos de gestión de continuidad y disponibilidad, ITIL v.3 mejora e incluye el proceso de gestión de la SI, protegiendo los activos de información frente a los daños que producen la falta de disponibilidad, confidencialidad e integridad, autenticidad y no repudio. Para ello, establece y requiere un SGSI que guíe el desarrollo y la gestión de un programa de seguridad de la información que cubra los objetivos de la organización.

También diferencia un cuarto proceso relativo a la Gestión de Accesos, el cual se ejecuta en relación con la gestión de disponibilidad y seguridad.

2.1.2.4 Estudio comparativo de guías de gestión de servicios en IICC

El estudio comparativo del enfoque gestión de servicios se ha hecho sobre las mismas bases del apartado 2.1.1.6. Además, como se ha visto, tanto modelos normativos específicos como generalistas incluyen el uso de técnicas y actividades relacionadas con gestión de riesgos y con la gestión de la SI.

Los procesos de gestión de continuidad y de disponibilidad adquieren en todos los casos especial importancia y se vinculan con las necesidades de disponibilidad de TI para procesos organizacionales en situaciones normales y críticas. Dado el carácter esencial de las IICC tanto el NIST Framework como las TSP Best Practices priorizan la integración de la gestión de la SI en el conjunto de la gestión corporativa.

Mientras que ISO/IEC 20000 e ITIL realizan recomendaciones para la gestión de proyectos que generan servicios TI, interesa en el análisis realizado chequear el nivel de detalle respectivo al proceso de gestión de SI en el proyecto de desarrollo.

Siguiendo el método descrito en el apartado 2.1.1 dedicado a la perspectiva de gobernanza, se revisan elementos de seguridad asociados a la perspectiva de gestión de servicios. Estos factores y los resultados de su evaluación en el marco NIST, prácticas ITIL, el estándar ISO/IEC 20000 y las TSP Best Practices se analizan a continuación.

Tabla 2.3. Elementos de estudio para el análisis de las guías, normas y modelos de gestión de servicios TI en IICC.

CÓDIGO	Factor a estudiar	NIST Framework	TSP-Best practices	MODELOS GENERALISTAS ISO/IEC 20000 E ITIL v3
GV_01	Proporciona políticas de seguridad a proyectos TI	●	◗	○
GV_02	Define directrices para crear un catálogo de activos de seguridad estándar	●	◗	◗
GV_03	Define un plan de proyectos seguros	●	○	◗
GB_04	Define los factores que aseguran una gestión de proyctos TI que genere productos y servicios seguros TI	●	○	○
GV_05	Proporciona guía para parametrizar los proyectos de TI	●	○	○
GV_06	Proporciona directrices para evaluar la seguridad de la gestión de proyectos de TI	●	◗	◗
GV_07	Proporciona directrices sobre la evaluación de la seguridad de los productos o servicios resultantes de los proyectos TI	◗	◗	◗
GV_08	Proporciona técnicas para garantizar el cumplimiento de planes de proyectos seguros	●	◗	○
GV_09	Proporciona directrices de competencias y formación en seguridad	◗	◗	○
GV_10	Proporciona guías para conocer las causas raíces (gestión de problemas de seguridad) en proyectos TI	◗	◗	◗
GV_11	Proporciona guías que permitan conocer el "know how" o "modo de hacer" en cuanto a la seguridad del producto	○	◗	◗
GV_12	Proporciona guías sobre su aplicación en organizaciones empresariales	○	○	○
GV_13	Proporciona guías sobre su aplicación en IICC	○	◗	○

2.1.3 Mejora de procesos

El auge en torno a la mejora continua en la década de 1990 se aplicó en el ámbito del software y la gestión TI a partir del liderazgo del *Software Engineering Institute* bajo la batuta de Humphrey (1989) que previamente había comenzado esta filosofía en su trabajo dentro de la multinacional IBM.

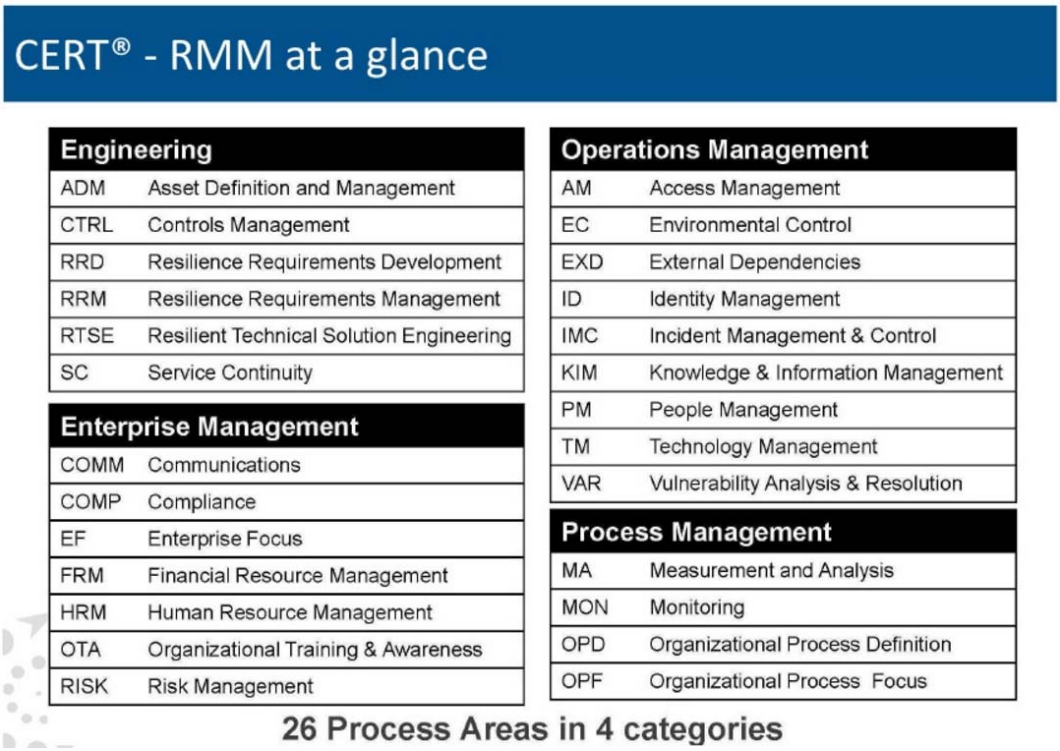
A nivel específico, el modelo que sirve de referencia para los marcos de referencia en gestión y mejora de procesos lo constituye en IICC el Programa de Evaluación CSEP, fundamentado en el modelo Cyber Resilience Review (CRR), que a su vez está fundamentado en el Modelo de Gestión CERT-RMM desarrollado por la Universidad Carnegie Mellon. Mediante una perspectiva de mejora de procesos como la que bebe de CMMI del SEI, su finalidad es ayudar a una organización a a responder a situaciones críticas con un rendimiento basado en la madurez y de los procesos y la mejora continua.

Además, entre los distintos estándares y modelos generalistas orientados a la mejora de procesos de producción de software más utilizados a nivel mundial se encuentran el CMMI propuesto por el SEI y el estándar ISO 15504 para el desarrollo de software de ISO (INTECO, 2008), (Garzas. J., 2013), aunque otros modelos de gestión de servicios en outsourcing como eSCM-CL (Hefley & Loesche, 2010) y eSCM-SP (Hefley, 2010) van adquiriendo auge en los últimos años.

2.1.3.1 Programa de Evaluación CSEP

La división National Cyber Security Division (NCSD), responsable de mejorar la seguridad y la resiliencia de las infraestructuras tecnológicas y de las comunicaciones de los EEUU, que depende del Dpto. del Homeland Security (DHS) norteamericano, coordina el Programa de Ciberseguridad *The Cyber Security Evaluation Program* (CSEP), de carácter voluntario para las organizaciones privadas, y que tiene el objetivo de evaluar las capacidades en materia de ciberseguridad. El programa está orientado a los 16 sectores de Infraestructuras Críticas y está basado en Cyber Resilience Review (CRR), que a su vez está fundamentado en el Modelo de Gestión CERT-RMM desarrollado por la Universidad Carnegie Mellon (Caralli et al., 2010). El CERT Resilience Management Model (CERT-RMM) constituye una base para la aproximación en mejora de procesos específicamente relacionados con la resiliencia operacional. Define las prácticas esenciales a nivel organizacional que son necesarias para gestionar la resiliencia, y permite a los responsables de gestión determinar la capacidad de respuesta corporativa en resiliencia, establecer objetivos y metas, y desarrollar planes adecuados para cerrar brechas identificadas entre aquellos y el rendimiento de los procesos.

Figura 2.2. Áreas de proceso cubiertas por el CERT Resilience Management Model (CERT-RMM) (Fuente: SEI-CMU)



Las organizaciones que participen en el programa CSEP recibirán un informe que reporta los resultados en cada una de las áreas del proceso SI.

2.1.3.2 CMMI

El Modelo SW-CMM (Software Capability Maturity Model) fue impulsado por el Dpto. de Defensa norteamericano y desarrollado por el SEI de la Carnegie Mellon, para proporcionar a las organizaciones una guía de cómo obtener el control sobre sus procesos de desarrollo y mantenimiento del software. CMM fue diseñado para guiar a las organizaciones a orientarse a mejorar sus procesos (Paulk et al., 1995; De la Cámara, 2016). En 2010, el SEI publica el modelo orientado a la mejora de procesos de gestión de servicios, CMMI for Services, Version 1.3 (Forrester, 2011) y (SEI, 2013) adaptado a su uso en el sector de proveedores de servicios TI.

Posteriormente, en 2013 el SEI evoluciona el modelo a partir de la perspectiva de la mejora de procesos relativos a la seguridad de los proyectos, como continuación de una colaboración con el Departamento de Defensa Australiano dentro del programa +SAFE (SEI, 2007) y, con la colaboración de la multinacional Siemens, desarrolla el modelo *Seguridad por Diseño con CMMI for Dev V. 1.3*, (en adelante CMMI–SbD, de *Security by Design with CMMI for Development*. Version 1.3. An application guide for improving processes for secure projects) (SEI, 2013_b). El modelo responde a la necesidad de desarrollo de productos de seguridad crítica que requieran procesos especializados, técnicas y habilidades, y experiencia en una organización.

De los modelos CMMI existentes, en los sub-apartados que siguen, se resumen los modelos CMMI for Development V1.3 y CMMI for Services, resaltando cómo tratan la mejora de la gestión de SI en los proyectos. El modelo Seguridad por Diseño con CMMI

- DEV se desarrolla en el apartado dedicado a los modelos, estándares y guías de gestión de la SI.

CMMI para Desarrollo de Software, V 1.3

El objetivo del modelo CMMI-DEV v.1.3 (SEI, 2010) es proporcionar una guía a las organizaciones para mejorar sus procedimientos y ayudar en la administración del desarrollo, mantenimiento y adquisición de servicios/productos. Se trata de un conjunto de buenas prácticas estructuradas para ayudar a la organización a evaluar tanto su madurez organizacional como la capacidad de sus áreas de proceso.

Una organización que apuesta por la representación continua del modelo podrá priorizar las mejoras en orden a mejorar la eficiencia para satisfacer los objetivos del negocio y mitigar las áreas de riesgo y podrá comparar los resultados y representaciones discretas, de un área de proceso bien a través de la organización o entre varias organizaciones, incluso comparando resultados con la mejora obtenida con el modelo ISO/IEC 15504: 2004, cuyas áreas de proceso son similares a CMMI.

Para evaluar a las organizaciones que usan CMMI-DEV se utiliza el método SCAMPI (Ahern et al., 2005), que permite obtener calificaciones bien en niveles de capacidad (incompleto-realizado-gestionado-definido) o de madurez (inicial-gestionado-definido-gestionado cuantitativamente-en optimización) (SEI, 2013).

2.1.3.3 ISO/IEC 15504

El estándar ISO/IEC 15504 (ISO, 2004) fue desarrollado por ISO e IEC a través del proyecto SPICE (Software Process Improvement and Capability dEtermination), y es un marco aplicable a cualquier organización software que desee establecer y/o mejorar sus capacidades en la planificación, gestión, supervisión, control, adquisición, suministro, desarrollo, operación, evolución y soporte del software.

Permite también evaluar los niveles de capacidad de los procesos e incluye una referencia en su apartado 5 *An exemplar software life cycle process assessment model,* para la realización de una evaluación basada en la metodología de la norma ISO/IEC 12207:2008 (ISO/IEC, 2008).

La familia de normas ISO/IEC 15504 incluye en su parte 10 especificaciones para organizaciones y entornos que requieren una extensión relativa a la seguridad, su gestión, y acreditación.

2.1.3.4 Estudio comparativo de guías de ciclo de mejora de procesos en IICC

El estudio comparativo del enfoque mejora de procesos se ha hecho sobre las mismas bases del apartado 2.1.1.8. Para esta perspectiva se han elegido los marcos de mejora de procesos principalmente basados en los desarrollos del SEI, CSEP y la matriz original

CMMI para el desarrollo de software y para servicios, así como el estándar ISO/IEC 15504. .

Tabla 2.4. Elementos de análisis de las guías, normas y modelos de mejora de procesos TI en IICC

CÓDIGO	Factor a estudiar	CSEP-CERT-RMM	CMMI-DEV 1.3	CMMI-SVC 1.3	ISO/IEC 15504
MP_01	Enfocado a procesos estandarizados	●	●	●	●
MP_02	Cuestionarios de evaluación orientados a desarrollo	◗	◗	◗	◗
MP_03	Cuestionarios de evaluación orientados a gestión de la seguridad	◗	◗	◗	◗
MP_04	Parametrización de las necesidades de seguridad en el proyecto	◗	◗	◗	○
MP_05	Declaración de viabilidad de proyecto seguro	◗	◗	◗	◗
MP_06	Objetivos de control de seguridad de proyectos	◗	◗	◗	◗
MP_07	Controles de seguridad	◗	◗	◗	◗
MP_08	Registro de umbrales y valores de seguridad	○	○	○	○
MP_09	Auditorías de seguridad	◗	◗	◗	◗
MP_10	Gestión de proveedores de producto seguro	◗	○	○	○
MP_11	Gestión de configuración y activos de seguridad (PAL)	◗	◗	◗	○
MP_12	Se define un plan de mejora	◗	◗	◗	◗
MP_13	Proporciona directrices de competencias y formación en seguridad	◗	◗	◗	○
MP_14	Proporciona guías sobre su aplicación en IICC	◗	○	○	○

2.1.4 Gestión de Proyectos

Se analizan a continuación sucintamente las bases de las metodologías para la gestión de proyectos más relevantes a nivel internacional tales como PMBOK, PRINCE, Metrica 3,

PSP, TSP y SCRUM, así como modelos y metodologías SLDC (Systems development life cycle) o Ciclos de Vida del Software.

En gestión de proyectos, un proyecto puede definirse tanto con un ciclo de vida de proyecto (PLC) como con un SDLC, el cual se centra en la realización de los requisitos de producto (Taylor, 2004: p. 39).

Los Ciclos de Vida del Software SDLC pueden van desde el grupo de las metodologías AGILE, donde XP o SCRUM se han popularizado hasta las iterativas o las secuenciales, tales como Rational Unified Process y DSDM.

2.1.4.1 Métodos Generalistas: PMBOK O PRINCE

PMBOK fue diseñado por PMI[15] para ofrecer a las organizaciones un marco de gestión exitosa de procesos, y posteriormente dio lugar a la norma IEEE 1490-1998 (IEEE, 1999). No es una metodología con un ámbito de aplicación exclusiva en la administración de proyectos software y se organiza en diez áreas de conocimiento (PMI, 2009):

Figura 2.3 Marco de trabajo PMBOK (Fuente: PMI, 2009)

Gestión de la Integración	Gestión del Alcance	Gestión del Tiempo	Gestión del Costo	Gestión de la Calidad
• Desarrollar acta de inicio • Desarrollar plan de dirección del proyecto • Dirigir y manejar el trabajo del proyecto • Monitorear y controlar el trabajo del proyecto • Realizar control integrado de cambios • Cerrar proyecto o fase	• Planear gestión del alcance • Recolectar requerimientos • Definir alcance • Crear EDT • Validar alcance • Controlar alcance	• Planear gestión del cronograma • Definir actividades • Secuenciar actividades • Estimar recursos • Estimar duración de actividades • Desarrollar cronograma • Controlar cronograma	• Planear gestión del costo • Estimar costos • Determinar presupuesto • Controlar costos	• Planear gestión de la calidad • Realizar aseguramiento de la calidad • Controlar la calidad
Gestión de los Recursos H	**Gestión de las Comunicaciones**	**Gestión de los Riesgos**	**Gestión de los Abastecimientos**	**Gestión de los Interesados**
• Planear gestión de recursos humanos • Adquirir equipo del proyecto • Desarrollar equipo del proyecto • Manejar equipo del proyecto	• Planear gestión de las comunicaciones • Manejar comunicaciones • Controlar comunicaciones	• Planear gestión de los riesgos • Identificar riesgos • Realizar análisis cualitativo de riesgos • Realizar análisis cuantitativo de riesgos • Planear respuesta a los riesgos • Controlar riesgos	• Planear gestión de los abastecimientos • Conducir abastecimientos • Controlar abastecimientos • Cerrar abastecimientos	• Identificar Interesados • Planear gestión de los interesados • Manejar relación con los interesados • Controlar relación con los interesados

Un segundo modelo generalista para la gestión de proyectos dentro del contexto de trabajo y en el ciclo de gestión de servicios propuesto también por las guías ITIL (OGC, 2009), es el método *Projects In Controlled Environments Version 2* (PRINCE2) y que fue desarrollado por la Oficina británica de Comercio (OGC). PRINCE2 es aplicable a cualquier tipo de proyectos en general.

[15] El Project Management Institute (PMI), fundado en 1969, ha desarrollado una serie de estándares para la gestión de proyectos (PMI, 2009), (PMI, 2014).

2.1.4.2 MÉTRICA V3

MÉTRICA Versión 3 es un método desarrollado por el gobierno de Espaal (MAP, 2001) para asegurar los objetivos de calidad, costes y calendario previsto de un proyecto. Además posee un enfoque orientado a procesos siguiendo la tendencia general de la norma ISO/IEC 15504 SPICE, y a norma ISO/IEC 12207:1995 orientada a los procesos del ciclo de vida del software.

La estructura principal de MÉTRICA 3 tiene tres áreas de proceso: planificación, desarrollo y mantenimiento de Sistemas de Información.

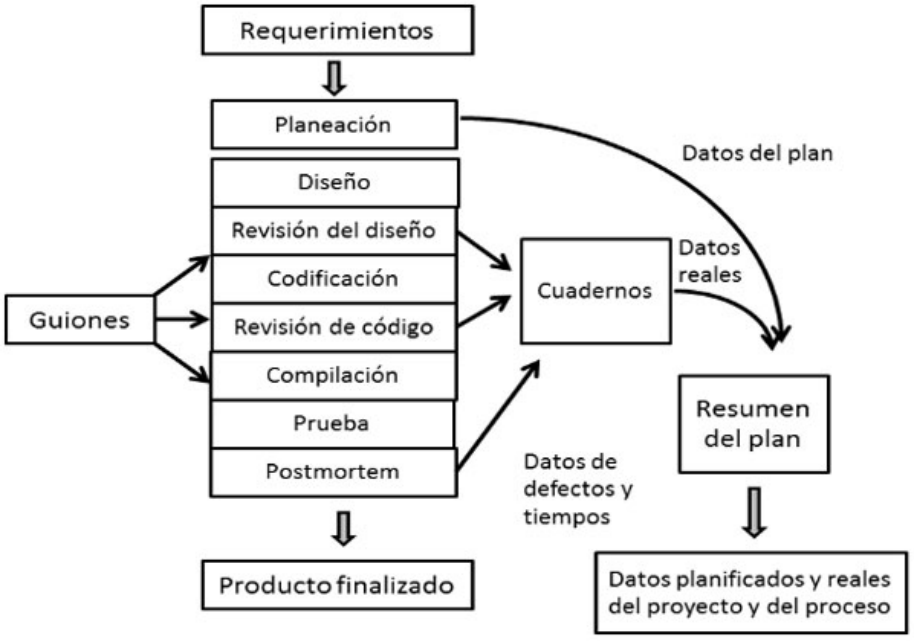
La SI aparece como prerrequisito del desarrollo del sistema y dispone de un interfaz propio.

2.1.4.3 Metodologías Predictivas

El modelo Proceso Software Personal (PSP –Personal Software Process) que fue creado por Humphrey (1997) como extensión del modelo de madurez CMMI al proceso de desarrollo SW de un programador. Este modelo tiene como objetivo hacer más fácil a los ingenieros del software las habilidades (skills) de proceso necesarias para trabajar en un equipo TSP (team software process).

Su propósito es desarrollar productos con cero-defectos dentro del tiempo establecido y con los costes planificados.

Figura 2.4. Esquema de procesos de PSP (Fuente: Humphrey, 1997)



TSP

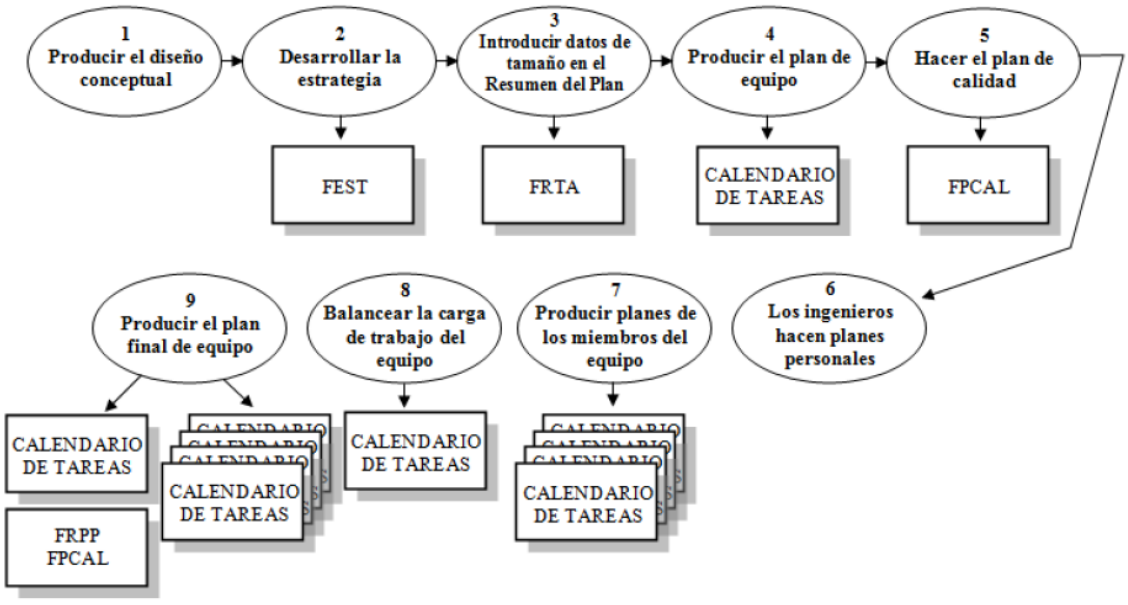
El Team Software Process (TSP) es un modelo integrado, automatizado a grandes escalas, para conducir equipos de desarrollo en la producción de sistemas intensivos en software de alta calidad, con ahorro de plazos y de costes.

El procedimiento aplica el ciclo de mejora continua de Deming (1989) a partir del énfasis en el trabajo disciplinado de equipos muy capacitados y adecuadamente formados (Humphrey, 2002).

Así, la guía TSP ayuda a los equipos de ingeniería en el desarrollo intensivo de productos software. TSP está diseñado para usarse con equipos de 2 a 20 miembros, y el proceso TSP más grande para múltiples equipos está diseñado para equipos de más de 150 miembros.

La Figura 2.5 muestra los pasos de la planificación con TSP.:

Figura 2.5 Flujo de procesos con TSP (Fuente: Humphrey, 2002)



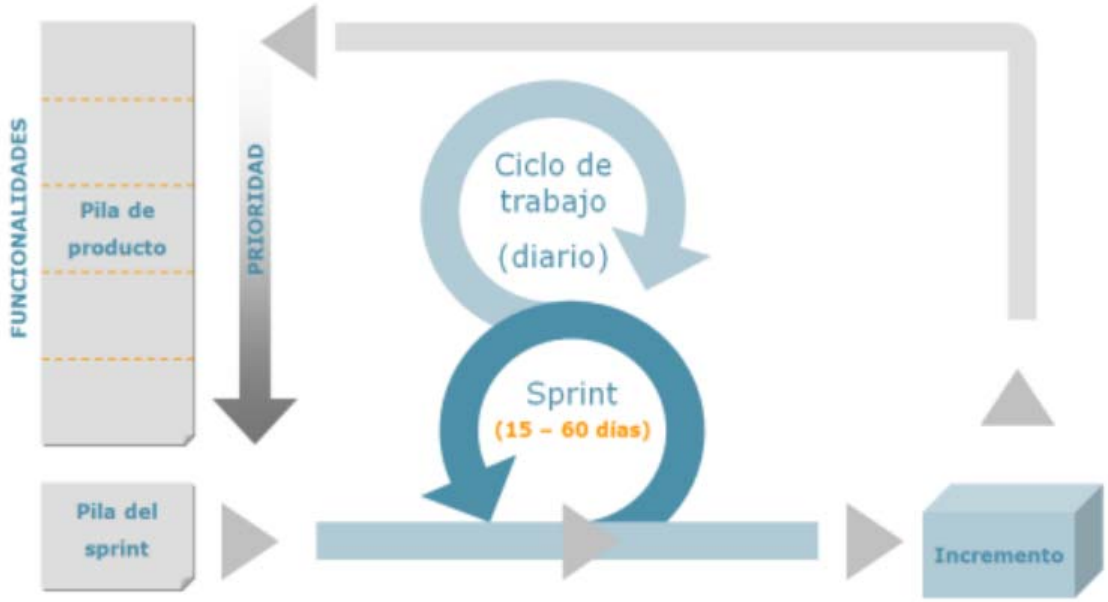
2.1.4.4 Metodologías Adaptativas

A comienzos de la década de 1990 se desarrolla la metodología Ágil o AGILE que fomenta el trabajo en equipos auto-dirigidos que trabajan de modo cooperativo y aplica inspecciones frecuentes como mecanismo de control. Parte de la base de que los procesos definidos funcionan bien, sólo si las entradas están perfectamente definidas y el ruido, ambigüedad o cambio es muy pequeño. Se trata de una metodología aconsejable para proyectos con requerimientos inestables.

Los modelos inscritos en la organización Agile Aliance y que desarrollan métodos específicos ágiles son los siguientes (Palacio y Ruata, 2011) entre los cuales la más popular puede ser SCRUM y su sistema de *sprints* de desarrollo. Otros métodos son AD - Agile Database Techniques, ASD - Adaptive Software Development, AUP - Agile

Unified Process, Crystal, DSDM - Dynamic Systems Development Method, Lean Software Development, entre otros.

Figura 2.6. Esquema típico de diagrama SCRUM (Fuente: Palacio y Ruata, 2011)



2.1.4.5 Estudio comparativo de guías de gestión de proyectos

El proceso de estudio de este apartado ha sido el mismo que los apartados anteriores. Así, los marcos y estándares elegidos para el estudio han sido los descritos en los sub-apartados 2.1.4.1 al 2.1.4.4. Los factores que han resultado del estudio de las prácticas SbD en cada uno de ellos han sido analizados en todos ellos.

Tabla 2.5. Elementos de análisis de las guías, normas y modelos de gestión de proyectos TI aplicables en IICC

CÓDIGO	Factor a estudiar	MÉTODOS GENERALISTAS: PMBOK Y PRINCE	METRICA V3	METODOLOGÍAS PREDICTIVAS	METODOLOGÍAS ADAPTATIVAS
GP_01	Gestión enfocada a procesos estandarizados	◗	◗	◗	○
GP_02	Define factores de seguridad de producto de desarrollo de software	◗	◗	◗	◗
GP_03	Parametrización de las necesidades de seguridad en el proyecto	○	◗	◗	○
GP_04	Objetivos de control de seguridad	◗	◗	◗	◗
GP_05	Controles de seguridad	○	◗	◗	◗
GP_06	Registro de umbrales y valores de seguridad	○	◗	◗	◗
GP_07	Gestión de proveedores de producto seguro	○	◗	○	◗
GP_08	Define guía de evaluación de seguridad de producto software	◗	◗	◗	○
GP_09	Proporciona guías sobre técnicas de seguridad de producto en desarrollo	◗	◗	◗	○
GP_10	Gestión de configuración y activos de seguridad (PAL)	○	◗	◗	○
GP_11	Proporciona guías sobre su aplicación en IICC	○	◗	○	◗
GP_12	Respaldo y compromiso de la dirección	◗	◗	◗	◗
GP_13	Proporciona directrices de competencias y formación en seguridad	◗	◗	◗	○

2.1.5 Gestión de Seguridad

En este apartado 2.1.5 se focaliza el análisis en los marcos y estándares desde la perspectiva de la seguridad de los SI en general, y a la gestión de proyectos segura en particular.

Por lo tanto, en los sub-apartados que siguen se detallan las características más importantes de los siguientes marcos y guías de seguridad:

- NERC CIP
- NRC-RG 5.71

- CFATS
- PCI DSS
- El estándar ISA/IEC 62443
- ISO 27000
- Security by Design with CMMI-DEV (SEI, 2013_b).
- Los *Common Criteria*
- Metodologías de análisis de riesgo

2.1.5.1 NERC CIP

La *Federal Energy Regulatory Commision* (FERC) es el organismo que tiene la jurisdicción sobre el sector energético en Estados Unidos incluyendo el sistema tarifario eléctrico, la concesión de licencias hidroeléctricas, aprobación de tasas de gas natural o regulación en materia de suministro y distribución de derivados del petróleo, incluyendo oleoductos.

En febrero de 2006 la FERC encomendó, dentro de un mandato gubernamental[16], a la entidad de normalización North American Electric Reliability Corporation (NERC), la preparación de un grupo de normas para regular la seguridad de las IICC en el sector energético y específicamente su ciberseguridad.

Objetivos del Modelo

NERC CIP se debe cumplir obligatoriamente para las compañías relacionadas con el subsector eléctrico de alta tensión que soportan la red eléctrica estadounidense, de tal manera que se garantice la fiabilidad de la misma, frente a posibles ataques o incidentes.

Clasificación de Activos

El estándar NERC CIP establece una taxonomía de activos que las organizaciones utilizan para clasificar los suyos. En concreto, esta taxonomía se encuentra en el estándar CIP-002, que a continuación se describe:

- Se define un grupo llamado BES Cyber System, utilizado para agrupar activos que sean considerados críticos por una organización, de forma que se puedan utilizar diferente tipos de agregaciones, entre las que se encuentran:
    - Central Eléctrica
    - Centro de Control
    - Red de generación
    - Red de transporte

A su vez, cada uno de los activos BES Cyber System están asociados a los siguientes activos:

[16] De acuerdo con la Sección 215 de la Federal Power Act, habilitada por la Energy Policy Act de 2005.

- *Electronic Access Control or Monitoring Systems* (EACMS): Esta categoría trata activos como servidores de autenticación (Radius, Active Directory), control de eventos y sistemas de detección de intrusos, entre otros.
- *Physical Access Control Systems* (PACS): En este grupo se incluyen los sistemas de autenticación físicos (sistemas de tarjeta, biométricos, código de seguridad, etc.).
- *Protected Cyber Assets* (PCA): Esta categoría incluye activos del tipo: file server, sevidores ftp, time server, switches, impresoras de red, etc.

Valoración de Impactos

El Estándar **CIP-002** también establece una **escala de los impactos asociados a los activos** y define los **criterios** para su correspondiente asignación: Alto, Medio y Bajo. A continuación se resumen los criterios:

- **Nivel Alto**:
  - Centros de control (tanto activos o de back-up) para la gestión y operación de la red.
  - Centros de control (tanto activos o de back-up) para el balanceo de la red para una potencia agregada superior a 3000 MW (Megavatios) o que excedan determinados criterios de las infraestructuras de nivel medio.
  - Centros de control (tanto activos o de back-up) para el operador de transporte que cumplan más de los criterios de nivel medio.
  - Centros de control (tanto activos o de back-up) para el operador de generación que cumplan más de los criterios de nivel medio.
- **Nivel Medio**:
  - Elementos de red de generación que cumplan unas determinadas características a nivel de potencia generada o que hayan sido designadas por la compañía, el operador de transporte o el regulador.
  - Instalaciones de la red de transporte que cubran determinadas condiciones de voltaje, como aquellas fundamentales para una central nuclear.
  - Elementos de protección y de operación de las instalaciones que sean críticas para las operaciones de los equipos.
  - Sistemas de balanceo de carga que no tengan intervención humana por encima de 300 MW.
  - Centros de control no incluidos en la criticidad alta.
  - Alguno ejemplos de este nivel son:
    - Grupo de instalaciones de generación con una sola interconexión con una capacidad igual o mayor que 1500 MW. También se incluyen aquellas instalaciones designadas por la compañía o por el operador de transporte.
    - Grupo de instalaciones reactivas de 1000 MVAR (Mega Volt Ampere Reactivo).
    - Estaciones de transporte por encima a 500 KV o aquellas que estén conectadas a un determinado tipo de línea.
- **Nivel Bajo**: Elementos que no hayan sido considerados anteriormente. Dentro de estos grupos destacan:

- Centro de control (tanto activos como restauración).
- Estaciones de transmisión y transporte.
- Recursos de generación.
- Instalaciones necesarias para realizar el back-up.
- Sistemas de protección.
- Elementos de distribución que cubran determinados criterios específicos como ser necesarios para el back-up.

Controles

El conjunto NERC CIP está constituido por diez normas que incluyen la definición de activos cibernéticos (CIP-002-5), el catálogo de controles (CIP-003-5), la formación (CIP-004-5), vigilancia perimetral y física (CIP-005-5 y CIP-006-5), SI de sistemas (CIP-007-5), incidentes de SI (CIP-008-5), continuidad de negocio (CIP-009-5), gestión del cambio (CIP-010-1) y seguridad de la información (CIP-011-1) que cataloga controles de confidencialidad, integridad y disponibilidad.

Existe un calendario de aplicación de las normas que, dependiendo de la clasificación de los a**ctivos** en función del impacto **medio y alto, o impacto bajo,** establece como plazos abril de 2016 o de 2017, respectivamente.

Las sanciones por incumplimiento oscilan entre mil y un millón de dólares diarios.

Los estándares NERC CIP están en continua revisión y se acompañan de un plan de implementación, lo que los convierte en una herramienta de ayuda muy útil.

2.1.5.2 NRC - RG 5.71

La *United States Nuclear Regulatory Commission* (USNRC) es el organismo encargado de otorgar las licencias para poder operar plantas nucleares en USA[17].

Uno de los requisitos para disponer de la licencia es cumplir con un Plan de Seguridad Física que está regulado federalmente en el artículo artículo 10 del *Code of Federal Regulation* (CFR) 75.55. Dependiendo de este Plan de Seguridad Físico, existe un requisito en materia de Ciberseguridad regulado en el artículo 10 (CFR) 75.54 "Protection of Digital Computer and Communication System and Networks".

Características del Modelo

La Regulatory Guide 5.71 (RG 5.71) proporciona un método, considerado como aceptable por la NRC para cumplir con esta regulación, que diferencia tres fases:

- Análisis de la situación, de la central nuclear, en cuanto a Ciberseguridad
- Establecer, Implementar y Mantener un Programa de Ciberseguridad

[17] http://www.nrc.gov/

- Incorporar el Programa de Ciberseguridad como un componente del Plan de Seguridad Físico.

La guía RG 5.71 establece un proceso para identificar los activos críticos digitales que deberían entrar en el alcance de la regulación. En concreto, el proceso establece que un activo digital es crítico si aplica a uno o varios de los siguientes aspectos:

- Afecta a la funciones de preparación de las emergencias de seguridad.
- Soporta el proceso de uno o varios activos críticos del negocio, anteriormente establecidos.
- Afecta a la protección de uno o varios activos críticos del negocio.

Controles

Uno de los requisitos propuestos por la NRC para cumplir con la regulación es disponer de una estrategia de defensa. En este sentido, un método aceptable que propone la RG 5.71 es establecer niveles de seguridad que dispongan de unas medidas de seguridad homogéneas que detecten, prevengan y mitiguen los posibles ataques cibernéticos.

El siguiente paso, una vez definida la estrategia de seguridad, es definir las medidas de seguridad que se van a asociar a cada una de los niveles o zonas de seguridad. La RG 5.71 propone un catálogo de controles que ha sido aceptado por la NRC.

En este sentido, la RG 5.71 diferencia dos tipos de controles por su naturaleza: 70 técnicos y 67 operativos.

- En la categoría de **Controles Técnicos** se incluyen las contramedidas para de securización para mantener confidenciales, íntegros y disponibles los sistemas que soportan los procesos críticos de las centrales nucleares. En concreto se categorizan en las siguientes áreas:
    - Control de acceso
    - Auditoría
    - Protección de los sistemas y de las comunicaciones
    - Identificación y autenticación
    - Robustecimiento del sistema
- En la categoría de **Controles Operativos** se incluyen las contramedidas en relación a:
    - Protección de medios
    - Seguridad en el personal
    - Mantenimiento
    - Protección Física y Medioambiental
    - Defensa en Profundidad
    - Respuesta a los Incidentes y mitigación en los Ataques
    - Plan de Contingencia de Ciberseguridad

- Entrenamiento
- Configuración y adquisición de TI y Servicios.

Cumplimiento del Modelo

La regulación prevé la revisión del Programa de Ciberseguridad como parte del Plan de Seguridad Física, al menos cada veinticuatro meses, y antes de doce en el caso de un cambio en el alcance, en particular que suponga cambios en las áreas de personal, procedimientos, equipos o instalaciones. Por último, se deben conservar todos los registros, evidencias y documentación, durante 3 años.

2.1.5.3 CFATS

La Office of Infraestructure Protection (OIP)[18] es un organismo dependiente del Department of Homeland Security (DHS), y es responsable de dirigir y coordinar los programas y las políticas sobre la seguridad de las Infraestructuras Críticas en Estado Unidos.

En el año 2007, El OIP desarrolla el Chemical Facility Anti-Terrorism Standards (CFATS), para regular la seguridad de las organizaciones del Sector Químico.

Características del Modelo

El objetivo del estándar CFATS es identificar y proteger las instalaciones químicas de alto riesgo que se consideran posibles objetivos de un ataque terrorista. El estándar se compone de cuatro fases:

- Top Screen: En esta fase se evalúan todas las instalaciones que almacenan cantidades de productos químicos potencialmente peligrosos. Las preguntas realizadas en esta fase son relativas a los 322 productos identificados como peligrosos por el DHS: tipo, cantidad y ubicación.
- SVA (Evaluación de Vulnerabilidad de Seguridad): El propósito de esta fase es determinar la probabilidad de que se produzcan incidentes de seguridad.
- SSP (Plan de Seguridad en el Sitio): El objetivo de esta fase es definir un plan de seguridad apropiado al nivel de riesgo asociado a la planta química.
- Implantación de los controles definidos en el Plan de Seguridad en el Sitio.

Alcance

CFATS es un estándar que regula las instalaciones que utilizan, fabrican, almacenan o manejan cantidades específicas de aproximadamente 322 sustancias químicas que el DHS ha identificado como extremadamente peligrosas.

[18] https://www.dhs.gov/office-infrastructure-protection

Clasificación de Activos

El estándar CFATS establece una **categoría de activos** sobre los que se realiza el proceso de regulación. Algunos de los activos que forman la taxonomía son:

- Activos utilizados en las instalaciones (generales y empaquetados).
- Activos liberadores de sustancias químicas de interés.
- Sistemas cibernéticos de control.
- Sistemas cibernéticos del negocio.

Valoración del Impacto

La regulación CFATS establece una escala de impactos o de riesgos de cuatro niveles (*tier* o ratio, nivel, en inglés). En este sentido, las organizaciones son categorizadas a través de uno de estos cuatro niveles.

En la primera fase del proceso CFATS, que tiene el nombre de Top Screen, se realiza un análisis de cada una de las 322 sustancias denominadas peligrosas. En función del tipo, de la cantidad y de la ubicación de cada una de estas sustancias se asigna un Tier (nivel del riesgo) de forma preliminar, o se determina que no existe un riesgo de que se produzcan incidentes de seguridad.

En el caso de que se identifique un rango de riesgos para la organización, esta deberá completar la segunda fase del proceso CFATS, que se trata de una evaluación de vulnerabilidades de seguridad (con siglas SVA en inglés) basándose en la posición de seguridad de la instalación. La evaluación de seguridad consistirá en evaluar cada una de las combinaciones de los siguientes elementos: activo, sustancia peligrosa y ataque (robo, sabotaje, atentado, etc).

En el caso de que se determine que existe un riesgo de ataque se asigna a la instalación un Tier (nivel de riesgo) definitivo.

Valoración de las Amenazas

El estándar CFATS establece una categoría de amenazas o escenarios de ataques sobre los que se realiza el proceso de regulación. Los escenarios de ataque que se establecen son:

- Aéreo / Aviones
- Marítimo
- Vehículo
- Equipo de asalto
- Zona de punto muerto
- Robo
- Descuido / Diversión.

Controles

Los controles de seguridad a implantar se definen en la tercera fase, que tiene el nombre de Plan de Seguridad en el sitio (en inglés con siglas SSP). El propósito de esta fase es definir un plan de seguridad apropiado al nivel de riesgo asociado a la planta.

Para definir el plan se utiliza un cuestionario que está compuesto por más de un millar de preguntas (de respuesta sí / no) categorizadas en 18 criterios de seguridad o riesgos base, que se listan a continuación:

- Área perimetral restringida
- Activos securizados
- Control de Acceso
- Protección y Detección
- Envío, recepción y almacenamiento
- Robo y Diversión
- Sabotaje
- Ciberseguridad
- Respuesta
- Monitorización
- Formación
- Personal garantizado
- Amenazas elevadas
- Amenazas, vulnerabilidades y riesgos
- Notificación de Incidentes de Seguridad Importantes
- Incidentes de Seguridad Significativos y Actividades Sospechosas
- Organización
- Registros.

Cumplimiento del Modelo

El Plan de Seguridad en el Sitio completado por parte de organización es revisado por parte del DHS para verificar que se adecua al nivel de riesgo de la instalación química. En el caso de que no se ajuste, el DHS lo devuelve para que la organización vuelva a completarlo hasta que sea adecuado.

Una vez que se decide que el Plan es válido empieza la fase de su implantación. En este caso, el DHS informa del tiempo de que dispone la organización para implantar el Plan.

Los controles que tiene que implantar la organización para cumplir con el estándar van a depender fundamentalmente de nivel de riesgo (Tier) que se asigne a la organización y

de los controles a los que se haya comprometido a implantar en el Plan de Seguridad en el Sitio.

Dentro de la documentación del proceso de regulación se encuentra una guía que relaciona los posibles niveles de riesgo asociados a las organizaciones y las métricas utilizadas en el Plan de Seguridad, de forma que tanto la organización como los inspectores conocen la granularidad del control a implantar.

Los incumplimientos pueden resultar en multas de 25.000$ por día y el cierre de las instalaciones. En este sentido, no se han identificado los criterios seguidos para establecer las sanciones.

2.1.5.4 PCI DSS

PCI DSS (*Payment Card Industry Data Security Standard*), es la norma de SI para las organizaciones del sector de medios de pago, y ha sido desarrollada en 2006 por un comité llamado *Payment Card Industry Security Standards Council* (PCI SSC) creado por American Express, MasterCard Worldwide y Visa entre otras compañías.

La norma regula doce requisitos de cumplimiento en materia de ciberseguridad, adaptados a la estructura organizativa y el tamaño de facturación al año. El procedimiento aplicado conlleva la realización de una autoevaluación anual, una auditoría externa y un chequeo trimestral de proveedor así como *penetration testing* también cada año.

Aplica a todas las organizaciones que participan en los procesos de los medios electrónicos de pago, tanto entidades financieras como emisores, comercios, proveedores y operadores, y en cuanto se produzca cualquier tipo de procesamiento, almacenamiento o transmisión de datos de poseedores de medios de pago electrónicos.

El sistema provee de un sistema de acreditación del auditor (QSA) y de la empresa que realiza los chequeos de proveedor trimestral.

Clasificación de Activos y áreas de control

Sobre cualquier elemento de red, servidor o aplicación que esté incluido en el área de datos del propietario del medio de pago o que tenga acceso a ellos, los doce requisitos se aplican en el siguiente orden:

- Requisito 1: Cortafuegos.
- Requisito 2: Contraseñas no predeterminados por los proveedores.
- Requisito 3: Protección de los datos almacenados de los titulares de medios de pago.
- Requisito 4: Cifrado de datos confidenciales a través de redes abiertas.
- Requisito 5: Antivirus.

- Requisito 6: Desarrollo y mantenimiento de sistemas y aplicaciones seguras.
- Requisito 7: Control digital de accesos.
- Requisito 8: Asignación de roles y permisos.
- Requisito 9: Control físico de accesos.
- Requisito 10: Monitorización de acceso a la red y datos.
- Requisito 11: Chequeo regular de los sistemas y procesos de seguridad.
- Requisito 12: Política de seguridad de la información.

2.1.5.5 ISA/IEC 62443

Desarrollada por la *International Society of Automation* (ISA), la norma ISA/IEC-62443 es una serie de normas, informes técnicos o información relacionada que definen los procedimientos para asegurar los Sistemas de Control Industrial.

Todas las normas que componen la familia ISA-62443 junto a sus informes técnicos están organizados en cuatro categorías: General, Política y Procedimientos, Sistema, and Componentes.

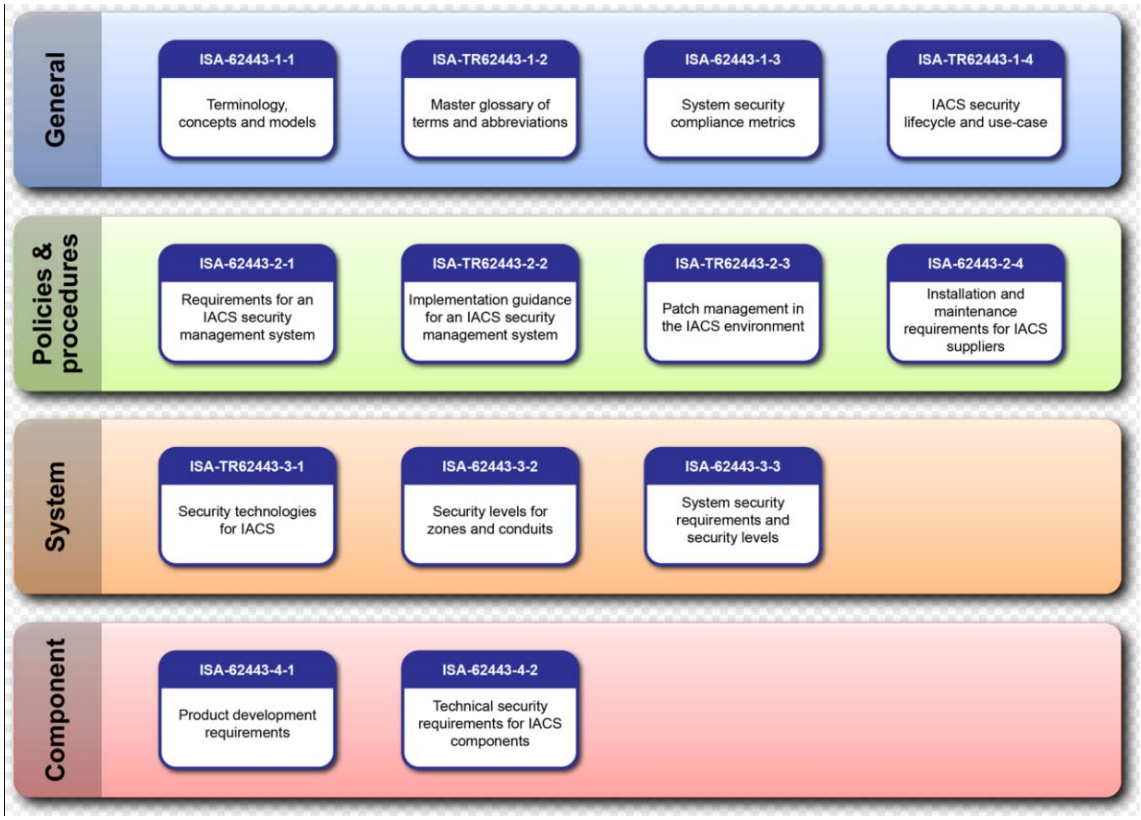


Figura 2.6. Elementos de la norma ISA 62443 planificados y publicados

El *ISA Security Compliance Institute* (ISCI) ha creado el programa de certificación *Embedded Device Security Assurance* (EDSA). En concreto, se trata de una certificación otorgada a los Sistemas de Control Industriales robustos contra ataques de seguridad y que cumplen con los requisitos de ISA/IEC-62443.

En este sentido, la certificación EDSA está centrada en la seguridad de los dispositivos integrados.

Certificación

System Security Assurance (SSA) es un programa que certifica que los Sistemas de Control Industriales son seguros. Esta certificación solo puede otorgarse a aquellos sistemas de control que cumplan una serie de criterios previos:

- Un conjunto integrado de componentes de control que incluye más de un dispositivo.
- El sistema de control está disponible y apoyado en su totalidad por un solo proveedor, aunque puede incluir componentes de hardware y software de varios fabricantes.
- El proveedor ha asignado un identificador de producto único en el sistema de control.

Por su parte, Security Development Lifecycle Assurance (SDLA) es una certificación que garantiza que los procesos del lifecycle para los SCI se han realizado correctamente.

2.1.5.6 Industrial Control System (ICS) Cyber Security: Recommended Best Practices

El Public Safety Canada (PSC) ha establecido las *Industrial Control System (ICS) Cyber Security: Recommended Best Practices*, en materia de ciberseguridad, para los Sistemas de Control Industrial. En concreto define 99 controles o buenas prácticas, distribuidas en 13 áreas de seguridad. La distribución de controles y de las áreas de seguridad es la siguiente:

1) Segmentación de red: 17 controles
2) Acceso remoto: 17 controles
3) Comunicación Wireless: 13 controles
4) Gestión de Patch: 7 controles
5) Política y Control de Acceso: 10 controles
6) Seguridad en el Host: 7 controles
7) Detección de intrusiones: 6 controles
8) Seguridad Física y Medioambiental: 8 controles
9) Protección y Detección de Malware: 3 controles
10) Concienciación: 3 controles

11) Auditorías y evaluaciones periódicas: 3 controles

12) Gestión de las configuraciones y control de cambios: 4 controles.

2.1.5.7 ISREC Catalogue

El británico Centre for the Protection of National Infrastructure (CPNI) promueve las mejores prácticas entre los operadores de la infraestructura nacional, ofreciendo diversos servicios para la protección de los operadores: guías de seguridad, asesorías, recomendaciones para mitigar vulnerabilidades, directrices acerca de buenas prácticas, etc. En este sentido ha promovido el trabajo del comité *Industry/Sector Related Expert Committee* (ISREC), que está focalizado en la seguridad de las IICC, orientadas a la información, en los sectores de finanzas y energía. ISREC ha desarrollado un catálogo de 184 medidas de seguridad categorizadas en 20 dominios de seguridad.

2.1.5.8 CSPN

En Francia se estableció el proceso de certificación que tiene el nombre de *Certification Sécurité Premier Niveau* (CSPN). Esta certificación se fundamenta en los criterios, la metodología y en los procesos desarrollados por la Agencia nacional de seguridad de la información (ANSSI).

La certificación CSPN está enfocada en certificar herramientas de seguridad, productos destinados a proteger la información relativa a la defensa nacional y proveedores de servicios confianza. La certificación CSPN tiene un carácter voluntario.

La autoridad gubernamental Secretaría General de la Defensa y la Seguridad Nacionales (SGDSN) obliga a los operadores estratégicos a elaborar un Plan de Seguridad del Operador, que contenga información relativa a los siguientes aspectos:

- Escenarios de amenazas.
- Evaluación del Riesgo.
- Medidas de seguridad.
- Principales activos.

El ministerio responsable de cada sector aprueba la respectiva planificación de la seguridad del operador, debiendo ser validado el documento final por parte de la SGDSN.

Por último, los operadores tendrán que elaborar el Plan de Protección Externo, en el que se incluyen: el tipo de vigilancia, las respuestas a las alertas, la intervención de las fuerzas de seguridad, etc.

2.1.5.9 ISO/IEC 27000

La serie de normas ISO 27000 (ISO/IEC_27000, 2014) son posiblemente el marco normativo más generalizado en gestión de la SI.

Figura 2.7. Dominios ISO 27002:2013

La norma ISO/IEC 27001, en su apartado 4.2, agrupa las 30 actividades de gestión de la SI (véase Figura 2.8):

Actividades del sistema de gestión de la seguridad (SGSI) en ISO/IEC 27001

4.2.1 Creación del SGSI

a) Definir el alcance.
b) Definir una política de seguridad.
c) Definir el enfoque de la evaluación de riesgos de la organización.
d) Identificar los riesgos.
e) Analizar y valorar los riesgos.
f) Identificar y evaluar las opciones para el tratamiento de riesgos.
g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
h) Obtener la aprobación de los riesgos residuales propuestos.
i) Obtener la autorización para implementar y operar el SGSI.
j) Elaborar una declaración de aplicabilidad.

4.2.2 Implementación y operación del SGSI

a) Formular un plan de tratamiento de riesgos.
b) Implementar el plan de tratamiento de riesgos.
c) Implementar los controles seleccionados.
d) Definir el modo de medir la eficacia de los controles.
e) Implementar programas de formación y de concienciación.
f) Gestionar la operación del SGSI.
g) Gestionar los recursos del SGSI.
h) Implementar procedimientos y controles para detección y respuesta a incidentes de seguridad.

4.2.3 Supervisión y revisión del SGSI

a) Ejecutar procedimientos de supervisión y revisión.
b) Realizar revisiones periódicas de la eficacia del SGSI.
c) Medir la eficacia de los controles.
d) Revisar las evaluaciones de riesgos en intervalos planificados y revisar los riesgos residuales.
e) Realizar las auditorías internas del SGSI en intervalos planificados.
f) Realizar una revisión general del SGSI.
g) Actualizar los planes de seguridad.
h) Registrar las acciones e incidencias que pudieran afectar a la eficacia o al funcionamiento del SGSI.

4.2.4 Mantenimiento y mejora del SGSI

a) Implementar en el SGSI las mejoras identificadas.
b) Aplicar las medidas correctivas y preventivas adecuadas.
c) Comunicar las acciones y mejoras a todas las partes.
d) Asegurar que las mejoras alcancen los objetivos previstos.

SGSI = Sistema de Gestión de la Seguridad de la Información o modelo formalizado con el que se gestiona la seguridad de la información. La Norma UNE-ISO/IEC 27001 define este sistema de gestión.

Fuente: UNE-ISO/IEC 27001:2007

Figura 2.8. Actividades del SGSI en ISO/IEC 27001.

2.1.5.10 Security by Design with CMMI-DEV

El desarrollo de aplicaciones y productos seguros requiere un enfoque metodológico y sistemático que permita abordar los proyectos de forma segura. Así, para abordar proyectos seguros que finalicen aportando productos seguros, el enfoque de Seguridad por Diseño identifica un conjunto de técnicas específicas, habilidades, experiencia y capacidades conforme al modelo CMMI-DEV, v.3.

El modelo Seguridad por Diseño presenta cuatro áreas de proceso que orientan los procesos de desarrollo: dos áreas en SI en ingeniería, un área para la gestión de la SI en proyectos, y otra para los temas de SI de la organización.

El modelo se puede utilizar como marco para evaluar y mejorar la capacidad de una organización en el desarrollo de productos seguros y como marco para evaluar la capacidad de un proveedor de productos con seguridad crítica.

2.1.5.11 ISO/IEC15408 / Common Criteria

ISO / IEC 15408-1 es una norma resultante del *Common Criteria Project Sponsoring Organizations* que permite evaluar la seguridad de las tecnologías de la información. Abreviado como *Common Criteria* esta norma dispone a su vez de la metodología de soporte *Common Evaluation Method* (ISO/IEC_15408, 2009b) que permite evaluar la seguridad de los sistemas de TI en una entidad. No sólo sirven de base para la certificación, sino que actúan como herramienta de ayuda a la mejora de los sistemas de seguridad.

Con su desarrollo se facilitó la homogenización de los sistemas de evaluación de las características de seguridad para productos TI en Europa, Canadá y Estados Unidos, facilitando la expansión de un mercado global como el de la ciberseguridad.

La evaluación conforme los *Common Criteria* se centra en criterios técnicos más que de tipo jurídico o de gestión, previendo actuaciones de tipo tanto subjetivas como objetivas.

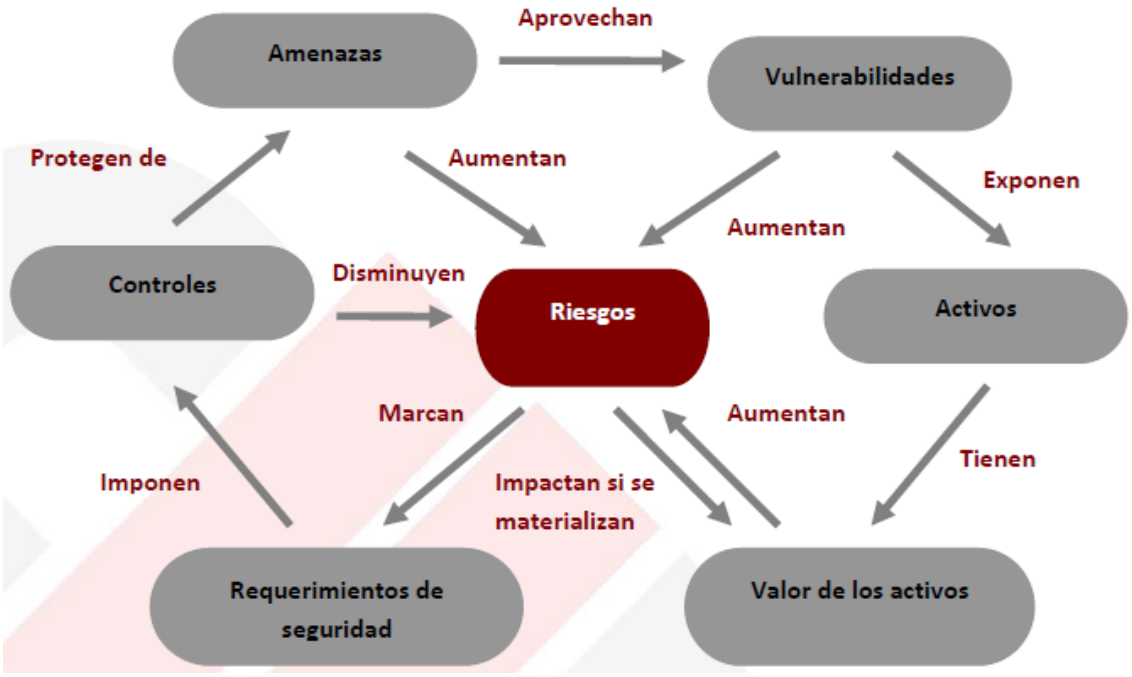
Esta norma establece un rango de evaluación a partir de siete niveles y, como principal ventaja, la cuantificación de criterios permite la certificación por entidades cualificadas, lo que no evita que tenga un nivel de complejidad técnica especialmente difícil de abordar por pequeñas organizaciones.

2.1.5.12 Metodologías de Análisis de Riesgo

El análisis de riesgos es un elemento inseparable del proceso de gestión de la SI a nivel de planificación y estrategia.

Cabe mencionar en este apartado los métodos que facilitan el análisis sistemático de riesgos. A nivel internacional, el método CRAM o *CCTA Risk Analysis and Management* desarrollado por la *Central Computer and Telecommunications Agency* (CCTA). Otros modelos como MAGERIT, Mosler (Rodríguez et al. 2013) o la metodología PILAR[19], todos comparten una serie de elementos que quedan representados en la figura 2.9:

Figura 2.9. Elementos comunes de las metodologías de análisis de riesgos (Fuente: Barrio y Ramos (2012: p. 14):



2.1.5.13 Estudio comparativo de guías de seguridad

El proceso de estudio de este apartado ha sido el mismo que el que se ha utilizado en los apartados relativos a la gobernanza, la gestión de servicios de tecnologías de la información, la gestión del ciclo de mejora de procesos y la gestión de proyectos. El resultado del estudio de estos elementos aporta información relativa a los mecanismos y técnicas para el aseguramiento de los productos de desarrollo a nivel del SW Lifecycle del proyecto desde la perspectiva de seguridad en sí misma en los distintos marcos y estándares propuestos.

[19] administracionelectronica.gob.es/ctt/pilar

Tabla 2.6. Consideraciones finales sobre las guías, estándares y marcos de gestión de seguridad

CÓDIGO	Factor a estudiar	NERC CIP	NRC-RG 571	CFATS	PCI DSS	ISA/IEC 62443	ICSCS	ISREC	CSPN	ISO/IEC 27000	SbD CMMI DEV	COMMON CRITERIA	METODOLOGIAS DE ANALISIS DE RISGO
GS_01	Política de seguridad en proyecto de desarrollo de software seguro	◗	◗	◗	◗	◗	◗	◗	○	◗	◗	○	○
GS_02	Plan de seguridad del desarrollo de software en el proyecto	●	●	●	◗	◗	◗	◗	◗	◗	◗	◗	◗
GS_03	Criterios de evaluación de vulnerabilidades de activos de desarrollo	●	●	●	●	●	○	○	○	◗	◗	○	○
GS_04	Criterios de evaluacion de seguridad de activos de desarrollo	●	◗	●	◗	◗	◗	●	◗	◗	◗	◗	◗
GS_05	Criterios de evaluación de riesgos de seguridad en desarrollo	◗	●	◗	◗	◗	◗	●	◗	◗	◗	◗	◗
GS_06	Declaración de riesgos de seguridad en desarrollo	●	●	●	●	●	●	●	◗	◗	◗	◗	◗
GS_07	Declaración de viabilidad de proyecto de desarrollo de software seguro	●	●	●	●	●	●	●	◗	◗	◗	◗	◗
GS_08	Parametrización de seguridad en proyecto de desarrollo	◗	◗	◗	●	●	◗	◗	◗	◗	○	○	○

GS_09	Medida de seguridad de desarrollo de software	◗	◗	◗	●	●	●	●	○	◗	○	○	○	
GS_10	Objetivos de control de seguridad de desarrollo de software	●	●	●	◗	◗	○	○	●	◗	○	○	○	
GS_11	Controles de seguridad en desarrollo de software	●	●	◗	●	●	●	●	●	◗	◗	◗	◗	
GS_12	Registro de umbrales y valores de seguridad en desarrollo de software	●	◗	◗	◗	●	◗	◗	●	◗	◗	◗	○	
GS_13	Auditorías de seguridad en desarrollo de software	●	◗	◗	◗	◗	○	○	○	○	○	○	○	
GS_14	Alternativas soluciones de seguridad en desarrollo de software	●	◗	◗	◗	◗	○	○	◗	◗	○	○	○	
GS_15	Plan de tratamientos de riesgos de seguridad	●	◗	●	◗	◗	◗	◗	◗	◗	◗	◗	◗	
GS_16	Gestión integrada de incidentes de seguridad en desarrollo de software	●	◗	●	◗	◗	◗	◗	◗	◗	◗	◗	○	
GS_17	Gestión de problemas de seguridad en desarrollo de software	●	◗	●	◗	◗	◗	◗	◗	◗	◗	◗	○	
GS_18	Gestión de configuración y activos de seguridad (PAL)	●	◗	●	◗	◗	◗	◗	◗	○	◗	◗	○	
GS_19	Gestión de proveedores de producto software seguro	●	◗	●	◗	◗	◗	◗	◗	◗	◗	◗	○	

GS_20	Gestón de conocimiento de seguridad en desarrollo de software	●	◗	●	◗	◗	◗	◗	◗	◗	◗	◗	◗	○
GS_21	Informes de seguridad en desarrollo de software	●	◗	●	◗	◗	◗	◗	◗	◗	◗	◗	◗	◗
GS_22	Plan de formación y desarrollo de competencias de seuridad en desarrollo de software	●	◗	●	◗	◗	◗	◗	◗	◗	◗	◗	◗	○
GS_23	Plan de concienciación de seguridad en desarrollo de software	●	◗	●	◗	◗	◗	◗	◗	◗	◗	◗	◗	◗
GS_24	Plan de mejora de seguridad desarrollo de software	●	◗	●	◗	◗	◗	◗	◗	◗	◗	◗	◗	◗
GS_25	Específico para IICC	●	◗	●	◗	◗	◗	◗	◗	○	○	○	○	

2.2 Revisión Sistemática

Con el objetivo de completar los trabajos realizados en el apartado 2.1, se va a realizar una evaluación sistemática de la literatura de los 10 últimos años, en relación a la gestión de proyectos segura en los entornos industriales y específicamente de infraestructuras críticas. En base a esta revisión, se podrán establecer algunas conclusiones en cuanto al estado del arte en el tema del Trabajo Fin de Master y, posteriormente, definir las hipótesis de trabajo.

Biolchini *et al.* (2005) proponen un método para realizar revisiones sistemáticas enfocadas a la ingeniería de software, que es aplicado por otros autores en trabajos de revisiones sistemáticas en relación a la gestión de proyectos como el que se presenta en (Calvo-Manzano, Cuevas, Gasca, San Feliu, & Vega, 2009), (Grossi & Calvo-Manzano, 2008), (Mesquida, Mas, Amengual, & Calvo-Manzano, 2012) (Bayona, Calvo-Manzano, & San Feliu, 2012). Se utilizará el protocolo marcado por Biolchini *et al.* (2005) comenzando por la definición de los objetivos de la evaluación para determinar el enfoque de la pregunta, estableciendo las fuentes de consulta y los criterios de exclusión e inclusión a aplicarse en el estudio, para proceder a la extracción de los datos y síntesis de resultados.

2.2.1 Objetivos de la revisión

Partiendo de la base de la problemática planteada en el capítulo anterior, en esta fase de la revisión sistemática se plantean preguntas cuya respuesta podría encontrarse en la literatura científica. Para ello, siguiendo el protocolo definido en Biolchini *et al.* (2005), se plantean las siguientes cuestiones:

- Problema (contextualizar el objetivo de la revisión sistemática). La falta de trayectoria en ciberseguridad de las IICC, así como de experiencia y de un marco de seguridad apropiado a este tipo de organizaciones, hace que sean un objetivo de interés para los ciberatacantes. Por lo tanto, la inversión realizada en estos proyectos necesita añadir una componente de seguridad, tanto en la gestión de sus procesos como en los resultados o productos de estos proyectos. Por ello resulta conveniente definir un marco para la gestión segura de proyectos TI adaptado a las necesidades de las IICC.
- Pregunta que orienta la revisión sistemática: ¿Qué modelos hay para el desarrollo seguro en las IICC?
- Resultados esperados: iniciativas y métodos propuestos para ayudar a desarrollar y evaluar la seguridad de los procesos y los productos de gestión de los proyectos TI en IICC.
- Medición del resultado: Número de propuestas identificadas.
- Población observada. Publicaciones sobre seguridad de los proyectos TI en entornos industriales de IICC.

- Aplicación de los resultados: Personal responsable de proyectos TI en general, responsables de seguridad, usuarios de TI de cualquier nivel organizativo en cualquier IICC que utilice la TI, e investigadores que trabajen en campos relativos a la seguridad y la gestión de proyectos TI en IICC.

Siguiendo el protocolo de Biolchini *et al.* (2005), se definen la continuación las fuentes sobre las que realizar la revisión sistemática, por lo que se han elegido BBDD reconocidas para el tema de nuestro Trabajo Fin de Master. Dos son los portales que albergan las BBDD seleccionadas por su carácter general y su disponibilidad a través de la Biblioteca de la UNED:

Tabla 2.6. Revisión sistemática. BBDD.

1	Portal ACM Portal	http://portal.acm.org/portal.cfm
2	Springer Link	http://www.springerlink.com

Partiendo de la búsqueda de estudios primarios relacionados con la seguridad en los procesos de administración de proyectos de desarrollo SW a partir de la metodología *SbD* de Siemens, investigador del SEI (SEI, 2013_b) y los resultados de la aplicación de los distintos marcos, guías o técnicas de gestión de proyectos segura en IICC, la revisión sistemática se realiza para el conjunto de palabras clave siguiente:

- {MANAGEMENT,
- PROJECT,
- SECURITY,
- DESIGN,
- CRITICAL INFRASTRUCTURES,
- CSSP,
- TSP,
- CSEP,
- NERC CIP,
- NRC RG 5.71,
- CFATS,
- PCI DSS,
- ISA/IEC 62443,
- NIST FRAMEWORK
- CSPN}

Además, se ha incluido "Security by Design", combinando mediante los operadores lógicos AND y OR las siguientes cadenas:

1. Para responder Gestión de Proyectos con Seguridad por Diseño en IICC: ((PROJECT) AND (MANAGEMENT) AND (SECURITY) AND (DESIGN)) AND (CRITICAL INFRASTRUCTURES).
2. Buscando sinónimos y los marcos y guías más reconocidos a nivel internacional: (Critical infrastructures AND (INDUSTRY OR ORGANIZATION OR COMPANIES OR TEAMS OR FIRMS OR SETTINGS)) AND ((SECURITY) AND (MANAGEMENT) AND (PROJECT)) AND (NIST OR CSSP OR TSP OR NERC OR RG571 OR CFATS OR PCIDSS OR 62443 OR CSPN).

Tabla 2.7. Revisión sistemática. Resultados de Búsqueda.

	FUENTE	Último acceso	Descubiertos	Rechazadas	Relevante	No disponible	Primarios
1	ACM Portal (Digital Library & Guide)	12/07/2016	B-76 C- 4	B-49 C-2	B-29 C-2	B-9 C-0	8
2	Springer Link	18/07/2016	C-289	C-231	C-44	C-17	13

La columna "Rechazadas" indica el número de publicaciones que fueron rechazadas en base a los factores siguientes (Kitchenham, 2007):

Tabla 2.8 Criterios a revisar.

CI_1	Documentos referidos a las palabras IICC y "Seguridad por diseño".
CI_2	Documentos coincidentes con la cadena de búsqueda.
CI_3	Documentos con resumen relacionado con la búsqueda
C_I4	Documentos con referencias a modelos de gestión de proyectos TI seguros en entornos industriales de IICC.
CE_1	Documentos excluidos pese a estar relacionados con la gestión de seguridad pero no con entornos de IICC
CE_2	Exclusión de documentos duplicados entre las BBDD

2.2.2 Resumen de resultados

Siguiendo las pautas del trabajo de Biolchini *et al.* (2005), en este apartado se adapta el protocolo propuesto para presentar los hallazgos encontrados a partir de los estudios realizados en este Trabajo Fin de Master. Para ello, se analizan los siguiente aspectos relativos a la tendencia de las publicaciones seleccionadas en relación al tema de estudio de este TFM (véase Tabla 2.7).

En el período estudiado (véase Tabla 2.9), se observa un creciente interés desde 2013 coincidiendo con la expansión mundial de los sistemas regulatorios sobre seguridad en entornos de IICC. El pico observado en 2014 podría tener su justificación en el interés que este trabajo causa entre los distintos profesionales relacionados con la gestión segura de los proyectos TI, desde distintas perspectivas.

Tabla 2.9. Tendencia anual de publicaciones relevantes.

2007	5
2008	5
2009	9
2010	7
2011	4
2012	4
2013	8
2014	14
2015	8
2016	9

El resultado de la investigación arroja como resultado la presencia de un total de 36 autores, de los cuales 4 son entidades tales como el Centro de ciberseguridad y análisis forense de la Universidad de Tallin, la Unit of ICT Research in Security and Trust, de la Comisión Europea o el CNRS francés y el del Italian National Research Council. Estos autores desarrollan su actividad profesional en 17 instituciones distribuidas geográficamente a lo largo de cuatro continentes (véase Tabla 2.10). En el 90% de las instituciones se cita 1 trabajo en relación con el tema de este Trabajo Fin de Master y tan sólo en el 10% se han encontrado 2 trabajos. El 66% de los trabajos se realizaron en alguna institución de Europa.

Tabla 2.10. Instituciones de trabajo de las fuentes primarias

	Instituciones	**Nº de Trabajos**
1	Universidad de Tolouse/ IRIT-CNRS	3
2	Universidad de Málaga	2
3	University of Luxembourg	2
4	Unit of ICT Research in Security and Trust, de la Comisión Europea	1
5	Italian National Research Council, ISTI	1
6	University of Twente	1
7	Tallin University of Technology	1
8	Universidad de Gröeningen	1
9	University of Seoul	1
10	University of Illinois	1
11	Universitá di Napoli	1
12	University of South Australia	1
13	Jamia Millia Islamia, New Delhi	1
14	Florida State University	1
15	McAffee	1
16	Symantec	1
17	Wien Universität	1

Destacan los trabajos de los siguientes autores:

- Los doctores Anas Abou El Kalam e Yves Deswarte, de la Universidad de Tolouse y el IRIT - CNRS, participan en 3 de los trabajos seleccionados, apareciendo como autores principales en (El Kalam & Deswarte, 2009; Deswarte, 2011) y como autores secundarios en (Baina *et al.*, 2008).

- T. Schaberreiter de la University of Luxembourg con dos trabajos sobre modelos y redes de IICC (Schaberreiter et al. 2011; 2013)
- Los doctores Bart Van Caenegem y Thomas Skordas de la Unit of ICT Research in Security and Trust, de la Comisión Europea (Van Caenegem & Skordas, 2007).
- WoongChul Choi y DaeHun Yoo de la Universidad coreana de Seúl.
- Silvano Chiaradonna et al. Consejo de Investigaciones científicas de Italia, ISTI, y Paolo Lollin de la University of Firenze (Chiaradonna, Giandomenico and Lollini 2008).
- El equipo de E. Zambon y S. Etalle de la University of Twente (Zambon et al. 2009).
- Hayretdin Bahsi et al. de la Universidad de Tallin (Bahsi & Maennel, 2009).
- Daniel Feitosa, doctorando de la Universidad de Gröeningen realiza en 2014 una revisión sobre modelos de desarrollo en sistemas software embebidos de carácter crítico (Feitosa, 2014).
- Sobre Gestión de Servicios IT y aseguramiento de Software, WoongChul Choi y DaeHun Yoo de la KwangWoon University, Seoul, Korea.
- Sobre modelos SDL: Joan Gregoire et al., de la Katholieke Universiteit Leuven.
- Sobre SCADAS, Christophe Feltus, del Centro Henri Tudor, de Luxemburgo.
- Sobre modelos de desarrollo seguro, Haralambos Mouratidis, de la Universidad de Brighton.
- Sobre Vulnerabilidades, Laura Falk et al (2008) of University Michigan, USA
- Sobre métricas y modelos de desarrollo seguro, Xueqi Cheng et al (2008) of Tianjin University, China; y Suhaila Ismail, Elena Sitnikova, and Jill Slay de la University of South Australia.
- Sobre casos de uso: William H. Sanders, de la University of Illinois.
- Sobre Gestión de incidentes en IICC, L. Coppolino et al. de la Universitá di Napoli "Parthenope"
- Finalmente, en España se han destacado las publicaciones del equipo de Javier Lopez, Cristina Alcaraz, y Rodrigo Roman de la Universidad de Málaga tanto sobre IICC como SCADA en IICC (López & Hämmerli, 2007).

En cuanto al conjunto de palabras clave utilizadas para la búsqueda, no todas las publicaciones, proporcionaban alguna de las palabras clave definidas. Algunas revistas científicas o técnicas de organizaciones no imponen en sus publicaciones el uso de palabras clave. Además, las cadenas de búsqueda definidas en el protocolo se tuvieron que adaptar a los buscadores. Después de la lectura de los resúmenes y, en algunos casos, del documento completo, se fueron identificando nuevas palabras que ampliaron el conjunto de palabras clave inicial, y la búsqueda se adaptó a las palabras clave de los artículos y trabajos encontrados.

Este nuevo conjunto de palabras clave fue alimentándose con el descubrimiento de diferentes intereses encontrados en los distintos trabajos, y permitió identificar y clasificar

nuevos trabajos relacionados con algún aspecto relacionado con el tema del Trabajo Fin de Master. Posteriormente, fue utilizado para la clasificación de los mismos en cuanto al tema de estudio.

Tabla 2.11. Clasificación en la extracción de datos. Resultados.

PALABRAS CLAVE	**% inclusión**
Acceso	3
Aplicación metodología	1
Arquitectura	1
Common criteria	1
Conformidad (Compliance)	1
Confianza (trust)	3
Dependencia	2
Desarrollo	1
Diseño	5
Confiabilidad (reliability)	5
Evaluación (evaluation, assessment)	3
Gestión (management)	3
Infraestructuras críticas	8
Integración	1
Languages	2
Mitigación	1
Medición (measurement)	1
Modelos	17
Normalización (standardization)	2
Políticas (Policies)	9
Privacidad	1
Procesos	1
Rendimiento (performance)	3
Regulación	1
Requisitos	2
Riesgos	3
SCADA	6
Investigación (research)	5
Seguridad (security, cybersecurity)	22
Validación (verification, checking)	8
Vulnerabilidades	10

Así, las palabras clave utilizadas en los trabajos, reflejadas en la Tabla 2.11, reflejan que el 22,6% de los trabajos encontrados están encaminados a los modelos de gestión de proyectos, el 29,3% trata aspectos de seguridad en el desarrollo de proyectos en IICC y el 13,3% habla de algún aspecto específico como las vulnerabilidades en IICC. El resto de palabras clave tuvieron una presencia menor, sin embargo el conjunto de ellas, dan una idea de los aspectos investigados.

Finalmente, destacar que el término *Security by Design*, no se encuentra entre las palabras clave del sistema de clasificación de ACM-IEEE (ACM, 2012), por lo que se ha recurrido al trabajo de referencia de De la Cámara (2016) para extraer las referencias hemerográficas y bibliográficas sobre este modelo genérico.

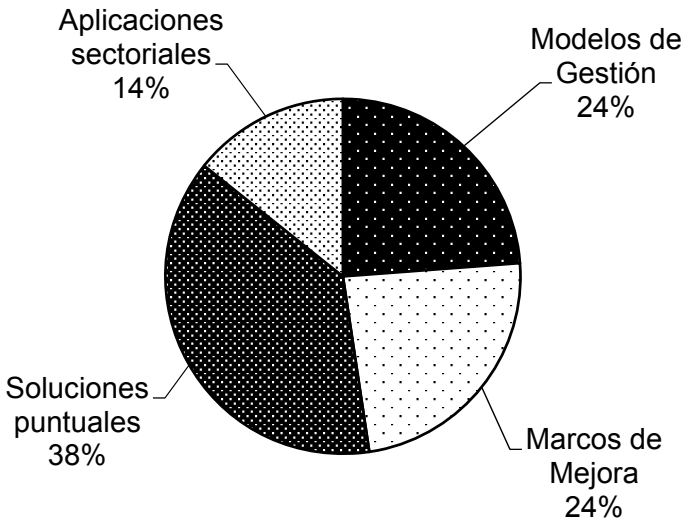
2.2.3 Consideraciones finales de la revisión sistemática

De acuerdo a los estudios encontrados y las palabras clave, se puede hacer una clasificación de los temas de investigación relacionados con el tema del Trabajo Fin de Master utilizando las siguientes categorías de estudio:

- Marcos de mejora de procesos (generalistas): (ISACA, 2009), (Kobashi, y otros, 2011), (Arboleda, Paz, & Casallas, 2013), (Arcilla, Calvo-Manzano, & San Feliu, 2013), (Sarriegi, Torres, & Santos, 2005) y (Curphey, 2009).
- Gestión de servicios IT y aseguramiento del software (Choi & Yoo, 2009)
- Sobre modelización y simulación de IICCC (Schaberreiter et al. 2011; 2013)
- Modelos de gestión de proyectos en IICC:
    - General: El Kalam & Deswarte (2009); Deswarte (2011); Bahsi and Maennel, 2009; Kaufmann et al. (2015)
    - SDL: (Gregoire et al, 2007)
- Soluciones Puntuales:
    - Gestión de incidentes en IICC: Coppolino et al. (2007)
    - SCADA: (Feltus & Khadraoui, 2013), (Blangenois et al. 2013).
- Aplicaciones en sectores IICC
    - Sector eléctrico (Sanders, 2012).
    - Transversales (Baker et al., 2010).
    - ICT (Van Caenegem & Skordas, 2007).
- Vulnerabilidades: (Rehman & Mustafa, 2009).
- Métricas: (Sánchez, Villafranca, Fernández-Medina, & Piattini, 2009); métricas y seguridad (Chen *et al*., 2009) y métricas en IICC (Ismail et al, 2014).
- Análisis de riesgos en IICC: Zambon et al. (2009).
- Evaluación de IICC: Chiaradonna, Silvano; Di Giandomenico, Felicita and Lollini, Paolo (2008) y Schmitz (2007).

En resumen, como se muestra en la Figura 2.10, el 48% de los trabajos presentan investigaciones sobre modelos y marcos de gestión de proyectos para el desarrollo seguro a lo largo de todo el Project lifecycle, para IICC.

Figura 2.10. Resultados de las investigaciones primarias sobre IICC



Existe una gran cantidad de trabajos publicados sobre seguridad del software y desarrollo de herramientas, atendiendo las vulnerabilidades y su clasificación (Wang and Guo, 2009; Chen et al. 2009), la detección y los fallos de diseño de software (Falk, 2008; Hadavi, 2008). Destacan las publicaciones orientadas a evaluar la seguridad en las diferentes fases del Sw Lifecycle (Rehman & Mustafa, 2009). El análisis de la SI a través del ciclo de desarrollo de software (SDC) ha llevado a diferentes propuestas de marcos para el desarrollo de sistemas seguros interesantes. De este modo, Chandra (2006) dirige el desarrollo, en el proyecto CLASP, de un módulo que puede integrarse en otros procesos como RUP (Rational Unified Process). Mouratidis y Giorgini (2007) desarrollan una funcionalidad integrada en la metodología Tropos y Mouratidis et al (2006) un marco de desarrollo seguro al completo. Meland y Jensen (2008) proponen por su parte un esquema de desarrollo de software orientado a la seguridad (SODA) también en una versión de sistema automatizado de desarrollo de software.

Otra segunda área que ha asistido a importantes líneas de investigación en la última década ha sido la de patrones de diseño seguro. Dougherty et al. (2009) del SEI propusieron los “Secure Design Patterns” como plantillas que permiten una solución general ante un problema de seguridad que pueda aplicarse en muchas situaciones diferentes.

2.3 Resultados del estado del arte

Se ha evaluado el estado del arte relativo al tema del Trabajo Fin de Master desde diferentes perspectivas organizativas: a nivel estratégico, se ha tenido en cuenta el punto de vista de gobernanza; a nivel táctico, los ciclos de mejora continua en procesos y en la service management; y a nivel operativo, se han estudiado distintos modelos de Project

management y administración de SI. El estudio se complementa con una revisión sistemática del tema del TFM.

El estudio comparativo, en los tres niveles estudiados, ha demostrado que en ninguno de ellos existe un modelo que proporcione información completa y dirigida sobre las actividades y técnicas de gestión segura de proyectos que aseguren aportar un producto o servicio seguro. Incluso en modelos normativos como pueden ser los marcos NERC-CIP o CFATS, los dos más extendidos a nivel de IICC en Estados Unidos, el alcance de ambos se circunscribe a subsectores de IICC muy específicos como la industria energética o química. Igualmente sucede con el modelo NRC-RG, específico para instalaciones nucleares.

En el plano de la estrategia, los marcos normativos existentes contemplan generalizadamente las políticas de seguridad aunque no se concreta su aplicación. En lo que a las normativas de control, alguno de los modelos normativos como FISMA en los Estados Unidos o la estrategia europea y española de protección de IICC, definen procesos y actividades encaminados a la gestión de la SI en proyectos de desarrollo de tecnologías de la información, en las áreas de operaciones y desarrollo. De tal modo, sólo se han identificado regulaciones, en Estados Unidos, para cumplir con ciertos criterios de seguridad en entornos industriales de los subsectores energético, químico y nuclear. Estas regulaciones tienen un elevado grado de madurez, algunas datan del año 2006 y son periódicamente revisadas y mejoradas. Además, todas las regulaciones se basan, directa o indirectamente, en la Protección de IICC, y crecientemente se ven orientadas a la lucha antiterrorista. En el caso de España, se han identificado algunos antecedentes de modelos de certificación muy ligados al sector financiero y que pueden ser considerados como referentes (certificación de seguridad en sistemas relacionados con medios de pago PCI DSS y los nuevos criterios de supervisión del BCE – SSM referentes a ciberseguridad).

Las regulaciones identificadas están legisladas y son promovidas por organismos gubernamentales en los que siempre tienen presencia los agentes públicos o privados sectoriales, lo que facilita el diálogo y la aproximación al principio de autorregulación de las empresas, sin embargo, aunque se establecen pautas y actividades de lo que hay qué hacer, no se especifica el cómo.

A nivel táctico, los marcos de gestión de servicios establecidos por marcos como el NIST Framework o el canadiense TSP Best practices establecen un conjunto de recomendaciones y buenas prácticas para la seguridad relativa a la gestión del proyecto de desarrollo. Los modelos generalistas tales como ITIL e ISO 20000, también los modelos de madurez, complementan las recomendaciones actividades aconsejables en la administración de servicios de tecnologías de la información.

El hecho de que no se hayan identificado certificaciones de seguridad de sistemas de gestión industrial en referencia a la seguridad de las IICC, es una evidencia de la dificultad para establecer marcos definidos de aplicación de la gestión de servicios. Existe una carencia de modelos orientados a la mejora, como podrían ser modelos de madurez, que permitan una evaluación continua mediante indicadores de los avances en la implantación de sistemas eficientes y que se adecuen a estándares de calidad y seguridad como los que persigue la normativa de protección de infraestructuras críticas

A nivel operativo, se han visto distintos enfoques de modelos de gestión de proyectos en IICC, que pueden tener características dispares, si comparamos por ejemplo un entorno

industrial duro como el energético o el químico con otros como el de transporte, salud o una administración pública. Así, se han considerado para el análisis de la seguridad en los distintos modelos de gestión de proyectos tanto los enfoques predictivos (PSP, TSP) como los adaptativos (Ágiles). Aunque los métodos ágiles dan mejor resultado en proyectos pequeños y con estructuras organizativas muy planas, se ha visto que a nivel operativo, tampoco los modelos estudiados, sea cual sea el enfoque de gestión de proyecto, define cómo establecer mecanismos y técnicas para lograr la gestión del proyecto de desarrollo seguro aportando servicios/productos seguros y acorde a las directrices estratégicas y tácticas establecidas.

Además, y tomando como referencia los Estados Unidos, todas las regulaciones identificadas tienen un carácter sectorial, en concreto, los sectores identificados son el eléctrico, nuclear y químico, y específicamente se orientan al cumplimiento de estas regulaciones y está supervisado en orden a identificar los posibles incumplimientos y materializarlos en sanciones. En estos casos los niveles de requisitos y controles a implantar son muy detallados, teniendo como base estándares reconocidos internacionalmente y facilitando los criterios a las IICC, creando un marco homogéneo de requerimientos. En el lado contrario, están los muy específicos controles que presentan estándares generalistas muy extendidos como ISO 27002 pero cuya implementación resulta compleja.

Finalmente, a través de la revisión sistemática, se han descubierto otras investigaciones a nivel académico y empresarial que son muy relevantes para el desarrollo de este Trabajo Fin de Master. El análisis de esta información ha sacado a luz que no existe un trabajo que proporcione información exhaustiva sobre el tema del TFM. La información encontrada está dirigida hacia un aspecto muy concreto dejando al margen los demás, o son de carácter general. Sin embargo, los trabajos indican el interés y necesidad de investigar en el tema objeto de este Trabajo Fin de Master.

3. Planteamiento del problema e hipótesis de trabajo

En este capítulo se hace una reflexión sobre la problemática presentada en el contexto del Trabajo Fin de Master y se realiza un resumen de los trabajos de investigación más significativos que, hasta la fecha, aportan alguna solución a la administración de proyectos de seguridad en el desarrollo en entornos de IICC, necesarios a tener en cuenta para la definición de un marco de trabajo.

3.1 Visión general del problema

En el Capítulo 1 ha quedado reflejado que, de acuerdo al Directorio Central de Empresas (DIRCE), que elabora anualmente el INE, el número total de empresas en España ha alcanzado en 2015 las 3.186.878, (ONTSI, 2016). Por su parte, el sector de empresas industriales se sitúa como el sector con más representación dentro de las empresas con 10 o más empleados en España, un 21,3%, junto al sector de Transporte y almacenamiento y el de Informática, Telecomunicaciones y Audiovisuales, alcanza un total del 32,4% del total del sector empresarial español.

En el contexto que nos ocupa, se analizó el papel que desempeñan las TI en el sector de las IICC. El resultado de este análisis (ONTSI, 2016), sobre distintos sectores empresariales, reveló que el nivel de desarrollo tecnológico en estas organizaciones industriales crece a un nivel exponencial, constituyendo una de las tendencias tecnológicas más pujantes, por efecto de la apertura de estos entornos a Internet y las nuevas tecnologías, en lo que se ha dado en llamar Industria 4.O o la penetración exponencial de las tecnologías digitales en el ámbito industrial (INCIBE, 2016).

Asimismo en el Capítulo 1 se mostró que las IICC abordan los problemas de seguridad de las TI en general, y de los servicios y proyectos de TI, en particular, de una forma adhoc. Las pérdidas económicas de las empresas por problemas de seguridad en las TI se han disparado en los últimos años y, en ocasiones, poniendo en riesgo la continuidad de la actividad de negocio.

Igualmente se explicó el requerimiento de que las IICC aborden la administración de proyectos de seguridad en el desarrollo de tecnologías de la información. Distintas iniciativas, modelos, estándares y estudios surgen con esa finalidad. En el Capítulo 2 de este Trabajo Fin de Master se ha realizado una revisión de las experiencias en entornos de IICC, mediante un estudio en el que se abordan desde las tres perspectivas: estratégica, táctica y operativa.

De este estudio comparativo, cabe destacar que, en una parte importante de los modelos normativos tratan el problema de la seguridad en administración de proyectos para asegurar el cumplimiento de la regulación a nivel de *compliance*, dado que las exigencias normativas gubernamentales tienen un peso esencial en su vertiente sancionadora. No obstante, el objetivo que se pretende con este Trabajo Fin de Master es facilitar la adopción de medidas que garanticen que el producto/servicio sea seguro, no solamente a efectos de cumplir con las medidas regulatorias, sino alcanzando el nivel óptimo de seguridad desde la fase de diseño del servicio. En consecuencia el capítulo 2 se

complementa con una revisión sistemática de otros marcos y experiencias publicadas en relación a lo que se pretende en este Trabajo Fin de Master.

Así, del estudio comparativo de los principales marcos y estándares y de la revisión sistemática, se observó que los marcos NERC-CIP, NRC-RG o CFATS son los que más se aproximan al marco de este Trabajo Fin de Master, pero su alcance se limita a sectores de IICC como el energético, el nuclear o el químico, mientras que se carece de un modelo más versátil para a disparidad de sistemas industriales y de servicios críticos. Así, De la Cámara (2016) señala el marco SbD descrito por Siemens (2013), como el que más se aproxima al objetivo de desarrollar un Marco de gestión de proyectos seguros en pymes, representando un grupo de prácticas aconsejables en la administración de proyectos, desde su concepción hasta su validación, y enfocadas al producto de desarrollo.

Concluidos los trabajos de estudio y comparación de los principales modelos y normas y la revisión sistemática, se pudo observar que hay un vacío en relación al tema de nuestro Trabajo Fin de Master motivado por:

- El predominio del enfoque normativo en la *compliance*, respecto de la normativa gubernamental y primando el cumplimiento con la legislación sobre la prioridad *per se* de la necesaria seguridad para optimizar el funcionamiento de la infraestructura.
- Las recomendaciones y pautas propuestas se tratan generalmente de orientaciones pero sin concreción aplicativa.
- La aplicación de los modelos y normas en el entorno de las IICC es difícil y requiere disponibilidad de recursos y experiencia de la que carecen incluso las empresas del sector TIC.

Con todo ello, el trabajo realizado en el Capítulo 2 de este Trabajo Fin de Master aporta un conjunto de factores de seguridad basados en SbD, deseables para cualquier marco de trabajo o modelo de proceso aplicable en la adminstración de proyectos de SI en tecnologías de la información (De la Cámara, Sáenz, Calvo-Manzano, & Arcilla, 2015). Esta estructura de factores de seguridad sirve para acercarse a una solución del problema explicado en el apartado siguiente y para la definición de las hipótesis de nuestro TFM.

3.2 Aproximación a la solución

Por ello, en este Trabajo Fin de Master se detalla una solución al problema a través de la definición de un patrón aplicable en la administración de proyectos de SI en desarrollo, abordable por las IICC, y que establezca un hilo conductor en todos los niveles organizativos de la organización, e integre directivas de gobernanza con las buenas prácticas de mejora de procesos.

Por lo tanto, el trabajo de investigación realizado en este TFM y las actividades que nos aproximan a la solución del problema deseada se pueden secuenciar como sigue:

1. Analizar los distintos procesos que tratan la gestión de la SI en los principales modelos y normas de gobierno y gestión de las TI en las IICC.

2. Establecer las bases para realizar un análisis comparativo de la seguridad en los procesos de gestión y desarrollo de SI y, posteriormente, realizar el análisis comparativo de los principales marcos definidos en el punto 1.
3. Realizar una revisión sistemática con objeto de completar este estudio e identificar nuevas prácticas, guías y modelos que faciliten la administración de proyectos para el desarrollo seguro. Poniendo especial interés en aquellas prácticas y guías que se aplican en el entorno de las IICC.
4. Comparar los principales resultados de la revisión sistemática con los resultados del punto 2 y estudiar si alguno de los resultados del punto 3 resuelve todos los problemas planteados en el apartado 3.1 de este capítulo.
5. Definir un marco de solución a la problemática presentada en las IICC. Esto se realiza en dos fases:
    a) En la fase 1, se define el modelo de proceso de administración de proyectos en SI y;
    b) En la fase 2 se detalla un patrón de gestión de proyecto seguro incluyendo los parámetros de seguridad necesarios a cada IICC.
6. Definir las técnicas y las guías que ayuden al usuario en la realización de las buenas prácticas propuestas en el marco de gestión del proyecto de desarrollo seguro en entornos industriales de IICC.
7. Validar el marco propuesto a través de su aplicación sobre un caso aplicado de IICC.
8. Identificar, a través de cuestionarios de evaluación, las oportunidades de mejora del marco propuesto.

Los puntos, del 1 al 4 han sido desarrollados en los Capítulos 1 y 2. En el Capítulo 4 se desarrollan los puntos 5 y 6. En el Capítulo 5 se desarrollan los puntos 7 y 8 contrastando el marco propuesto a través de la experimentación en un caso aplicado de proyecto concreto, identificando aquellos aspectos que sean susceptibles de ser mejorados, posibilitando la definición de patrones, que se adapten a las necesidades diversas de las IICC.

3.3 Hipótesis del trabajo

Siguiendo a De la Cámara (2016: p. 164), un marco de trabajo es una herramienta que facilita alcanzar las metas en las tareas en las que se aplica, el cual establece una guía que pueda repetirse y que ayude a mejorar los resultados de las acciones, reduciendo los errores más comunes.

Así, en este apartado se plantean las siguientes hipótesis del Trabajo Fin de Master:

1 HIPÓTESIS GENERAL. “Si una IICC, sea cual sea su sector de actividad, se apoya en un marco de trabajo que le facilite un patrón de seguridad aplicable en la gestión de sus proyectos para el desarrollo de proyectos de tecnologías de la información, conseguirá mejorar la seguridad del producto del proyecto durante el desarrollo”.

2 HIPÓTESIS DERIVADA 1. Si, una IICC redacta y transmite una Política de Seguridad y un Manual de seguridad detallado que la soporte, ofrecerá a los empleados de la organización, los objetivos y directrices para conocer los riesgos de sus activos de TI.

3 HIPÓTESIS DERIVADA 2. Si una IICC define un Catálogo de Requisitos de Seguridad podrá asociar, a cada activo TI, el/los requisitos de seguridad adecuados y, más tarde, gestionar eficazmente los controles o Activos de Seguridad TI que faciliten su cumplimiento.

4 Resolución

4.1 Introducción

Se propone GPS-IICC como un entorno de Gestión de Proyectos de desarrollo de SI en entornos industriales de IICC. Se trata de aportar una solución a la problemática presentada en el Capítulo 1 de este Trabajo Fin de Master.

Todos los componentes de seguridad que se definen, tanto en el modelo como en el patrón, formarán parte de una librería de activos de seguridad (SAL, Security Asset Library). El modelo que se define establece la estructura de la SAL que, a su vez será registrada en una BBDD de activos de seguridad.

En los sub-apartados que siguen se describen:

(1) las actividades necesarias para definir el modelo de proceso, detallando para cada actividad: entradas; salidas, tareas y KPIs (Key Performance Indicators) que faciliten su implantación y evaluación en las IICC;

(2) la estructura del patrón de proyecto TI seguro; y

(3) la estructura de la BBDD de activos de seguridad (SAL). Es necesario que la descripción sea detallada y aporte a las IICC mecanismos sencillos para su aplicación. Con ello, se mostrará la relevancia de la principal contribución de la investigación realizada.

Este capítulo constituye la base para la experimentación realizada en este TFM, cuyos resultados se muestran en el Capítulo 5.

4.2 Resolución del problema

La resolución del problema se plantea en dos fases. La primera fase, denominada “Fase de estandarización y definición”, se describe en este capítulo, y consiste en definir un marco de solución a la problemática presentada en las IICC. Esto se realiza a través de:

1. La definición del modelo de proceso de administración de proyectos SI para el desarrollo seguro estándar.
2. La definición detallada para un patrón de gestión de proyecto seguro que incluya los parámetros de seguridad necesarios con las características de seguridad adecuadas a cada IICC.
3. Definir las técnicas y las guías que ayuden al usuario en la realización de las buenas prácticas propuestas en el marco de gestión del proyecto de desarrollo seguro.
4. Validar el marco propuesto a través de su aplicación sobre distintos casos de proyectos, en IICC.
5. Identificar, a través de cuestionarios de evaluación, las oportunidades de mejora del marco propuesto.

La segunda fase, “Fase de evaluación”, se desarrolla en el Capítulo 5 de este Trabajo Fin de Master. Permite la evaluación del modelo de proceso, que se ha propuesto en este capítulo.

4.2.1 Estandarización y definición del modelo.

Se realizan los siguientes pasos preliminares:

- Seleccionar un Sector que ayude a la realización de un Piloto en el que se pueda desarrollar y probar el Modelo. En nuestro caso hemos seleccionado un Laboratorio de IICC especializado en el sector energético, uno de los más evolucionados en materia reguladora y en el que podremos contrastar la utilidad de nuestro modelo.
- Identificar los Actores que van a participar en el Piloto: organismos gubernamentales, agentes, operadores, empresas privadas, proveedores, etc.
- Definir los Roles y las Responsabilidades de cada uno de los actores intervinientes.
- Establecer las directrices del Modelo:
  - Agentes de la organización que van a participar.
  - Metodología que contemple los requisitos a cumplir.
  - Método y niveles de supervisión.
  - Planificación de tiempos y periodicidad de las supervisiones.
  - Nivel de madurez de la IICC seleccionada.

Además, el modelo debe tener las siguientes características:

- Estar integrado con otros estándares y normas aplicables a entornos industriales de IICC. Los componentes del modelo deben ser acordes a otras reglas y estándares que la organización deba o vaya a asumir.
- Ser replicable en entornos diversos y, por tanto, fácil de aplicar. Para ello, además de la sencillez, debe detallar un conjunto de componentes a los que se denominarán activos de seguridad que la organización utilizará en las tareas del modelo.
- Aportar un hilo conductor en las actividades de los distintos niveles organizativos de la organización.
- Ser medible.

Con el desarrollo de un modelo generalista, una vez establecido el modelo, cada IICC podrá elegir, en cada momento y dependiendo del contexto del proyecto, el patrón más adecuado que le sirva de guía.

4.2.2 Modelo estándar de proceso para la administración segura de proyectos de tecnologías de la información en IICC

El modelo estándar de proceso de gestión que se propone, denominado GPS-IICC, está basado en las mejores prácticas de SbD que tiene en cuenta aspectos de seguridad de proyectos de desarrollo seguro a nivel de estrategia, táctica y operativa. Respecto al análisis de marcos y modelos del Capítulo 2, se ha visto en el capítulo 1 que uno de los principales problemas que tienen las IICC es que la aplicación de estos marcos no es sencilla para ellas.

La principal ventaja de los Modelos Generalistas frente a los Sectoriales es que, realizando un estudio de aplicabilidad en función de los requisitos del entorno, se pueden utilizar en cualquier organización o sector. Por lo tanto, el marco GPS-IICC pretende aportar un modelo de proceso estándar fácil de utilizar y orientado a la seguridad de los servicios/productos TI, que facilite la definición de diferentes patrones de aplicación en las IICC, independientemente de las características del sector en el que se aplique.

Para desarrollar un modelo de proceso de GPS-IICC, este Trabajo Fin de Master toma como base del índice y elementos de normalización el modelo GPS-PYMEs desarrollado por De la Cámara (2016) para entornos empresariales. De este modo, estructuraremos nuestro submodelo para IICC a partir de cinco fases que a su vez despliegan una serie de actividades (De la Cámara, 2016: pp. 167-240):

1 ***Inicio y Dirección de Proyecto*** [ID]: Se define la política de seguridad se analizan riesgos y clasifican los activos que permitan identificar vulnerabilidades, amenazas y riesgos.
   - Actividad 1. Declaración de la política de seguridad.
   - Actividad 2. Definición de prerrequisitos de seguridad.
   - Actividad 3. Planificación y comunicación del plan de proyecto de seguro.

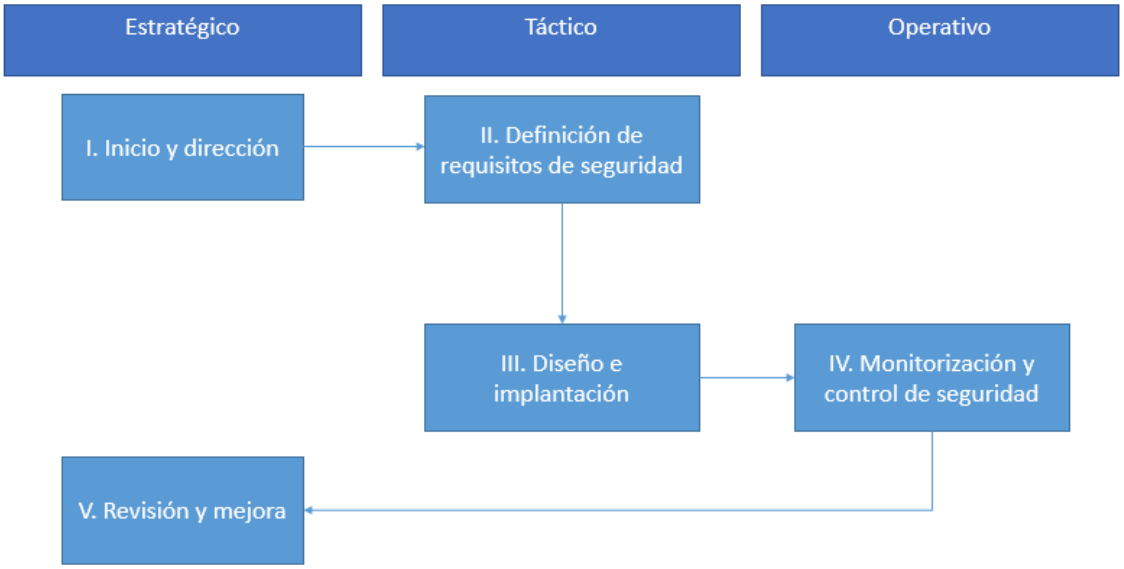
2 ***Definición de Requisitos de Seguridad*** [DRS]. Se definen los criterios de catalogación de requerimientos de seguridad y catalogan consecuentemente.

3 ***Diseño e Implantación de Solución de Seguridad*** [DISS]. Se diseñan e implantan las soluciones de gestión de los riesgos. Para ello, se diseñan e implantan controles a los que llamaremos Activos de Seguridad. Estos activos de seguridad se contemplan como herramientas facilitadoras de los requisitos de seguridad, mitigadora del riesgo y reductora del impacto de las amenazas sobre los activos de TI asociados a un Servicio/Proyecto.

4 ***Monitorización de las Soluciones de Seguridad*** [MSS]. Se gestionan los controles implantados en la fase III, y se realizan informes relativos a la evolución y cumplimiento de los requisitos definidos en las fases I y II.

5 ***Mejora Continua del Proyecto de TI seguros*** [MCP]. Se revisan los informes de monitorización y auditorías para realizar propuestas de mejora. Además, se comunican las decisiones a las partes implicadas.

Figura 4.1. Fases del marco GPS-IICC



4.2.1.1 Fase I. Inicio y Dirección

La fase Inicio y dirección del proyecto recoge las actividades previas de la organización antes de la aprobación para abordar el desarrollo en sí. El objetivo de esta fase es situar a la empresa en un estado inicial desde donde abordar un proyecto de desarrollo seguro. Para ello se plantean 3 actividades, cada una de ellas con un conjunto de prácticas específicas:

- A1 Declaración de la política de seguridad.
- A2 Definición de prerrequisitos de seguridad.
- A3 Planificación y comunicación del plan de proyecto de seguro.

4.2.1.1.1 I. A1. Declaración de la política de seguridad

Tabla 4.1. Prácticas Específicas para establecer la Política de Seguridad

Entradas	Tareas	Salidas	KPI
I. SP 1.1. Declarar la política de seguridad.			
-Estructura organizativa de la entidad. -Organigrama con las responsabilidades asignadas a cada área. -Calendario de elaboración y aprobación de la política. Registro de control de versiones del documento. -Descripción de los compromisos y obligaciones de la entidad, para el cumplimiento de sus objetivos en relación con la seguridad en los sistemas de información. - El nivel de confidencialidad del propio documento.	Definir la Política de Seguridad. Redacción de compromisos de la alta dirección en relación a: • Definir el manual de seguridad. • Realizar un análisis y tratamiento de riesgos de los activos. • Asegurar la continuidad de la empresa a través de los planes de continuidad y disponibilidad de los servicios/proyectos. • Gestionar las incidencias de seguridad.	Política de Seguridad de la entidad. Registro de comprensión de la política de seguridad.	N° de aceptaciones (leído y conforme) de la política de seguridad / N° de usuarios servicio/proyecto)*100
I. SP 1.2. Definir el Manual de Seguridad.			
- La Política de Seguridad de la Empresa.	Redactar y aprobar el Manual de Seguridad:	Documento con el Manual de Seguridad de la organización	(N° de procedimientos de seguridad definidos con responsable

- La estructura organizativa. - Activos de TI que se ven afectados en el servicio/proyecto.	- Establecer el alcance. - Definir los beneficios esperados y las métricas que permitirán verificar el cumplimiento de estos objetivos. - Definir los roles y asignar responsabilidades a cada rol dirigiendo así las funciones a realizar en relación con la gestión de los servicios/proyectos y su desarrollo seguro. - Definir los procedimientos que hay que realizar para el desempeño de las. - Establecer una fecha de aprobación y el período de revisión para su adecuación a la normativa. - Definir el registro de auditoría		asignado / N° de procedimientos de seguridad declarados en el manual de seguridad) * 100.
I. SP 1.3. Análisis de Riesgos.			
- Manual de seguridad - Activos de TI de la empresa. - Catálogo de servicios de empresa. Se incluyen tanto los servicios soporte de TI como los que soportan la actividad de la organización.	Realizar análisis de riesgos	- Catálogo de amenazas. - Matriz de análisis de riesgo. - Solicitud de cambio.	(1- (N° de incidencias o fallos de seguridad detectados en un activo / N° de Amenazas)) * 100.
I. SP 1.4. Definir un documento de respaldo financiero y compromiso.			
- Catálogo de los servicios de TI de la organización. - La estructura organizativa. - Matriz de riesgos	Definir el documento de respaldo financiero y compromiso de la dirección.	- Documento con presupuesto detallado para la implantación del plan de proyecto para desarrollo seguro.	- (N° de activos de seguridad presupuestados / N° de activos asociados al servicio/proyecto) * 100.

4.2.1.1.2 I. A2. Definición de prerrequisitos de seguridad

Tabla 4.2. Definición de prerrequisitos de seguridad

Entradas	Tareas	Salidas	KPI
I. SP 2.1. Definir el catálogo de servicios/proyectos de TI.			
- Catálogo estándar de servicios/ proyectos de TI. - La estructura organizativa.	Definir el catálogo de Servicios/Proyectos de TI para la IICC.	Catálogo de Servicios/Proyectos de TI de la IICC	(N° de Servicios TI del catálogo relacionados con algún proceso (negocio o TI) / N° de Servicios TI del catálogo) * 100.
I. SP 2.2. Definir el catálogo de servicios/proyectos de seguridad de TI.			
- Catálogo de Servicios/Proyectos de TI de la IICC. - Leyes y normativas de la empresa. - Categorías estándar de servicios de seguridad TI	Definir el catálogo de Prerrequisitos de seguridad TI para los Servicios / Proyectos para el desarrollo TI de la IICC.	- Catálogo de Prerrequisitos de seguridad TI para los Servicios/Proyectos que se abordan en la empresa	- (N° de Prerrequisitos de Seguridad TI incluidos en catálogo / N° de cláusulas de seguridad de estándares y leyes) * 100.
I. SP 2.3. Establecer un vínculo entre servicios/proyectos de seguridad de TI con los servicios TI.			
- Catálogo de Servicios/Proyectos de TI de la IICC. - Catálogo de Prerrequisitos de seguridad TI para los Servicios/Proyectos para desarrollo TI que se abordan en la IICC.	- Establecer un vínculo entre servicios/proyectos de TI y prerrequisitos de seguridad de TI.	- Catálogo de Prerrequisitos de seguridad TI vinculados a cláusulas y normativas de seguridad.	-(N° de cláusulas de seguridad en Normativa con Prerrequisitos de Seguridad TI incluidos en catálogo de requisitos/ N° de cláusulas de seguridad de la Normativa) * 100. - (N° de Normativas con Prerrequisitos de Seguridad TI incluidos en catálogo de requisitos/ N° Normativas) * 100.

4.2.1.1.3 I. A3. Planificación y comunicación

Tabla 4.3. Planificación y comunicación

Entradas	Tareas	Salidas	KPI
I. SP 3.1. Definir plan de servicio/ proyecto para desarrollo seguro.			

- La estructura organizativa. - Catálogo de Servicios/Proyectos de TI de la IICC. - Catálogo de Prerrequisitos de seguridad TI vinculados a cláusulas y normativas de seguridad.	- Definir un plan de servicio/proyecto para desarrollo seguro.	- Plan de desarrollo proyecto para desarrollo seguro.	- Nº de prerrequisitos de seguridad con respaldo financiero / Nº de Prerrequisitos de seguridad definidos. - Nº de prerrequisitos de seguridad con recursos y tiempo asignados / Nº de Prerrequisitos de seguridad definidos.
I. SP 3.2. Comunicar el plan de proyecto para desarrollo seguro.			
- La estructura organizativa. - Manual de seguridad. - Catálogo de Prerrequisitos de seguridad TI. - Plan de desarrollo de proyecto para desarrollo seguro.	- Comunicar el plan de desarrollo y mantenimiento de servicio/proyecto de desarrollo seguro.	- Registro de aceptación del plan de desarrollo y mantenimiento de requisitos del servicio/proyecto para el desarrollo seguro. - Registro de solicitudes de cambio al plan.	- Nº de aceptaciones del plan para desarrollo y mantenimiento / Nº de partes implicadas. - Nº de solicitudes de cambio de prerrequisitos del plan / Nº de prerrequisitos del plan.
I. SP 3.3. Revisar el plan de proyecto para desarrollo seguro.			
La estructura organizativa. - Manual de seguridad. - Catálogo de prerrequisitos de seguridad TI. - Plan de desarrollo de proyecto para desarrollo seguro. - Registro de aceptación del plan de desarrollo. - Registro de solicitudes de cambio al plan.	- Revisar el plan de proyecto.	- Informe de mejora.	- Nº de cambios solicitados al plan aceptaciones del plan para desarrollo y mantenimiento / Nº de cambios solicitados en el servicio/proyecto.

4.2.1.2 Fase II. Definición de Requisitos de Seguridad

4.2.1.2.1 II. A1. Clasificación de activos

Tabla 4.4. Clasificación de activos

Entradas	Tareas	Salidas	KPI
II. A1 Clasificación de activos.			
- Principios de seguridad vigentes.	- Definir los criterios de seguridad para los activos de TI.	- Criterios de seguridad para categorizar los requisitos de seguridad de los activos de TI.	- (Nº de criterios de seguridad vinculados con algún requisito/Nº de criterios de seguridad) *100.

4.2.1.2.2 II. A2 Definición del catálogo de requisitos de seguridad

Tabla 4.5. Definición de los requisitos de acceso

Entradas	Tareas	Salidas	KPI
II. SP 2.1. Definición de los requisitos de acceso.			
-Organigrama de la organización. Con necesidades de acceso a los activos de TI en cada puesto de trabajo y la/s persona/s asociadas. - Manual de seguridad. Con restricciones de acceso a cada activo. - Catálogo de Activos de TI. Aporta información acerca de los niveles de seguridad y riesgo que tiene el activo con los prerrequisitos de seguridad definidos en Fase I.	-Definir los roles. - Asignar roles a usuarios concretos. - Establecer los permisos de acceso a los activos para cada rol. -Establecer permisos a los sujetos para que puedan adoptar roles. - Gestión de autorizaciones. - Establecer jerarquía de roles.	- Matriz de acceso.	KPI-01 (Nº de roles con acceso / Nº de roles total) *100 . - KPI- 02 (Nº de activos del servicio TI con matriz de permisos asignados / Nº de activos del servicio TI) * 100.

Tabla 4.6. Definir requisitos de seguridad de terceros

Entradas	Tareas	Salidas	KPI
II. SP 2.2. Definir requisitos de seguridad de terceros.			
- Catálogo de requisitos de seguridad de la IICC. - Servicio o Activo de Seguridad. - Información relativa a la seguridad de empresa proveedora.	- Solicitud previa de contratación. - Categorización del tipo de servicio TI o activo TI. - Certificación. Determinar si se requieren determinadas certificaciones técnicas. - Elaboración del pliego de cláusulas técnicas. - SLA. Con la siguiente información: ✓ Horas de disponibilidad. ✓ Tiempos de respuesta. ✓ Mantenimiento y cambios. ✓ Contingencias e incidencias cubiertas por el acuerdo. ✓ Procedimiento de escalado. ✓ Fecha de entrada en vigor y revisión del SLA. ✓ Aprobador del SLA. ✓ Revisor del SLA.	- SLA con tabla de requisitos de seguridad del servicio /proyecto contratado.	- (Nº de Incidencias de incumplimiento de SLAs / Nº de SLAs firmados) * 100.

Tabla 4.7. Estructurar el catálogo de requisitos de seguridad

Entradas	Tareas	Salidas	KPI
II. SP 2.3. Estructurar el catálogo de requisitos de seguridad.			
- Manual de seguridad. - Matriz de riesgos.	- Establecer niveles de clasificación. - Definir cada nivel. Con esta actividad, no se trata de aportar soluciones a las amenazas, sino de conocer y registrar los requisitos de seguridad que están asociados a cada amenaza de activo para que posteriormente, en la fase III, pueda ser tratado por una solución.	- Catálogo de requisitos de seguridad.	- N° de Requisitos dentro de catálogo. Medido por (N° Requisitos de seguridad catalogados / N° de requisitos de seguridad) * 100.
II. SP 2.4. Definir los requisitos de seguridad de los servicios/proyectos de TI.			
- Manual de seguridad. - Matriz de riesgos. - Catálogo de requisitos de seguridad.	- Definir los requisitos de seguridad de activos TI del servicio, vinculando los requisitos del catálogo de requisitos de seguridad con los requisitos de seguridad de los activos de TI que se necesitan para el servicio de TI. Se trata de conocer y registrar los requisitos de seguridad que están asociados a cada amenaza de cada activo para que posteriormente, en la fase III, pueda ser tratado por una solución.	- Documento requisitos de seguridad de los activos de TI relacionados con el servicio/proyecto.	- (N° de activos TI con requisitos de seguridad catalogados/N° de activos de TI) * 100.

4.2.1.2.3 II. A3 Definición de requisitos de monitorización del catálogo

Tabla 4.8. Definición de requisitos de monitorización del catálogo

Entradas	Tareas	Salidas	KPI
II. SP 3.1. Definir el registro de monitorización del catálogo de requisitos de seguridad.			
- Catálogo de requisitos de seguridad. - Matriz de permisos de acceso	- Definir el registro de monitorización del catálogo de requisitos de seguridad	- Estructura del registro de monitorización del catálogo de requisitos de seguridad	- (N° Accesos al catálogo de requisitos de seguridad / N° de registros de monitorización de acceso al catálogo de requisitos de seguridad) * 100.

4.2.1.3 Fase III. Definición de Requisitos de Seguridad

4.2.1.3.1 III. A1. Gestión de Riesgos TI

Tabla 4.9. Diseño del procedimiento de implantación de activos de seguridad

Entradas	Tareas	Salidas	KPI
III SP 1.1. Diseño del procedimiento de implantación de activos de seguridad.			
- Manual de seguridad. Aporta información sobre las restricciones vinculadas de acceso a cada activo de acuerdo a la política de seguridad. - Matriz de Riesgo. Aporta información acerca de los niveles de seguridad y riesgo que tiene el activo -Matriz de acceso. - Documento Requisitos de Seguridad.	- Analizar los activos de seguridad. - Estructurar los activos de seguridad. - Definir el procedimiento de implantación de los activos de seguridad.	- Catálogo de activos de seguridad. - Procedimiento de implantación de activos de seguridad. - Registro de implantación de activo de seguridad.	(N° de solicitudes de cambio/implantación de activos de seguridad implantados/N° solicitudes de cambio /implantación de activo de seguridad) * 100.

Tabla 4.10. Diseño de los procedimientos transversales

Entradas	Tareas	Salidas	KPI
III SP 1.2. Diseño de los procedimientos transversales.			
- Manual de seguridad. Aporta información sobre las restricciones vinculadas de acceso a cada activo de acuerdo a la política de seguridad. - Matriz de Riesgo. Aporta información acerca de los niveles de seguridad y riesgo que tiene el activo. - Documento Requisitos de Seguridad. - Registro de implantación de activo de seguridad. - Catálogo de activos de seguridad.	- Definir el procedimiento de gestión de incidencias de seguridad. - Definir el procedimiento de solicitudes.	- Procedimiento gestión de incidencias de seguridad.	- (Nº de solicitudes de cambio/implantación de activos de seguridad implantados/Nº solicitudes de cambio /implantación de activo de seguridad) * 100. - (Nº de incidencias de activos de seguridad /Nº de incidencias de TI) * 100.

4.2.1.3.2 III. A2. Implementación de la Solución

Tabla 4.11. Implementación de la Solución

Entradas	Tareas	Salidas	KPI
III SP 2.1. Diseño de la BBDD de Activos TI.			
- Catálogo de servicios TI. - Catálogo de activos de seguridad.	- Diseñar el modelo lógico de Servicio /Proyecto de TI y Activos de TI.	- Registros de Servicios y Activos de TI.	- Nº de requisitos de seguridad asociados a cada activo de TI. - Nº de cambios registrados en los requisitos de seguridad por activo de TI. - Nº de pruebas de requisitos de seguridad asociadas a cada activo de TI.
III SP 2.2. Diseño de la BBDD de Activos de Seguridad (SAL).			
- Manual de seguridad. Aporta información sobre las restricciones	- Diseñar el modelo lógico de datos. - Diseñar la estructura física acceso a ficheros.	- Diseño lógico SAL. - Diseño físico.	- Nº de activos de seguridad TI con activos/servicios TI asociados y registrados.

vinculadas de acceso a cada activo. - Matriz de Riesgo. - Matriz de acceso. - Documento Requisitos de Seguridad. Aporta información relativa a las restricciones de seguridad del activo. - Registro de implantación de activo de seguridad. Información de la estructura del activo de seguridad. - Catálogo de activos de seguridad. Registros de la BBDD.			- Nº de registro de activos de seguridad TI sin activo / servicios de TI asociado. - Nº de pruebas de activos de seguridad TI registradas.
III SP 2.3 Implantación de los Activos de Seguridad.			
- Registro de implantación de activo de seguridad. - Arquitectura de TI	- Entrega y despliegue de los activos de seguridad.	- Activo de seguridad operativo en un servicio de TI.	- Nº de activos de seguridad TI con activos/servicios TI asociados y registrados. - Nº de registro de activos de seguridad TI sin activo / servicios de TI asociado. - Nº de pruebas de activos de seguridad TI registradas.

4.2.1.3.3 III. A3. Diseño del procedimiento de monitorización de la solución

Tabla 4.12. Diseñar el cuadro de mando de seguridad (CMS)

Entradas	Tareas	Salidas	KPI
III SP 3.1. Diseñar el cuadro de mando de seguridad (CMS).			
- Catálogo de servicios TI. - Registros de monitorización del catálogo de requisitos de seguridad. (Registros con valores de KPIs).	- Diseñar el cuadro de mando de ciberseguridad (CMS).	- Cuadro de mando de seguridad (CMS).	- (Nº registros de monitorización utilizados/Nº de informes utilizados en la fase de revisión y mejora) * 100. - (Nº de campos del cuadro con información/ Nº de campos vacíos)*100.

4.2.1.4 Fase IV. Monitorización

4.2.1.4.1 IV. A1. Definición del procedimiento de monitorización y recuperación

Tabla 4.13. Definición de las métricas y controles de monitorización de activos

Entradas	Tareas	Salidas	KPI
IV. SP 1.1. Definición de las métricas y controles de monitorización de activos			
- Manual de seguridad. Aporta información sobre las restricciones vinculadas de acceso a cada activo de acuerdo a la política de seguridad. - Matriz de Riesgo. Aporta información acerca de los nivel de seguridad y riesgo que tiene el activo. - Documento Requisitos de Seguridad. - Catálogo de activos de seguridad. - Registro de implantación de activo de seguridad. - SAL.	-Definir la estructura de las métricas de los activos de seguridad implicados en servicio/procesos que se van a realizar. - Aplicar las métricas y registrar la eficacia de los activos en el servicio/proyecto.	- Registros de monitorización de activos de seguridad.	- (Nº registros de monitorización de activo con medida de KPI / Nº de registro de monitorización de activo) * 100.

Tabla 4.14. Monitorización de la recuperación y la continuidad

Entradas	Tareas	Salidas	KPI
IV. SP 1.2 Monitorización de la recuperación y la continuidad			
- Manual de seguridad. Aporta información sobre las restricciones vinculadas de acceso a cada activo de acuerdo a la política de seguridad. - Matriz de Riesgo. Aporta información acerca de los niveles de seguridad y riesgo que tiene el activo. - Matriz de acceso. - Documento Requisitos de Seguridad . - Catálogo de activos de seguridad. - Registro de implantación de activo de seguridad - SAL.	- Definir los activos críticos a monitorizar. - Definir la estructura del registro de monitorización contingencia.	- Plan de continuidad. - Registros de continuidad.	(Nº registros de monitorización de continuidad con KPI/ Nº de registros de monitorización) * 100.

4.2.1.4.2 IV. A2. Revisión de los activos de seguridad

Tabla 4.15. Revisión de los activos de seguridad

Entradas	Tareas	Salidas	KPI
IV. SP 2.1 Revisión de activos relativos a la política de seguridad			
- Política de seguridad. - Manual de seguridad. - Registros de monitorización de activos de seguridad.	- Revisar estado de registro de cumplimiento de leyes y estándares. - Revisar estado divergencias entre procedimientos definidos en el manual y los implantados. - Realizar el informe de resultados de monitorización de política de seguridad.	- Informe resultados de monitorización de la política y manual de seguridad	- Nº de disconformidades encontradas en la política de seguridad / Nº de leyes y estándares comprometidos por la empresa. - (Nº de procedimientos definidos en el manual susceptibles de ser cambiados / Nº de procedimientos definidos) * 100.
IV SP 2.2 Revisión de activos relativos a los requisitos financieros de seguridad			

- Presupuesto de seguridad de TI. - Registros de monitorización de contabilización de gastos en activos de seguridad.	- Revisar estado de registro de contabilidad. - Revisar estado divergencias entre presupuesto y gasto. - Realizar el informe de resultados de monitorización de presupuestos.	- Informe resultados de monitorización de requisitos y gastos financieros en gestión de proyectos de desarrollo seguro.	- (1 - Nº de desviaciones de presupuesto mayores que el umbral establecido) * 100.
IV SP 2.3 Revisión de activos transversales de la seguridad			
- Registros de monitorización de contabilización de gastos en activos de seguridad. - Registros de monitorización del catálogo de requisitos de seguridad. (Registros con valores de KPIs). - Registros del Cuadro de Mando de Seguridad (CMS).	- Revisión de registros de incidencias de seguridad. - Revisar registros de cambios y solicitudes. La monitorización de los activos de seguridad, relativos a los procesos de gestión transversal: gestión de cambios y gestión de incidencias, va a generar información sobre la dinámica de evolución, a nivel operativo, del proceso de gestión de proyectos.	- Registro de resultados del análisis incidencias del CMS. - Registro de resultados del análisis cambios y solicitudes del CMS. - Registro de resultados del análisis presupuestos del CMS.	- (Nº de registros de resultados de análisis emitidos en período establecido/ Nº de registros de resultados de análisis esperados) * 100.

4.2.1.4.3 IV. A3. Emisión de informes

Tabla 4.16. Emisión de informes

Entradas	Tareas	Salidas	KPI
IV. SP 3.1 Emisión de informes de monitorización de la seguridad servicio/proyecto			
- Manual de Seguridad. - Registros de monitorización de Activos de Seguridad. - Registro de resultados del	- Realizar y emitir informes de monitorización.	- Informe de eficacia de los activos de seguridad. - Informe resultados de monitorización de incidencias de seguridad. - Informe resultados de monitorización de	- (Nº de informes emitidos y aceptados por e destinatario sin cambios / Nº de informes emitidos) * 100.

análisis incidencias del CMS. - Registro de resultados del análisis cambios y solicitudes del CMS. - Registro de resultados del análisis presupuestos del CMS. - Plantilla de emisión de informe.		cambios y solicitudes.	

4.2.1.5 Fase V. Revisión y Mejora

4.2.1.5.1 V. A1. Revisión del estado actual

Tabla 4.17. Revisión del estado actual

Entradas	Tareas	Salidas	KPI
V. SP 1.1. Revisión de estado seguro y revisión de informes de monitorización			
- Política de Seguridad. - Informe de eficacia de los activos de seguridad. - Informe resultados de monitorización de incidencias de seguridad. - Informe resultados de monitorización de cambios y solicitudes.	- Revisión del estado seguro y de los informes de monitorización.	- Acta de reunión con decisiones cuanto a nuevos servicios / proyectos para el desarrollo seguro, o modificaciones a abordar. - Nuevos planes de actuación (si se diera el caso).	- (Nº de decisiones y planes de actuación / Nº de informes revisados) * 100.
V. SP. 1.2. Comunicación de resultados de revisión			
- La estructura organizativa. - Manual de seguridad. - Acta de reunión con decisiones cuanto a nuevos servicios / proyectos para el desarrollo seguro, o modificaciones a abordar. - Nuevos planes de actuación (si se diera el caso).	- Comunicar las decisiones a las partes implicadas.	- Registro de comunicación de las decisiones. - Aceptación del comunicado.	- (Nº de decisiones comunicaciones aceptadas / Nº de comunicaciones) * 100.

4.2.1.5.2 V. A2. Planificar y comunicar el plan de mejora

Tabla 4.18. Planificar y comunicar el plan de mejora

Entradas	Tareas	Salidas	KPI
V. SP 2.1. Planificación del procedimiento de mejora			
- La estructura organizativa. - Manual de seguridad. - Acta de reunión con decisiones en cuanto a nuevos servicios / proyectos para el desarrollo seguro, o modificaciones a abordar. - Nuevos planes de actuación (si se diera el caso).	- Detallar el plan de actuación.	- Planificación detallada de actuación de mejora.	- (Nº tareas planificadas con recursos asignados / Nº de tareas planificadas) * 100. - (Nº tareas planificadas con KPI identificado / Nº de tareas planificadas) * 100.
V. SP 2.2. Comunicación de resultados de decisión			
- La estructura organizativa. - Acta de reunión con decisiones cuanto a nuevos servicios / proyectos para el desarrollo seguro, o modificaciones a abordar. - Planificación detallada de actuación de mejora.	- Comunicar a las partes implicadas el inicio de un nuevo servicio/proyecto para el desarrollo seguro de TI.	- Registros de comunicación y aceptación de compromiso de desarrollo de tareas.	- (Nº tareas enviadas / Nº de Tareas planificadas) * 100. - (Nº registros de tareas aceptadas/ Nº de tareas enviadas) * 100.

5. Experimento

Se ha procedido al contraste de hipótesis mediante un experimento consistente en la proposición de prácticas en un análisis de caso mediante diseño expeerimental de ingeniería del software.

5.1 Metodología experimental.

Entre los métodos empíricos utilizados para experimentación en ingeniería de Sw y para este Trabajo Fin de Master se recurrirá a la propuesta de experimentación de Wohlin et al. (2003) que ha sido ampliamente utilizada con éxito en este área (Arcilla, 2013; De la Cámara, 2016). Se trata de un método apto para investigaciones cualitativas como cuantitativas dentro del estudio o análisis de casos en el que se establece una comparación de resultados entre dos propuestas: la de partida o línea base y la nueva propuesta.

En este Trabajo Fin de Master se aplica la estrategia de comparación de resultados. Para ello, se llevan a cabo los siguientes pasos sobre un caso de estudio específico:

1. Se crea un cuestionario de evaluación basado en los parámetros definidos en el Capítulo 4 de este Trabajo Fin de Master y en base al modelo de evaluación de gestión y desarrollo seguro en proyectos TI desarrollado por De la Cámara (2016) (véase ANEXO I).

2. Antes de implantar el marco propuesto, los jefes de proyecto rellenan este cuestionario de evaluación.

3. Los resultados obtenidos constituyen la línea base inicial con la que comparar los resultados tras la aplicación del marco propuesto. Esta línea base servirá como instrumento de validación del marco propuesto en este TFM.

4. Se implanta el proceso de administración de proyectos de SI en desarrollo, descrito en el Capítulo 4 de este TFM.

5. Se repite el paso 2. Los jefes de proyecto rellenan de nuevo el mismo cuestionario.

6. Finalmente, se comparan los resultados obtenidos y se analizan los resultados.

5.2 Caso de estudio

En los sub-apartados que siguen se muestra el contexto del entorno de gestión de infraestructura crítica industrial y las actividades realizadas en el proceso de validación del marco propuesto en el Capítulo 4 de este Trabajo Fin de Master.

5.3.1 Contexto de caso

LABORATORIO DE IICC (el nombre es ficticio por razones de confidencialidad) es una organización con sede en Castilla y León que fue constituida en el año 2015 perteneciente a su vez de una corporación constituida en 1979. Cuenta con 12 usuarios internos entre

personal de plantilla y personal en formación. Su actividad funcional se realiza en los siguientes departamentos:

- Dirección (D). Responsable de impulsar, dirigir, coordinar y tomar decisiones sobre las actividades de la organización. Además del Director, y en dependencia directa del mismo, existen dos Responsables de Proyecto, diferentes del Responsable de TI.
- Departamento de Control e Investigación (DCI). Se encarga de realizar todas las funciones relativas al desarrollo de proyectos, incluidos proyectos TI. Cuenta con cinco (5) perfiles de analista y dos (2) analistas en formación)
- Departamento de Desarrollo (DD). Se encarga de las labores de programación. Cuenta con cuatro (4) perfiles.
- Departamento de TI (TI). Se encarga de las funciones que dan soporte informático a toda la empresa. Además, se ocupa de todos los asuntos relacionados con la SI de la organización. Cuenta con un perfil que ejerce como Responsable de TI.

Aunque a nivel corporativo cuenta con un departamento de informática en el que recae la responsabilidad de proveer los servicios que permitan adecuación a la LOPD, los compliance corporativa, así como la continuidad del negocio, no obstante cuenta con autonomía a nivel de gestión y desarrollo de servicios TI mediante la existencia de un Responsable TI que depende directamente de la Dirección del Laboratorio. Las instalaciones son de nueva creación y en la actualidad están completando el traslado e instalación definitiva en el edificio que se encuentra a 500 metros del emplazamiento original de la corporación. No obstante, el laboratorio cuenta con una trayectoria anterior de control de sistemas industriales que convierte al equipo humano que lo gestiona en altamente experimentado, con más de 10 años de experiencia, más de 20 en el caso del Director.

Centrándose en el área de interés para el Trabajo Fin de Master, la actividad de LABORATORIO DE IICC que se desea evaluar es la gestión de la SI de los proyectos de tecnologías de información que aborda el laboratorio en el ámbito de infraestructuras críticas industriales. Por lo tanto, el objetivo de este caso es aplicar el marco propuesto en el Capítulo 4 y conocer el estado de seguridad de los proyectos de TI antes y después de la aplicación de dicho marco.

El LABORATORIO DE IICC cuenta con la siguiente infraestructura de TI.

- Hardware:
  - Seis servidores de gama media (para datos y aplicaciones).
  - Todos los usuarios internos disponen de un ordenador personal e incluso tres más (15 en total) para realizar su actividad profesional.
  - Dos (2) portátiles, que se conectan por una red privada virtual (VPN) al servidor, en el caso de acceso autorizado.
  - Una (1) impresora láser, conectada a la red de área local (LAN) y que comparten todos los usuarios del Laboratorio.
- Software

- Cada uno de los ordenadores personales dispone del software necesario según el departamento al que pertenezca y la función desempeñada. Los usuarios internos de cada departamento sólo pueden acceder a las aplicaciones software necesarias para su función en su departamento.
- En cuanto a las aplicaciones propias:
  - El Laboratorio cuenta con 12 licencias del programa de sistema operativo WS (nombre ficticio), 5 licencias del programa de gistema operativo WSS (nombre ficticio) y 15 licencias del programa de ofimática OW (nombre ficticio).
  - El departamento de desarrollo cuenta con 6 licencias del programa de virtualización VM (nombre ficticio).
  - El departamento de control e investigación cuenta con 20 licencias de software específico de automatización y control, incluyendo software tipo SCADA.
  - A nivel corporativo, se dispone de servicios TI proporcionados por el departamento de TI de la corporación que dan soporte al acceso a gestión de personal y nóminas, gestión presupuestaria y otros.
- Dicha organización dispone también de una página web que da salida a todos los servicios del LABORATORIO DE IICC, cuya dirección es www.IICCPX1.com. Dicha web está alojada en un proveedor de servicios externo (ISP), que proporciona servicio a las necesidades de seguridad y almacenamiento, y confiere independencia al Laboratorio respecto a los servicios web corporativos.

- Además, el Laboratorio tiene implantados 6 categorías de Servicios de TI:
  - Gestión de puesto de trabajo: encargado del alta y el mantenimiento del hardware del Laboratorio, así como de las aplicaciones software base de los puestos de trabajo.
  - Gestión de la cuentas de correo: instalación, actualización y mantenimiento de las cuentas de correo electrónico propias e independientes del procedimiento de Gestión de cuentas de correo de la corporación matriz.
  - Internet: instalación, actualización y mantenimiento del navegador y del sitio web.
  - Aplicaciones software: instalación, actualización y mantenimiento de software específico, e instalación, actualización y mantenimiento del software de la BBD.
  - Seguridad: Backup de datos, Backup sitio web.

5.3.2 Establecimiento de la línea base

Esta se ha hecho a partir de las respuestas dadas, por los tres jefes de proyecto y el Director, al cuestionario que se adjunta en el ANEXO I de este Trabajo Fin de Master. Este cuestionario está compuesto por un conjunto de preguntas que resultan de la

estructura de factores de seguridad para servicios/proyectos de TI, planteada en base a la filosofía SbD y validadas con los principales modelos de gobernanza, y administración de servicios y proyectos de TI (De la Cámara, 2016).

Las preguntas se han agrupado de acuerdo a las actividades y tareas propuestas en el marco de trabajo expuesto en el Capítulo 4. Están orientadas a cumplir con la Fase II, relativa a la evaluación del modelo estándar sobre distintos patrones de proyecto TI en GPS-IICC.

El cuestionario cuenta con 88 preguntas distribuidas entre las distintas fases del modelo.

Tabla 5.1. Distribución de cuestiones por fase

Fase	**Número de preguntas**
I: Inicio y Dirección.	18
II: Definición de Requisitos.	18
III: Diseño e Implantación.	14
IV: Monitorización.	19
V: Revisión y mejora	19
Total	88

Cada una de las preguntas se ha planteado y discutido con los gestores de servicios/proyecto. Los gestores del Laboratorio han respondido el grado con el que, el objetivo de la pregunta, se realiza en los proyectos que abordan su empresa. Se responde en los siguientes términos:

- N. Nunca. 0 veces
- R. Rara vez. Entre 1% y el 25% de las veces.
- A. Algunas veces. Entre un 26% y un 50% de las veces.
- U. Usualmente. Entre un 51% y un 75% de las veces.
- S. Siempre. Entre 76% y el 100 % de las veces.

Las preguntas están organizadas de acuerdo a la estructura que se presenta en el modelo GPS-IICC. Su objetivo es conocer cómo se realizan un conjunto de prácticas específicas para cada una de las actividades, que se definen en cada fase. El cuestionario inicial de evaluación se ha ido rellenando, en reuniones al efecto con los responsables de proyecto elegidos para la validación. Cada pregunta ha sido detallada con los jefes de proyecto recabando alguna evidencia para su posible respuesta, en el caso de que hubieran varias alternativas de evidencias.

El cuestionario de evaluación inicial y final se muestra en el ANEXO I de este Trabajo Fin de Master.

A partir del primer resultado se propone un plan de actuación para acometer la adecuación y mejora de una selección de prácticas correspondientes a los procedimientos de las siguientes áreas:

- Gestión del puesto de trabajo que incluya el hardware y el software base.
- Administración de servicios de tecnologías de la información.
- Gestión de aplicaciones de software específicas.

- Control de accesos a datos, y aplicaciones básicas y específicas.
- Desarrollo SW.

En este contexto, las siguientes subsecciones muestran los resultados de la validación de marco que se presenta en este Trabajo Fin de Master a través de cuatro pasos:

1. Establecer la línea base inicial, antes de la aplicación del patrón.

2. Aplicar, a partir del proceso estándar, el proceso definido en el patrón para la gestión segura de proyecto de TI en el Laboratorio.

3. Volver a pasar el mismo cuestionario de evaluación después de haber aplicado el patrón del marco propuesto, y mostrar los resultados a los responsables del Laboratorio.

4. Hacer un estudio comparativo final.

5.3.2.1 Resultados Línea Base Inicial

La Tabla 5.2 muestra los resultados de los cuestionarios correspondientes al análisis ponderado de las respuestas en el caso estudiado, identificando los grados de aplicación o cobertura para cada pregunta. Para ello, se considera el nivel de cobertura de cada pregunta del cuestionario (columna "Cobertura Pregunta" del ANEXO II), que se obtiene sumando ponderadamente los porcentajes de cobertura de sus tipos de respuestas, de acuerdo a la expresión siguiente (Cuevas et al., 2002):

$$Cpi = CriS * \mathbf{1} + CriU * \mathbf{0'75} + CriA * \mathbf{0'5} + CriR * \mathbf{0'25} + CriN * \mathbf{0}$$

siendo Cpi el porcentaje total de cobertura de la pregunta i.

Tabla 5.2. Línea base inicial. Resultado de la evaluación de las preguntas

F I		F II		F III		F IV		F V	
I.P01	0	II.P01	2	III.P01	0	IV.P01	0	V.P01	0
I.P02	1,25	II.P02	0,75	III.P02	0	IV.P02	0	V.P02	0
I.P03	3,50	II.P03	0	III.P03	0	IV.P03	0	V.P03	0
I.P04	0	II.P04	4	IV.P04	2	IV.P04	4	V.P04	2
I.P05	2,50	II.P05	3,50	III.P05	1	IV.P05	4	V.P05	0
I.P06	0	II.P06	2	III.P06	0	IV.P06	4	V.P06	0
I.P07	0	II.P07	4	III.P07	0	IV.P07	0	V.P07	0
I.P08	0	II.P08	0	III.P08	4	IV.P08	2	V.P08	0
I.P09	0	II.P09	0	III.P09	2	IV.P09	0	V.P09	0
I.P10	4	II.P10	0	III.P10	3	IV.P10	0	V.P10	0
I.P11	4	II.P11	0	III.P11	0	IV.P11	0	V.P11	0
I.P12	4	II.P12	2	III.P12	0	IV.P12	0	V.P12	0
I.P13	0	II.P13	0	III.P13	0,25	IV.P13	0	V.P13	0
I.P14	2	II.P14	0	III.P14	0	IV.P14	0	V.P14	0
I.P15	0	II.P15	0			IV.P15	4	V.P15	0
I.P16	0	II.P16	4			IV.P16	0	V.P16	0
I.P17	0	II.P17	2			IV.P17	0	V.P17	0
I.P18	0	II.P18	4			IV.P18	0	V.P18	0
						IV.P19	0	V.P19	0

La ponderación refleja que las afirmaciones más fuertes deben tener más importancia que aquellas que son más débiles, y para cada pregunta se calcula su media y su desviación típica,

$$Mediap_i = \frac{(n^oS^*4 + n^oU^*3 + n^oA^*2 + n^oR^*1 + n^oN^*0)}{\text{nº Responsables de proyecto}}$$

siendo Mediapi la media para la pregunta i.

Para cada pregunta se van a aplicar unos pesos de ponderación mayores (4, 3, 2, 1 y 0), aplicando un factor, de forma que las diferencias existentes sean más notables. Es importante destacar que existe una correspondencia biunívoca o mismo significado entre el porcentaje de cobertura de la pregunta y su media (la única diferencia es que los factores de escala son diferentes), con lo que un porcentaje de cobertura elevado, también reflejará una media elevada y en la misma proporción que dicho porcentaje.

$$Desvp_i = \sqrt{\frac{[n^oJP^*(4^2 + n^oS + 3^{2*}n^oU + 2^2 * n^oA + 1^{2*}n^oR) - n^oJP^2 * Mediap_{i^2}]}{nº\ Responsables\ de\ proyecto^2}}$$

Finalmente, se calcula la "cobertura total" de la fase como la media de las diferentes "coberturas de las preguntas".

$$Cp(xy) = \frac{\sum_{i=1}^{n} Cp_i}{n}$$

El umbral establecido para que una práctica esté bien implantada se establece en un 75%, lo que se representa por un valor medio de 3,00. Se puede considerar que en aquellas preguntas con un valor de cobertura < 3,00 (en la escala de 4) y desviación típica <0,8, la práctica correspondiente a esa pregunta no está suficientemente implantada en la organización y se considera como un aspecto a mejorar (punto débil).

En la fase final se aplica el mismo procedimiento.

5.3.2.2 Conclusiones Línea Base

De la evaluación del cuestionario de validación en la *Fase 1. Inicio y Dirección* se pueden extraer las siguientes conclusiones:

1. Dos de las preguntas mejor valoradas son coincidentes, se trata de las preguntas P10 y P12 del ANEXO I. Esto se debe a que en el LABORATORIO IICC se observan buenas prácticas mediante un conjunto de aplicativos, que no servicios, y reglas de cifrado de información confidencial, donde muestran un elevado grado de capacitación y experiencia. No obstante, los responsables del Laboratorio son conscientes de que no tienen definidos, ni establecidos, los procedimientos que permiten formalizar sus acciones.

2. Las preguntas P06 y P09 del ANEXO I también coinciden en la valoración de las respuestas, con un valor inferior de 0. El LABORATORIO IICC no tiene definidos procedimientos que permitan evaluar los riesgos de sus activos de TI, sus

vulnerabilidades, amenazas y el impacto que éstas podrían tener sobre el negocio. Tampoco tienen una estimación cuantificada del valor de los activos de seguridad que tiene implantados.

En gran medida a la reciente constitución del Laboratorio, apenas 12 meses, en esta fase inicial es necesario realizar un mayor esfuerzo por establecer el estado inicial de sus activos de TI, sometiéndolos a análisis de riesgo.

En cuanto a los resultados de la evaluación inicial de la *Fase II. Definición de requisitos de seguridad*, varían con respecto a la anterior en los siguientes términos:

1. Sólo en las preguntas P04, P05, P16 y P18, la valoración supera el umbral mínimo establecido de 75% del valor máximo (umbral mínimo =3). En el resto de los casos las valoraciones están entre 0 y 2. La definición de los requisitos se ajusta al cumplimiento y auditoría de la legislación y, al tratarse de un Laboratorio perteneciente al sector de la industria TIC la definición de los requerimientos de seguridad de algunos de sus servicios y aplicaciones alcanza un nivel básico de desarrollo.

2. Las P16 y P18 se han valorado por los responsables de proyecto con un 4. Se trata de cuestiones relativas a la necesidad de monitorizar unos requisitos de seguridad, y dada la misión de control de infraestructuras industriales, se alcanzan niveles destacables pese a la carencia de procedimientos de monitorización documentados y sometidos a mejora continua.

La evaluación de la *Fase III. Diseño e Implantación de las Soluciones* aporta valores más bajos. Cabe destacar:

1. Un 64% de las preguntas se han valorado entre 0 y 0,25 en el LABORATORIO IICC. Esta valoración de 0 ha coincidido en ambas empresas para un mismo subconjunto de preguntas (P01, P02, P03, P07, P11, P12, P13 y P14). En el Laboratorio las soluciones se implantan sin tener en cuenta un diseño previo que integre las TI con los procesos de negocio.

2. Únicamente el 14% de las valoraciones, en esta Fase III, ha obtenido un valor superior al 3,00 esperado como umbral mínimo.

En la evaluación de la *Fase IV. Monitorización* cabe destacar:

1. Un 73% de las preguntas se han valorado con 0. Esta valoración de 0 ha coincidido en ambas empresas para un mismo subconjunto de preguntas (P01, P02, P03, P07, P10, P12, P13 y P14). En este caso, las valoraciones están condicionadas por la preocupación relativa a la continuidad de negocio y las auditorías de la LOPD.

2. Sin embargo, no se valora positivamente un subconjunto de preguntas orientadas a la monitorización de los activos de seguridad (P09, P11, P12, P16, P17, P18 y P19), implantados como controles de seguridad de las TI. Por lo tanto, no se valoran suficientemente las consecuencias de la monitorización de estos controles.

Finalmente, la evaluación de la *Fase 5. Revisión y Mejora*, orientada a la mejora continua, arroja los peores resultados frente a las cuatro anteriores. Son los siguientes:

1. Ninguna de las preguntas en esta fase ha alcanzado el umbral mínimo de 3,00. El valor máximo alcanzado ha sido de 2 exclusivamente para la pregunta P04.

2. La ausencia significativa de procedimientos de auditoría completos, así como la indefinición de un procedimiento que permita la revisión de los activos de seguridad, y tomar decisiones orientadas tanto al mantenimiento y mejora de los controles existentes como a la creación de nuevos servicios / proyectos para el desarrollo seguro, lastra esta Fase de manera casi total.

5.3.3 Definición del patrón del proyecto

En los sub-apartados que siguen se muestran las aplicadas en el caso de estudio propuesto, como prioritarias:

I. Inicio y Dirección de Proyecto [ID]. Se define la política de seguridad y se propone un Manual de Seguridad como eje vertebrador del SGSI en el LABORATORIO IICC.

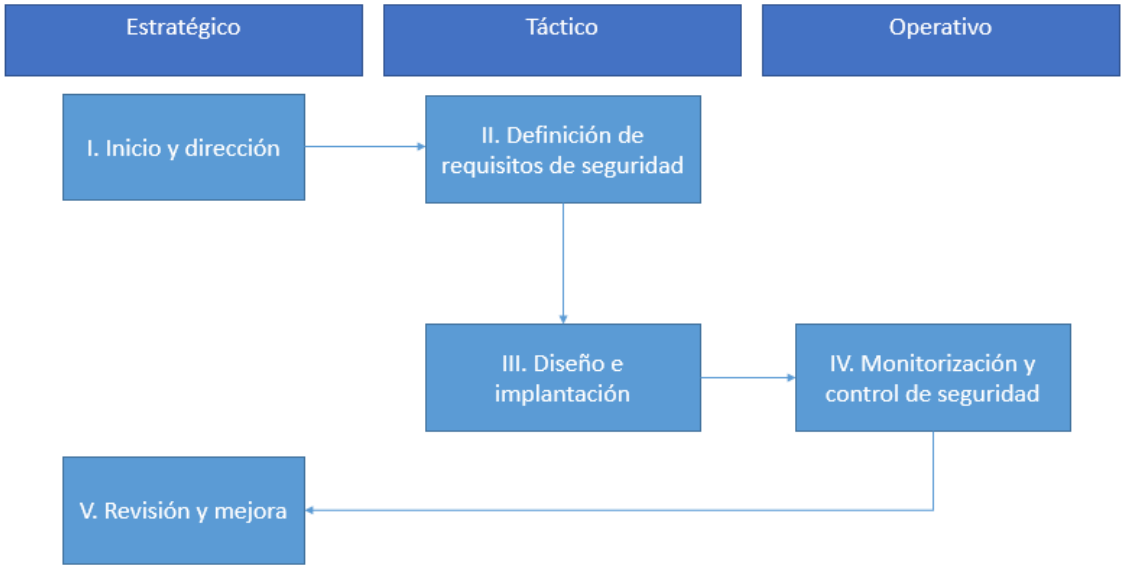
II. Definición de Requisitos de Seguridad [DRS]. Se definen los criterios de catalogación de requisitos de seguridad y se proponen criterios de catalogación.

III. Diseño e Implantación de Solución de Seguridad [DISS]. Se diseñan e implantan soluciones de gestión y control de seguridad que están asociadas a los riesgos y requisitos identificados.

IV. Monitorización de las Soluciones de Seguridad [MSS]. Se gestionan los controles implantados en la fase III, y se realizan informes relativos a la evolución y cumplimiento de los objetivos y metas definidos en las fases I y II.

V. Mejora Continua del Proyecto de TI [MCP]. Se revisan los informes de monitorización y auditorías para realizar propuestas de mejora. Además, se comunican las decisiones a las partes implicadas.

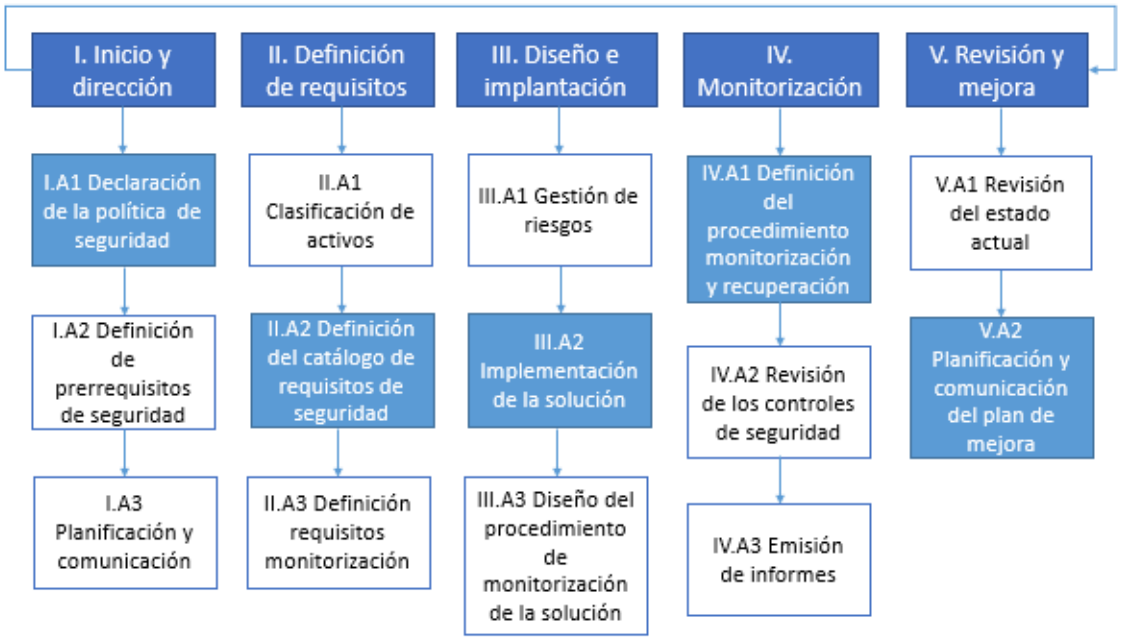
Figura 5.1. Fases del marco GPS-IICC



En este contexto, y con la línea base inicial de partida mostrada en el apartado 5.3.2, se propone a los Responsables del Laboratorio la definición del patrón de proyecto que implanta un conjunto de prácticas específicas que se muestran en la Figura 5.3. De acuerdo a las reuniones mantenidas con los responsables de proyecto, se consensua que el patrón tiene que cumplir las siguientes condiciones:

a) Contemplar actividades prioritarias para el conjunto de los responsables de proyecto. Los criterios para determinar la prioridad se basan en el cumplimiento de los principios y servicios básicos de seguridad, del estándar ISO 9001 y la ley LOPD. Los principios y servicios básicos de seguridad son definidos por el estándar ISO/IEC 27001 (ISO/IEC27001, 2013) como sigue:
    - Principios de información confidencial, íntegra y disponible (C-I-D).
    - Servicios básicos de seguridad (A-T-AC-NR)
        - Autenticación (A). Servicio mediante el cual se verifica la identidad de un usuario.
        - Trazabilidad (T). Servicio por el que se tiene control acerca de la creación, incorporación y conservación de información, los movimientos y uso de la información como activo. Esto afecta a conocer en todo momento quién, cuándo y a qué información se ha tenido o se tendrá acceso.
        - Control de Acceso (AC, Access Control).
        - No Repudio (NR). Servicio que permite probar la ocurrencia de una acción reivindicada y sus entidades de origen. El objetivo es resolver las controversias sobre la ocurrencia, o no, de una acción y de las partes implicadas en dicha acción.
b) Incluir al menos una actividad de cada una de las fases propuestas del marco, asegurando así un nivel básico del ciclo de vida del proyecto completo.

Figura 5.2. Actividades del patrón aplicadas (fondo relleno)



A continuación se describe una fase del marco propuesto y sus actividades. Además, se muestra un esquema con todas las actividades de la fase, en el que se identifican tanto las actividades y mejores prácticas propuestas y elegidas para la validación del marco (con relleno de color azul) como el producto de cada práctica específica (con relleno de color verde). Las prácticas específicas que han sido propuestas a los responsables del LABORATORIO IICC, se relacionan a continuación.

5.3.3.1 Inicio y Dirección

La *Fase I. Inicio y dirección del proyecto*, recoge las actividades previas de la organización antes de la aprobación para abordar el desarrollo en sí. El objetivo de esta fase es situar a la organización en un estado inicial desde donde abordar un proyecto de desarrollo seguro. Para ello, se plantean 3 actividades, cada una de ellas con un conjunto de prácticas específicas:

- I. A1 Declaración de la política de seguridad.
- I. A2 Definición de prerrequisitos de seguridad.
- I. A3 Planificación y comunicación del plan de proyecto de desarrollo seguro.

Para la validación del marco propuesto se van a implantar las prácticas específicas definidas para la actividad *A1 Declaración de la política de seguridad*, que se detalla en el ANEXO III.

La política de seguridad es una declaración de intenciones de alto nivel. El propósito de esta definición es comunicar las intenciones de la organización en relación a los objetivos con los que se compromete en relación a la seguridad de los proyectos TI que se abordan en la organización. Para ello, debe sentar las bases sobre las que posteriormente se definirán y delimitarán las responsabilidades y las distintas prácticas, tanto técnicas como organizativas, que se requieran.

5.3.3.2 Definición de requisitos de seguridad

El objetivo es definir y mantener una descripción de los distintos tipos de requisitos de seguridad necesarios para la organización. Esta descripción detallada y actualizada facilita el abordar nuevos servicios/proyectos con un menor esfuerzo y una mejor monitorización de los servicios/proyectos. Para ello, se plantean 3 actividades, cada una de ellas con un conjunto de prácticas específicas:

- II. A1 Clasificación de activos.
- II. A2 Definición del catálogo de requerimientos de SI.
- II. A3 Definición de requisitos de monitorización del catálogo.

Para la validación del marco propuesto se van a implantar las prácticas específicas definidas para la actividad *A2 Definición del catálogo de requisitos de seguridad*, que se detalla en el ANEXO VI.

Un requisito de seguridad hace referencia a las necesidades de seguridad que tienen cada uno de los activos para desempeñar correctamente su función en la empresa. Así, el propósito de la definición del catálogo de requisitos de seguridad es definir una colección de requisitos de seguridad clasificados que responda a las necesidades de seguridad en las tareas que realiza la empresa.

Para su definición GPS-IICC recurre a realizar una clasificación a través de una taxonomía. Esta taxonomía utiliza como criterio de clasificación los principios y servicios de seguridad básicos (C/I/D) y (A-T-AC-NR) y su objetivo es facilitar:

- La aparición de nuevos requisitos de seguridad Project Lifecycle.
- Comprensión de la problemática por todas las partes implicadas, que redunda en un mayor compromiso con los requisitos de seguridad del servicio/proyecto.
- La definición de pre-requisitos como medida preventiva en la Fase I del marco propuesto.
- La utilización de una lista de comprobación de seguridad o *checklist* para determinar si se han considerado todos los requerimientos de seguridad de cada uno de los tipos.

La taxonomía de requisitos de seguridad puede incluirse en el manual de seguridad. Su mantenimiento (el de la taxonomía) puede utilizarse tanto en la revisión y redefinición de políticas de seguridad como para abordar el diseño y la implantación de nuevos servicios/proyectos que respondan a necesidades de seguridad de servicios y operaciones de la organización.

Se proponen dos de las cuatro prácticas específicas para la definición del catálogo de requisitos de seguridad, numeradas como 2.1 y 2.4:

- **II. SP 2.1. Definir requisitos de acceso.**
- II. SP 2.2. Definir requisitos de proveedores.
- II. SP 2.3. Estructurar el catálogo de requisitos de seguridad.

- **II. SP 2.4. Definir los requisitos de seguridad de los servicios / proyectos de TI.**

a) Definir requisitos de acceso.

En el marco GPS-IICC se propone, para la definición de los requisitos de acceso, la utilización de técnicas basada en roles. Cada rol tiene unas necesidades organizativas. Estas necesidades dependen de la función que desempeña cada rol en el SI. Para cada usuario o aplicación se define:

- Un perfil usuario de: los servicios, procesos, aplicaciones, procedimientos, datos, instalaciones, etc. a los que necesita acceder.
- Un perfil de seguridad que determina el modo de acceso: lectura, escritura, lectura y escritura, añadir, ejecutar, propietario, etc.

El objetivo de la definición de los requisitos de acceso es establecer las condiciones que aseguran que los activos sean disponibles para los usuarios con autorización y restringirlo en las condiciones que cada usuario requiere. En este apartado se detallan las entradas, tareas y salidas para esta práctica específica.

Las acciones incluyen:

- Definir los roles: Con el fin reutilizar la información en el caso de experimentación, esta práctica específica se va a aplicar sobre los roles que tengan una funcionalidad similar y los roles propios del marco GPS-IICC. Los roles relativos al tema que nos ocupa en este TFM están definidos en el ANEXO V y la Tabla 5.7 los roles R_01 a R_15, así como la función de los roles generales del LABORATORIO IICC:

Tabla 5.3. Roles de la organización

Código		Rol	Nivel de función
R_01	D	Director del Laboratorio	Estratégico
R_02	RP1	Responsable de proyecto 1	Táctico
R_03	RP2	Responsable de proyecto 2	Táctico
R_04	RP3TI	Responsable de proyecto 3-Resp. TI	Táctico
R_05	AN1	Analista 1	Operativo
R_06	AN2	Analista 2	Operativo
R_07	AN3	Analista 3	Operativo
R_08	AN4	Analista 4	Operativo
R_09	AN5	Analista 5	Operativo
R_10	AN1	Analista en formación 1	Operativo
R_11	AN1	Analista en formación 2	Operativo
R_12	TD1	Técnico de desarrollo 1	Operativo
R_13	TD2	Técnico de desarrollo 2	Operativo
R_14	TD3	Técnico de desarrollo 3	Operativo
R_15	TD4	Técnico de desarrollo4	Operativo

En la Matriz de Acceso (véase ANEXO VII) se han clasificado los roles definidos en la Tabla 5.6. Los activos se han clasificado atendiendo al tipo de activo accesible. Los permisos están formados por el conjunto R = {A, E, R, W, U}. Donde:

- A: Acceder a un lugar físico.
- E: Ejecutar.
- R: Leer.
- W: Escribir.
- U: Utilizar.

A continuación se establece una jerarquía de roles en la que se pueden heredar privilegios y permisos de otros roles de menor jerarquía, simplificando así la administración de las autorizaciones. Con la Matriz de Acceso es fácil crear:

- Una Lista de Control de Accesos (ACL, *Access Control List*) por cada activo, que indica los permisos que tiene cada sujeto (rol) sobre el activo tratado. Esto permite conocer los permisos de acceso a cada activo.
- Una lista de Capacidades almacenando una Lista de Control de Capacidad por cada rol. Esto permite conocer los permisos de acceso de cada rol.

La implementación de los roles se va a realizar mediante las herramientas que facilitan:

- Microsoft Active Directory.
- Oracle Database.
- MS Sql Server Database.

5.3.3.2.2. Definir los requerimientos de seguridad de los servicios y proyectos en tecnologías de la información.

Creación de un catálogo de requisitos de seguridad es conocer qué principios básicos de seguridad (C/I/D) se están protegiendo o vulnerando en el SGSTI. Con esta actividad, no se trata de aportar soluciones a las amenazas, sino de conocer y registrar los requisitos de seguridad que están asociados a cada amenaza de activo para que posteriormente, en la fase III, pueda ser tratada por una solución.

Para cada amenaza identificada, se comprueba la necesidad, o no, de analizar cada subcategoría de seguridad de la clasificación realizada en la Tabla 5.8. Una vez comprobada, se establecen el/los requisitos que permitan el diseño e implantación de una solución y su posterior monitorización.

Tabla 5.4. Niveles del Catálogo de Requisitos de seguridad

Nivel 1. Requisito básico	Nivel 2. Requisito específico
NR_01 Confidencialidad (C)	NR_01_1 Cifrado
	NR_01_2 Autenticación
	NR_01_3 Agregación
	NR_01_4 Atribución
	NR_01_5 No Repudio
	NR_01_6 Consentimiento y notificación
	NR_01_7 Cardinalidad

	NR_01_8 Trazabilidad
NR_02 Integridad (I)	NR_02_1 Modificación
	NR_02_2 Borrado
	NR_02_3 Validación de la integridad del dato
	NR_02_4 Manejo de excepciones
	NR_02_5 Prerrequisitos
	NR_02_6 Separación de roles y funciones
	NR_02_7 Tiempo
NR_03 Disponibilidad (D)	NR_03_1 Tiempo de respuesta
	NR_03_2 Vencimiento
	NR_03_3 Asignación de recursos
	NR_03_4 Control de Acceso

Cada requisito de seguridad se registra con la siguiente información:

- Código de requisito: código único.
- Categoría: categoría de seguridad (véase Tabla 5.8) que requiere el requisito que se define.
- Activo/s. Activo donde se identifica la amenaza que justifica el requisito.
- Servicio/s que necesita/n del activo/s amenazados.
- Lista de cláusulas, normas, o leyes que justifican el requisito.
- Definición. En caso de que pueda realizarse una definición formal se hace. Si no, se hace una descripción textual. La definición formal permite una mejor verificación.
- Umbrales. Valores máximos y mínimos del requisito.
- Métrica asociada al requisito definido.

Tabla 5.5. Estructura del registro de requisito de seguridad

Campo del registro	**Descripción del requisito**	
Código	RQ01	Código de requisito
Categoría	NR	Código de categoría de seguridad (véase Tabla 5.12)
Lista de Activo	Lista de códigos de activos amenazados y que necesitan del requisito	
Lista de Servicios	Lista de servicios que necesitan de cada uno de los activos de la Lista de Activos	
Lista de Restricciones	Lista de cláusulas, apartados de normas y leyes, que reflejan el requisito como necesario	
Descripción	Descripción textual o formal del requisito	
Umbrales	Valores de umbrales del requisito	
Métrica	Métodos de medida de monitorización y detección del estado del requisito	

5.3.3.3 Diseño e Implantación de la Solución de Seguridad

La *Fase III. Diseño e Implantación de la Solución de Seguridad* parte de los requisitos definidos en la Fase II. Presenta una lista de posibles soluciones a cada requisito, las analiza, se decide cuál es la más apropiada y se diseña, desarrolla e implanta. Necesita establecer controles, con activos de seguridad TI, que aseguren que las actividades se realizan de acuerdo al Manual de Seguridad. Las actividades propuestas por el marco GPS-IICC son las siguientes::

- A1. Gestión de Riesgos.
- A2. Implementación de la Solución.
- A3. Diseño del procedimiento de monitorización de la solución..

Para la validación del marco propuesto se van a implantar las prácticas específicas definidas para la actividad *A1. Gestión de Riesgos*, que se detalla a continuación.

5.3.3.3.1. Gestión de Riesgos

A partir del organigrama, se conocen los activos, se ha realizado el análisis de los riesgos activos y servicios, se han establecido los requisitos de seguridad para cada uno de estos activos, en función de las amenazas, es el momento de tomar decisiones en cuanto a cómo se va a reducir el riesgo y el impacto asociado a cada activo. Se trata de realizar la gestión de riesgos.

GPS-IICC propone las siguientes prácticas específicas que se detallan en los siguientes sub-apartados:

- **III. SP 1.1. Diseño del procedimiento de implantación de activos de seguridad.**
- III. SP 1.2. Diseño de los procedimientos transversales.
- III. SP 1.3. Implantación de los activos de seguridad.

De estas prácticas específicas se ha implantado, para la validación del marco en el LABORATORIO IICC, la marcada en negrita y se describe a continuación.

a) Diseño del procedimiento de implantación de activos de seguridad.

El procedimiento de implantación de activos de seguridad describe un conjunto de tareas para implantar los activos de seguridad más adecuadas en cada caso.

Por lo tanto, tomando como base los resultados de las salidas de las tareas descritas en las fases anteriores, el objetivo del diseño del procedimiento de implantación de los activos de seguridad es definir las acciones a realizar para implantar los activos de seguridad vinculados con los activos de TI.

Las acciones incluyen:

- **Análisis de los activos de SI**. El objetivo de los activos de seguridad es reducir el riesgo y el impacto posible. Por lo tanto, los activos de seguridad se orientan a proteger los distintos tipos de activos. GPS-IICC define activos de seguridad

contra las amenazas a los distintos tipos de activos a proteger. Los activos de seguridad tratan amenazas materializadas, limitando su impacto (el de las amenazas) sobre los activos.

La eficacia de los activos de seguridad, se mide por el cumplimiento de sus objetivos:

- Disminución del Nº de amenazas materializadas y asociadas en el activo a proteger. En el caso ideal, el activo de seguridad mitiga totalmente la amenaza.
- Disminución del impacto de la amenaza:
- Disminución del número de activos afectados por el fallo.
- Aumento del número de fallos identificados y frenados.
- Disminución del tiempo de recuperar el sistema en caso de caída.

- **Estructurar los activos de SI**. Los activos de seguridad no son independientes unos de otros. GPS-IICC define una dependencia de activos de seguridad asociada a la estructura de los activos que se protege y que ha sido definida en el análisis de riesgos. Además, cada activo de seguridad se define y registra de acuerdo a los campos de la Tabla 5.12. Entre los campos se incluyen las métricas que permiten conocer su eficacia. La estructura del registro del activo de seguridad contempla los siguientes campos:

Tabla 5.6. Registro de activos de seguridad

Campo	**Descripción**
Código	Identificación única del activo de seguridad
Presencia	Estado que define su existencia o no en el sistema
Lista de amenazas que mitiga	Lista de amenazas objetivo para mitigar
Impacto sobre los activos	Cálculo acumulado del valor económico perdido por la materialización de las amenazas de acuerdo a lo establecido en el apartado c) del análisis de riesgos
Criticidad	Gravedad de acuerdo a lo establecido en el apartado c) del análisis de riesgos.
Frecuencia actual de la amenaza	Valor del número de veces que se ha materializado la amenaza
Frecuencia esperada	Valor del número de veces que se espera que se materialice la amenaza
Costes de la implantación	Estimación del coste de implantación del activo de seguridad. Coste de la aplicación (contratación y/o desarrollo) más las horas de trabajo persona/año. (Se consideran distintas alternativas de acuerdo al Manual de Seguridad)
Costes de mantenimiento	Estimación del coste de gestión de mantenimiento del activo de seguridad. Renovación de licencias, tiempo de mantenimiento. (Se consideran distintas alternativas de acuerdo al Manual de Seguridad)
Valor	Diferencia entre valor económico de los daños y el coste total del activo de seguridad
Eficacia	Métricas asociadas a la eficacia del activo de seguridad

El ANEXO VI describe un catálogo con los activos de seguridad básicos.

- **Definir el procedimiento de implantación de los activos de seguridad**. El procedimiento de implantación de los activos de seguridad, supone cambios en el sistema. GPS-IICC propone la definición de un Registro de implantación de activo de seguridad que sea tratado con las siguiente tareas:
  - Generar y definir un Registro de solicitud de cambio de seguridad que contenga referencias de todos los documentos y componentes que dieron lugar a la implementación del activo de seguridad (amenazas, vulnerabilidades de activos, activos afectados, procesos, impacto y riesgo).
  - Firma de que ha sido comprobado y verificado de acuerdo a las normas y al manual de seguridad.
  - Firmado por el responsable de seguridad y de implantación.
  - Lista de posibles incidentes de seguridad relacionados con el activo de seguridad.

5.3.3.4 Monitorización de los Activos de Seguridad

La *Fase IV. Monitorización de los activos de seguridad implantados* persigue detectar a tiempo los errores generados en los procesos, identificar posibles brechas, y anticiparse a los fallos de seguridad que provocan incidencias de seguridad. El uso de activos de seguridad TI y los informes que resultan de estos activos de seguridad permiten a los responsables de la organización identificar el comportamiento de los distintos recursos, garantizan el cumplimiento de los requisitos de seguridad previstos en el manual de seguridad. Las actividades propuestas por el marco GPS-IICC son las siguientes:

- **A1. Definición del procedimiento de monitorización y recuperación.**
- A2. Revisión de los Activos de seguridad TI.
- A3. Emisión de informes.

Para la validación del marco propuesto se van a implantar las prácticas específicas definidas para la actividad *A1. Definición del procedimiento de monitorización y recuperación*, que se detalla en el ANEXO VII.

5.3.3.4.1. Definición del procedimiento de monitorización y recuperación

Esta actividad contempla implantar los mecanismos que permitan obtener evidencias del cumplimiento de:

- La efectividad de cada activo de seguridad que se ha implantado.
- La recuperación del sistema de acuerdo a los requisitos que se han establecido.

Para ello, GPS-IICC propone las siguientes prácticas específicas que se detallan en los siguientes sub-apartados:

- IV. SP 1.1. Definición de las métricas y controles de monitorización de activos.
- **IV. SP 1.2. Monitorización de la recuperación y la continuidad.**

De estas prácticas específicas se han implantado, para la validación del marco en las empresas, las marcadas en negrita y se describen a continuación.

Monitorización de la recuperación y la continuidad

El principio de disponibilidad está estrechamente vinculado con la continuidad, ya no sólo del desarrollo del servicio o proyecto, sino también de la propia organización. Por ello, en el caso analizado sobre el que se ha validado el marco GPS-IICC se prioriza la monitorización de la recuperación del sistema garantizando la continuidad entre las prácticas específicas a implantar. La monitorización de la continuidad está estrechamente vinculada con la monitorización de las incidencias. El plan de contingencia se ejecuta ante la aparición de una incidencia de máximo impacto. Su objetivo será la recuperación del servicio evitando pérdidas.

A continuación, se muestra la descripción de las tareas:

- **Definir los activos críticos a monitorizar**. El plan de contingencia previene las acciones que se deben realizar en el momento en que surge una incidencia de alto riesgo. Los principales activos que GPS-IICC propone estudiar en cada caso de validación incluyen al menos los siguientes:

Tabla 5.7. Activos de TI críticos

Activos críticos de TI	**Descripción**
PC de puestos de trabajo	Hardware y software conectados a la LAN que permiten desempeñar la función del empleado del Laboratorio.
Servidor de aplicaciones	Servidor en el que se aloja el software operativo que necesita el Laboratorio para desempeñar sus funciones.
Control server	Software de control de supervisión de PLC y que jerárquicamente tiene ascendencia sobre dispositivos de control de niveles inferiores.
Servidor SCADA o unidad maestra	*Master unit* del sistema.
Unidades y terminales remotas RTU	Dispositivos de campo equipados muchas veces con interfaces de telemétricos.
Controlador Lógico programable (PLC)	Realiza funciones lógicas de relays, switches, y temporizadores/contadores mecánicos.
Dispositivos de Electrónica Inteligente (IED).	
Interfaces hombre-máquina	
Servidor Input/Output (IO).	
Servidor de datos	Servidor que aloja las BB.DD. necesarias con los datos utilizados por las aplicaciones en el desempeño funcional del Laboratorio
Servidor de configuración	Servidor que aloja toda la información en relación con la configuración del sistema: aplicaciones, BB.DD., servicios, roles, etc.
Línea/s ADSL	Acceso a Internet por una línea de banda ancha.

Cortafuegos	
Switch de la LAN	
Suministro eléctrico	Fuente energética que alimenta todo el HW del Laboratorio.
Gestión de Incidencias	Proceso por el que se monitorizan las incidencias que ocurren y el impacto sobre los activos, y se activan los mecanismos de solución hasta su cierre.
Proceso de negocio clave	Proceso de negocio cuyo valor es clave para la organización. Su no disponibilidad supone la pérdida de confianza del/os usuario/s y pone en peligro la continuidad de la organización.

- **Definir la estructura del registro de contingencia**. El plan de contingencia necesita tener definido de antemano, las acciones que se han de realizar en distintos escenarios, en los que una amenaza, con un factor de impacto crítico, se materialice y termine con el servicio/proyecto o la misma empresa. Por ello, GPS-IICC define un plan de contingencia con una estructura (véase ANEXO VII) que permite conocer cómo actuar, antes, durante y después de una incidencia de seguridad crítica:
  - Código de la incidencia ocurrida. Único que la identifica como única.
  - Activos afectados. Activo/s afectados por la incidencia.
  - Acciones a realizar. Acciones que se han de realizar en caso de que ocurriera la incidencia.
  - Tiempo máximo de resolución. Tiempo estimado para la resolución de la incidencia.
  - Responsable de cada acción. Responsables de las acciones que se describen (ejecutar, informar…).
  - Pruebas de mantenimiento. El plan de continuidad hay que mantenerlo y se describen las pruebas a las que someter cada acción definida.
  - Periodicidad de las pruebas. La periodicidad con la que se prueba el éxito de las acciones también se describe.
  - Registro e Informes. La incidencia se registra utilizando la misma estructura que las incidencias y se realiza un informe de los resultados de cada prueba con los resultados esperados, las variaciones que se han producido, y las solicitudes justificadas de posibles cambios.

5.3.3.5 Mejora Continua del Proyecto de TI seguros

La *Fase V. Mejora continua del proyecto TI seguro* persigue tomar un conjunto de decisiones que, en un futuro, permitan la mejora de los servicios/proyectos Las actividades propuestas por el marco GPS-IICC son las siguientes:

- A1. Revisión del estado actual.
- **A2. Planificar y comunicar plan de mejora.**.

Para la validación del marco propuesto se va a implantar la práctica específica SP 2.2 relativa a la gestión de decisiones de mejora de la Actividad A2. Esta práctica específica se describe en el siguiente sub-apartado.

5.3.3.5.1. Planificación y comunicación del plan de mejora

Con las medidas e informes extraídos de las medidas de monitorización, está definido el estado de seguridad actual del servicio o proyecto. En este punto, el marco propone la implantación y comunicación de un plan de mejora. Se proponen dos prácticas específicas:

- V. SP 2.1. Planificación del procedimiento de mejora.
- V. SP 2.2. Comunicación de resultados de decisión.

Para la validación del marco GPS-IICC, se propone abordar, en el patrón que se define, la implantación de la práctica específica SP 2.2. Comunicación de resultados de decisión que se describe en el sub-apartado siguiente.

Comunicación de resultados de decisión

Las decisiones tomadas después de las revisiones de los informes de monitorización, se comunican a las partes implicadas de los servicios/proyectos revisados. Tanto, si no se ha tomado decisión alguna como si con la decisión, existe un plan de actuación asociado, todas las decisiones son comunicadas.

- **Detallar el plan de actuación**. El plan de actuación requiere del estudio y priorización de las decisiones de mejora. Necesita de los datos producidos en los informes de monitorización de la fase anterior.
  - Convocar reunión de mejora. El comité de mejora genera un acta de cada reunión de la dirección del LABORATORIO IICC con el objetivo de planificar las mejoras. Esta reunión se realiza mensualmente, o si fuera necesario, después de un cambio importante. La estructura del acta de reunión de Revisión y Mejora es la que sigue:
    - Personas convocadas: director general, gestor de seguridad, responsable de proyecto y representante de las partes implicadas en el objetivo de la reunión.
    - Personas que asisten: nombre y firma de las personas que asisten a la reunión.
    - Fecha: fecha de celebración de la reunión.
    - Duración: duración estimada de la reunión.
    - Lugar: punto de reunión.
    - Objetivo a tratar: tema del día y objetivo/s que se pretende alcanzar.
    - Puntos del orden del día: pasos a realizar en la reunión.
    - Documentación asociada a la reunión.

- Conclusión: conclusiones como resultados de los temas tratados.
- Planes de Acción: acciones detalladas a realizar, mecanismos de monitorización y aprobación del acta.
- Fecha de próxima reunión: fecha prevista para la próxima reunión de revisión y mejora.

o Detallar el plan. Con estos datos, se realizan las siguientes acciones:

- Definir el objetivo de mejora, y los criterios seguidos para su evaluación y medida.
- Definir los recursos necesarios para planificar y en función del respaldo económico en caso de que no se dispongan.
- Revisar la actualización de los activos TI relacionados con el servicio/ proyectos que se está planificando.
- Determinar los responsables del servicio/proyecto y de cada tarea.
- Analizar las distintas alternativas de solución.
- Describir las actualizaciones que derivarán durante la vida del servicio/proyecto.
- Revisar que los nuevo prerrequisitos de seguridad estén alineados con la política.
- Priorizar y describir las tareas de realización del proyecto.
- Determinar los hitos de cada tarea planificada.
- Determinar los factores clave de éxito del proyecto.

5.3.4 Resultados de la línea final

Una vez aplicado el patrón para el marco propuesto, se repite el paso 2 del método de experimentación que se indica en el apartado 5.2. Se mantiene una reunión con los responsables de proyecto del LABORATORIO IICC y cumplimentan de nuevo el mismo cuestionario de la fase inicial.

La Tabla 5.8 muestra los resultados de los cuestionarios correspondientes al análisis ponderado de las respuestas en el caso estudiado. Igual que en la fase inicial y aplicando los mismo criterios, se conoce el nivel de aplicación o cobertura de cada pregunta en el caso analizado, valorando los activos de seguridad definidos en el marco GPS-IICC.

Tabla 5.8. Línea base final. Resultado de la evaluación de las preguntas

F I		F II		F III		F IV		F V	
I.P01	4	II.P01	2	III.P01	4	IV.P01	0	V.P01	0
I.P02	1,25	II.P02	0,6	III.P02	4	IV.P02	1	V.P02	0
I.P03	4	II.P03	0	III.P03	0	IV.P03	0	V.P03	0
I.P04	0	II.P04	4	IV.P04	2	IV.P04	4	V.P04	2
I.P05	2,75	II.P05	3,50	III.P05	1	IV.P05	4	V.P05	0
I.P06	2	II.P06	2	III.P06	0	IV.P06	4	V.P06	0
I.P07	0	II.P07	4	III.P07	0	IV.P07	0	V.P07	1

I.P08	**0**	**II.P08**	**0**	**III.P08**	**4**	**IV.P08**	**2**	**V.P08**	**0**
I.P09	**0**	**II.P09**	**0**	**III.P09**	**2**	**IV.P09**	**0**	**V.P09**	**0**
I.P10	**4**	**II.P10**	**0**	**III.P10**	**3**	**IV.P10**	**0**	**V.P10**	**0**
I.P11	**4**	**II.P11**	**0**	**III.P11**	**1**	**IV.P11**	**0**	**V.P11**	**0**
I.P12	**4**	**II.P12**	**2**	**III.P12**	**0**	**IV.P12**	**0**	**V.P12**	**0**
I.P13	**3,50**	**II.P13**	**0**	**III.P13**	**0,25**	**IV.P13**	**0**	**V.P13**	**0**
I.P14	**4**	**II.P14**	**0**	**III.P14**	**0**	**IV.P14**	**0**	**V.P14**	**0**
I.P15	**4**	**II.P15**	**2**			**IV.P15**	**4**	**V.P15**	**0**
I.P16	**0**	**II.P16**	**4**			**IV.P16**	**1**	**V.P16**	**0**
I.P17	**0**	**II.P17**	**2**			**IV.P17**	**0**	**V.P17**	**0**
I.P18	**0**	**II.P18**	**4**			**IV.P18**	**0**	**V.P18**	**0**
						IV.P19	**0**	**V.P19**	**0**

Así, de la línea final de la evaluación del cuestionario de validación en la *Fase I. Inicio y Dirección* se concluye:

1. Las valoraciones máximas han subido con respecto a la línea base inicial. Hasta un 38% de las preguntas de esta Fase I obtienen una puntuación de 4. Esto resulta de la aplicación de una política de seguridad que marca, a través del Manual de seguridad, las acciones necesarias para la implantación de los activos de seguridad. Además, se clasifican los activos de TI y se identifican las amenazas evaluando su impacto sobre la pérdida de valor de los mismos lo que repercute en un mayor alineamiento del Laboratorio y su dirección con la estrategia de seguridad TI.

2. Además, un 44% de las preguntas tienen una valoración igual o mayor que el umbral mínimo 3,00. Lo que supone que esta fase ha mejorado ampliamente respecto a la línea base inicial. Las preguntas que se ven afectadas son {P1, P2, P3, P10 a P15}. De estas valoraciones, de la fase de Inicio y Dirección, se deduce que se ha establecido una línea base de trabajo superior al 3,00. Esta línea base es aceptable por el LABORATORIO IICC, para continuar en las fases posteriores del marco.

Por lo tanto, en esta fase inicial, se ha hecho un esfuerzo por definir y establecer, para los activos de TI, su estado de seguridad inicial. Definiéndose la política de seguridad, el manual de seguridad, y el procedimiento para registro de los activos de TI con la información (amenazas, impacto y riesgo) de los resultados.

Respecto a la *Fase II. Definición de requisitos de seguridad*, proporcionan la siguiente información:

1. Un 27,7% de las preguntas se han valorado con un valor igual o superior al umbral 3,00. Este subconjunto de preguntas está formado por {P04, P05, P07, P16 y P18}, las cuales identifican las acciones encaminadas a la definición de un procedimiento que permita establecer los requerimientos de SI (C/I/D) para los activos de tecnologías de la información y la definición de los perfiles de acceso a cada servicio y la creación de un catálogo de requisitos estructurado con indicadores de cumplimiento.

2. A las prácticas específicas de las actividades de la fase de definición de requisitos de seguridad, y comentadas en el punto anterior, se añade la definición de un procedimiento de identificación de los requisitos de activos y la creación de un catálogo de requisitos estructurado con indicador de cumplimiento.

3. Los valores mínimos para el conjunto de las preguntas, en esta línea final, están por encima de los valores máximos establecidos en la fase inicial, aunque en menor medida que sucedía en la Fase I.

La línea final de evaluación de la Fase III. Diseño e Implantación de las Soluciones aporta los siguientes valores:

1. En esta fase de diseño, el 28,6% de las preguntas se han valorado con un valor igual o superior al umbral 3,00. Este subconjunto de preguntas está formado por {P01, P02, P08, y P10}, las cuales identifican algunas acciones realizadas y encaminadas a procesos de administración de riesgos, de BB.DD. con activos de seguridad asociados a los activos de TI, de incidencias relativas a los activos de tecnologías de información y pruebas de cumplimiento.

2. El incremento del 100% de los ítems con valoración aceptable apunta un enfoque acertado del patrón propuesto, el cual facilitará en la fase IV la monitorización y el seguimiento de las trazas de acceso y cambio en los registros de información.

En la línea final de evaluación para la *Fase IV. Monitorización* cabe destacar:

1. Sólo dos ítems han podido incrementar su valoración sin superar un valor igual o superior al umbral 3,00. Esto se corresponde con las preguntas {P02 y P16}. Se trata de algunas acciones orientadas a la monitorización, gestión de contingencia y a procedimientos de activación y monitorización de la gestión de copias de seguridad y respaldo.

2. El escaso tiempo dispuesto desde el diseño de patrón y su aplicación implica que no haya habido posibilidad de desarrollar acciones encaminadas a la recuperación de los umbrales mínimos definidos para los KPIs de los procedimientos, que se revise de modo efectivo la política de seguridad y se realicen informes para la mejora de los procedimientos. No obstante, la continuidad en el proceso de mejora introducido por el patrón permitirá generar evidencias más allá de la definición de procedimientos de activación y monitorización de la gestión de copias de seguridad y respaldo, y la revisión de los activos que permitirán la monitorización de los informes asociados.

Finalmente, la evaluación de la *Fase V. Revisión y Mejora*, orientada a la mejora continua arroja resultados similares a la Fase IV. Son los siguientes:

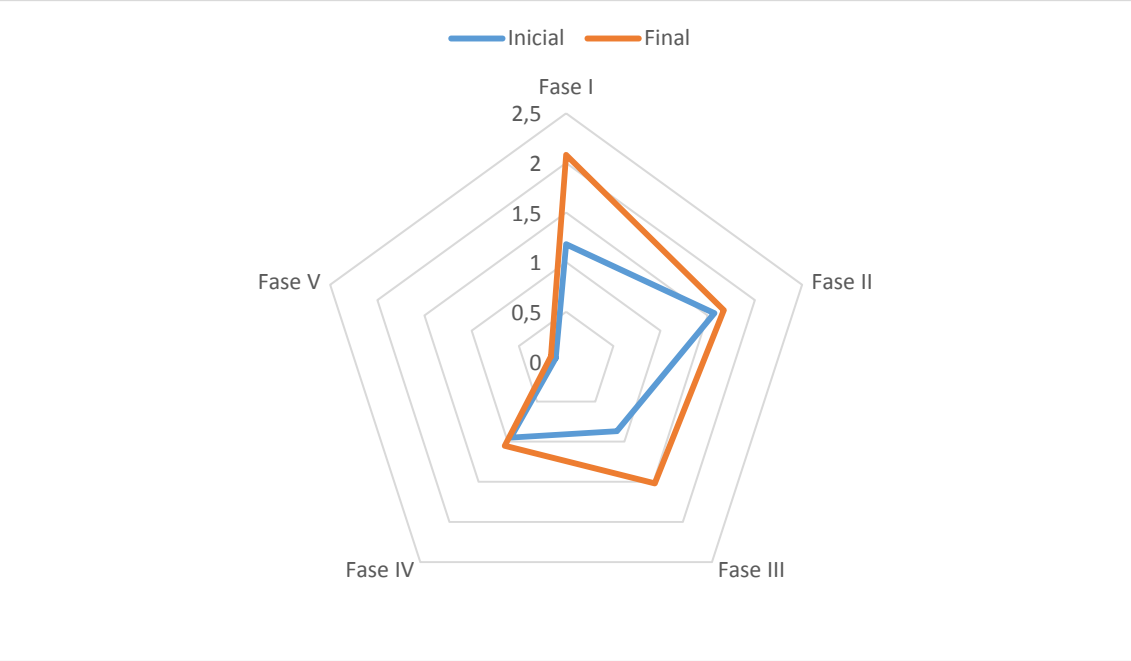
1. Sólo un ítem se ve incrementado en la validación, pero tampoco con un valor igual o superior al umbral 3,00. Esto se corresponde con la pregunta {P07}. Estas preguntas son relativas a la elaboración de informes que responden a un plan de mejora, en el que se utilizan los registros de monitorización para la toma de decisiones, en parte utilizando alguna herramienta, pero fundamentalmente intercambiando información entre los diferentes gestores o procesos de gestión.

2. La indisponibilidad de tiempo para observar la evolución del patrón propuesto en términos de desarrollo de un ciclo de mejora continua explica que tampoco la Fase V se vea afectada significativamente por su aplicación.

5.3.6 Comparación resultados líneas inicial y final

La Figura 5.3 muestra la combinación de los resultados de las líneas inicial y final, ofreciendo una visión de las áreas de proceso mejoradas para el caso del LABORATORIO IICC en cada fase para el patrón elegido.

Figura 5.3. Resultados comparados de las líneas inicial y final



Para la estimación de la mejoría en los resultados entre las líneas inicial y final se ha utilizado la expresión:

Mejora = ((Valoración Final - Valoración Inicial) / 4)* 100

1. En todas las fases se ha experimentado una mejor valoración tras la aplicación del patrón propuesto.

2. En la Fase I de Inicio y Dirección, el promedio de mejora es del 22,57%. En un 31,5% de las preguntas se ha mejorado.

3. En la Fase II de Definición de Requisitos de Seguridad, el promedio de mejora es del 2,5%.

4. En la Fase III de Diseño de la Solución, el promedio de mejora es del 16,1%. En esta fase EL 21,4% de las preguntas han mejorado.

5. En la Fase IV de Monitorización, el promedio de mejora es del 2,63%.

6. En la Fase V de Revisión y Mejora, el promedio de mejora de GESTORIA es del 1,32%.

5.3.7 Conclusiones

Un patrón de trabajo es una herramienta que facilita él éxito en las metas para las tareas en las que se aplica. No se trata de garantizar el éxito total sobre estas actividades. Se trata de establecer una guía que pueda repetirse y ayude a mejorar los resultados de las acciones, reduciendo los errores más comunes. El marco que se ha presentado pretende, a través del patrón, ayudar en la gestión de proyectos SI en entornos de IICC. Pretende recoger el Lifecycle completo de los proyectos de tecnologías de la información abordados en este tipo de organizaciones, sea cual sea el sector del que se trate,. Si se consigue esto, se puede decir que el marco de trabajo y más concretamente el patrón elegido para los proyectos es útil y ha cumplido su cometido. Y es lo que se trata de ver en este capítulo, si las hipótesis que daban sentido al trabajo de este Trabajo Fin de Master se han cumplido y, por tanto, se han conseguido los resultados buscados.

Así, después de: (a) establecer la línea base a través de un conjunto de preguntas basadas en SbD, (b) implantar el marco definido en un caso práctico, (c) evaluar las mismas preguntas a término, y (d) comparar los resultados de evaluación inicial y final, se puede concluir que se han cumplido parcialmente los objetivos esperados y se pueden validar las hipótesis de trabajo.

Para la hipótesis general:

HG1. "Si una organización, sea cual sea su sector de infraestructuras críticas, se apoya en un marco de trabajo que le facilite un patrón de seguridad para la gestión de sus servicios/proyectos de TI, conseguirá mejorar el desarrollo y la prestación de esos servicios / proyectos".

HD 1. Si una Infraestructura Crítica desarrolla una Política de Seguridad y la respalda con un Manual de Seguridad podrá obtener el compromiso tanto de los empleados TI, en relación al desarrollo de los servicios/proyectos de TI, como del resto de empleados de otros departamentos como usuarios de los servicios TI.

Esta hipótesis queda validada con la aplicación de la política y el manual de seguridad. Véase sección 5.3.3.1.1 Definir la política de seguridad, en sus apartados a) y b) y los ANEXOS III y IV.

HD 2. Si una IICC define un catálogo de requisitos de seguridad podrá asociar a cada activo, el/los requisitos y, más tarde, gestionar los Controles o Activos de Seguridad TI que faciliten su cumplimiento.

Esta hipótesis queda validada con la definición e implantación del procedimiento Definición del catálogo de requisitos, definida en la sección 5.3.3.2 concretada en su apartado c) Definir los requisitos de seguridad, y los ANEXOS IV y VI.

6. Aportaciones, conclusiones y líneas futuras

6.1 Introducción

El estudio del estado de la cuestión, realizado en el Capítulo 2, aporta una estructura de factores SbD para la evaluación de la seguridad los procesos a nivel de estrategia (Gobernanza TI), táctica (Mejora de Procesos y Gestión de Servicios) y operativa (Gestión de Proyectos y Gestión de SI). Además, se realiza un análisis comparativo con el los elementos de la metodología SbD en los principales modelos normativos y normas de protección de IICC. Este mapeo puede servir de ayuda a los distintos profesionales TIC que, en distintos niveles organizativos, estén desarrollando actividades con distintos marcos en IICC. Finalmente, se aporta un resumen de las publicaciones más significativas sobre modelos de administración de SI en IICC y que son el resultado de un proceso de revisión sistemática en las fuentes más reconocidas.

La principal aportación del Capítulo 4 es el marco GPS-IICC. Se trata de una versión del modelo GPS-PYMEs desarrollada por De la Cámara y Arcilla (2016), validada a la problemática planteada en el Capítulo 1 de este TFM: los entornos de organizaciones que trabajan sistemas de control de industrial e Infraestructuras Críticas. En cuanto a las prácticas propuestas en el modelo y el patrón de proceso validado y que se aportan, cabe destacar:

a) Política de seguridad en un Laboratorio de IICC. La política sería adaptable a un entorno variable y diferentes tipos de IICC.

b) Manual de seguridad orientado a usuarios tanto con perfiles de TIC como no.

c) Clasificación de activos TI. Útil para que la organización seleccione fácilmente sus activos.

d) Catálogo de activos de Seguridad.

6.2 Conclusiones

El déficit de normas de rango internacional que orienten la regulación de las aplicaciones concretas en SI afecta especialmente al ámbito de la seguridad tecnológica ya que al desigual nivel de desarrollo político y legal entre países, se une el dispar desarrollo tecnológico entre los mismos. Si en el marco del desarrollo de un marco común regulador en materia de seguridad cibernética existe el Convenio de Budapest, con sus limitaciones y escaso alcance mundial, en el ámbito de la securización de IICC no existe nada similar todavía.

Disponer de un modelo de evaluación y referencia de cumplimiento contra los principales estándares de seguridad TI puede servir para avanzar en la facilidad de utilizar SGSI en los servicios TI en Infraestructuras Críticas. Un modelo generalista como el que hemos probado en este Trabajo Fin de Master puede aportar algunas ventajas, pero una posterior

evolución hacia un modelo sectorial, que distinga la especificidad de las IICC puede ser aún más potente y útil.

A continuación se enumeran las ventajas que disponer de un Modelo generalista puede proporcionar a los operadores de las infraestructuras:

- La aplicabilidad del Modelo alinea los objetivos de seguridad TI de la Dirección y los procesos organizativos del operador con los objetivos de protección de sus infraestructuras, mitigando los riesgos de que se materialicen las amenazas.
- Ayuda a concretar los planes de acción o los proyectos de mejora de los operadores en relación a la protección de las infraestructuras.
- Facilita la mejora de los procesos a los operadores.
- Mejora la imagen corporativa y el prestigio de la organización ante los reguladores, usuarios y terceros. Se convierte, por tanto, en una demostración de la profesionalidad de la organización y en una garantía de su correcto funcionamiento.
- Facilita la posterior certificación de la solvencia técnica en materia de seguridad integral, y en especial, de los Sistemas de Control Industrial, y mejora la concienciación y la formación de los usuarios.
- Facilita una mayor visibilidad del área de seguridad (ya sea integral, física o ciberseguridad) de los operadores con el resto de áreas dependientes.

6.3 Líneas futuras de trabajo

Nuestro modelo tiene una vocación generalista, susceptible de ayudar a implantar un modelo de gestión de proyectos de desarrollo seguro en cualquier IICC independientemente del sector al que pertenezca. No obstante, futuras líneas de trabajo permitirían adaptar nuestro modelo GPS-IICC sectorialmente, de modo que

- Esté disponible un Modelo Sectorial permita particularizar todo el proceso del sector, como ya se ha comentado anteriormente en este documento: activos, amenazas, vulnerabilidades, cultura, madurez de la industria, etc.
- Establecer un Modelo de forma que se ayude, en mayor nivel, a las organizaciones a mitigar los riesgos sobre sus activos TI específicos.
- Definir el alcance en términos de las organizaciones que van a estar afectadas por el Modelo y los entornos de sistemas que van a ser considerados en el alcance. La evolución de los modelos normativos y estándares apuntan a esta línea de sectorización. Por ejemplo, NERC CIP en versiones anteriores se decantó por listar expresamente las organizaciones afectadas. Otro ejemplo, es el estándar PCI-DSS, en el que se detalla la tipología de organizaciones afectadas: empresas adquirientes, entidades emisoras, comercios, proveedores de servicios y procesadores de pago.
- El Modelo tendría que definir los roles y responsabilidades, clarificando las normas específicas aplicables.

- Identificar y categorizar los activos propios del sector proporciona una mayor consistencia a la evolución de un Modelo específico, siempre y cuando, las categorías de activos estén bien relacionadas con las amenazas, las vulnerabilidades y los controles que van a mitigar los riesgos de estos activos. El estándar NERC CIP es un ejemplo de cómo relacionar activos con los controles a implantar.
- Un aspecto similar a categorizar los activos es Valorar el Impacto asociado a los mismos de forma sectorial. Establecer una escala de niveles de impacto en la que se definan los criterios que diferencian cada uno de los niveles proporciona valor al resto del proceso. NERC CIP, CFATS o PCI-DSS son ejemplos de regulaciones en las que se han establecido escalas de impacto y asignar un nivel u otro conlleva tener que implantar controles diferentes.
- Identificar y Valorar las Amenazas a través de un catálogo de amenazas establecido en el Modelo ayuda a las organizaciones a conocer en que escenarios de ataque tienen que focalizar sus esfuerzos. NRC - RG 5.71 y CFATS son dos modelos en los que se definen catálogos de amenazas.
- Disponer de un adecuado Catálogo de Controles basado en estándares o buenas prácticas proporciona robustez al Modelo. De manera general, todos los modelos analizados disponen de catálogos de controles detallados y basados en buenas prácticas. Un ejemplo es el Framework de Ciberseguridad del NIST, en el que los controles establecidos están mapeados con varios estándares internacionalmente reconocidos.

Una evolución posterior aún más potente sería el desarrollo de una herramienta que pueda proporcionar una guía o una ayuda a las organizaciones que estén implantando los controles o los requisitos establecidos en el Modelo. Un ejemplo de referencia es la herramienta del Framework de Ciberseguridad del NIST, con nombre "Framework Profile", que facilita conocer el grado de madurez actual en cuanto a ciberseguridad, seleccionar el nivel objetivo a futuro y conocer la brecha (*gap*) que necesitan subsanar para llegar a los objetivos marcados.

Anexo I. Preguntas validación inicial y final

S=Siempre U=Usualmente A=A veces R=Rara vez N=Nunca						
Cód.	**Pregunta**	**S**	**U**	**A**	**R**	**N**
FASE I. A1	**Declaración de la política de seguridad**					
FASE I. SP 1. 1	**Definir la política de seguridad**					
I.P01	¿Existe un documento público con la política de seguridad para los proyectos de TI? EV: Documento con la declaración de la política de seguridad por la que apuesta la organización.					
I.P02	¿Existe un documento que defina los objetivos y metas de seguridad en cada proyecto que se aborda? EV: Objetivos (metas medibles) de seguridad que se afrontan en cada proyecto o servicio.					
FASE I. SP 1. 2	**Definir el "Manual de seguridad"**					
I.P03	¿Existe un fichero de roles asociados a responsabilidades de seguridad relacionadas con el uso de las TI? EV 1: Fichero con la descripción de los roles, sus responsabilidades, formación, privilegios, y obligaciones al principio, durante y al término de ejercer el rol (procedimiento de gestión de roles). EV 2: Existen distintos perfiles.					
FASE I. SP 1. 3	**Realizar el análisis de riesgo de los activos de información**					
I.P04	¿Existe un proceso de análisis de riesgos y seguridad en proyectos/servicios TI? Ej: Definición del proceso de análisis de riesgos y seguridad proyectos de TI.					
I.P05	¿Existen procedimientos que definen, cómo se evalúan, y registran las vulnerabilidades, amenazas y riesgos asociados a los proyectos/servicios de TI? Ej: Documento que explicita el procedimiento de Registro de vulnerabilidades, amenazas y riesgos asociados a los activos involucrados en proyectos/servicios de TI.					
I.P06	¿Existe un fichero de activos de la organización con vulnerabilidades, amenazas y riesgos asociados? Ej: Fichero con los activos de la empresa con vulnerabilidades, amenazas y riesgos asociados.					
FASE I. SP 1. 4	**Definir documento de respaldo financiero y compromiso**					
I.P07	¿Existe un procedimiento explícito para la estimación de los costes de seguridad asociados a los proyectos de TI? Ej: Procedimiento de asignación de costes a la partida de seguridad.					
I.P08	¿Existe una partida para seguridad TI en el presupuesto asignada a los proyectos de TI? Ej: Partida de seguridad del presupuesto del proyecto desglosada.					
I.P09	¿Existe un documento con la declaración de viabilidad de cada proyecto/servicio de TI? Ej:					

	Fichero con una declaración de la realización de los procedimientos que aseguran los servicios/proyectos de TI.					
FASE I. A 2	**Definición de prerrequisitos de seguridad**					
FASE I. SP 2.1	**Definir el catálogo de proyectos/servicios de TI**					
I.P10	¿Existe un catálogo de servicios de TI asociados a cada departamento de la empresa? Ex: Registro de servicios TI con descripción y departamento afectado.					
FASE I. SP 2.2	**Definir catálogo de proyectos/servicios de seguridad de TI**					
I.P11	¿Existe un catálogo de servicios de seguridad de TI? Ex:Lista de servicios de seguridad TI clasificados y descritos.					
I.P12	¿Hay implantado algún servicio de seguridad de TI? Ex: Conocimiento de la ejecución de algún servicio de seguridad de TI (p.ej., LOPD, autenticación, contraseñas, Backup, ...).					
FASE I. SP 2.3	**Vincular proyectos/servicios de seguridad TI a servicios TI**					
I.P13	¿Existe un procedimiento explícito que permita vincular proyectos/servicios de seguridad TI a otros servicios de TI? Ex: Documento que defina procedimiento para vincular servicios de seguridad TI a servicios TI.					
FASE I. A 3	**Planificación y comunicación**					
FASE I. SP 3.1	**Definir el plan de proyecto seguro**					
I.P14	¿Existe un plan de seguridad para abordar diferentes proyectos de TI? Ex: criterios de clasificación de prioridades de abordar los proyectos de seguridad de los servicios/proyectos TI (Backup, Puestos de trabajo, emails, SB, SE, ...).					
FASE I. SP 3.2	**Comunicar el plan de proyecto seguro**					
I.P15	¿Está disponible para todos los empleados un documento formal (PS, Plan de Seguridad) con los requisitos de seguridad y penalizaciones para la organización y es comprensible para ellos? Ex: Documento público con el plan de seguridad, plantilla de evaluación de comprensión del plan y penalizaciones o proceso disciplinario en caso de no cumplimiento.					
I.P16	¿Se comprueba con cada departamento que sus necesidades de seguridad están contempladas en el proyecto TI que se aborda? Ex Acta de reunión con las necesidades de seguridad necesarias en el servicio o proyecto que se aborda firmadas por las partes implicadas.					
FASE I. SP 3.3	**Revisión del plan de proyecto seguro**					
I.P17	¿Existe un documento con la declaración de viabilidad de cada proyecto/servicio de TI? Ex: Fichero con una declaración de la realización de los procedimientos que aseguran los servicios/proyectos de TI.					
I.P18	¿Existe una guía de auditoría de seguridad en los					

	proyectos de TI? E: Existe un documento que indica qué necesidades de seguridad se tienen que evaluar: LOPD, ISO 9001, regulaciones.					
FASE II. A1	**Clasificación de activos**					
FASE II. SP 1.1.	Definir criterios de C/I/D para los activos de información					
II.P01	¿Existe un procedimiento que permite clasificar la información de acuerdo a los criterios de confidencialidad, disponibilidad e integridad? Ev: Se definen los criterios de C/I/D de la información y se establece un proceso para definir los requisitos de C/I/D para cada activo de información de acuerdo a estos criterios (p.ej., confidencialidad de impagos, multas, juicios, datos de fallecidos, nóminas, errores, patentes, etc.					
II.P02	¿Se definen umbrales requeridos para la C/I/D de la información en cada proyecto de TI? Ev: Intervalos de No Disponibilidad, Tiempos de exposición de información confidencial al público, Tiempos de actualización de la información, Tiempos de no respuesta, Tiempos de emisión de informes, Número de incidencias de seguridad/Nº total de incidencias, etc.					
II.P03	¿Se define un procedimiento de etiquetado y manipulación de acuerdo a los criterios de C/I/D? Ev: Activos etiquetados junto con el procedimiento de manipulación y acceso.					
FASE II. A2	**Definición del catálogo de requisitos de seguridad**					
FASE II. SP 2.1.	**Definir requisitos de acceso**					
II.P04	¿Tiene cada identificador de acceso un propietario responsable de las acciones que se realicen? Ev: Cada identificador tiene un propietario responsable.					
II.P05	¿Se definen los perfiles de acceso a los servicios/proyectos de TI? Ev: Existen perfiles definidos acordes a los roles y responsabilidades.					
II.P06	¿Se define un proceso para la gestión de accesos a los servicios/proyectos de TI? Ev: Documento que define el procedimiento de control de acceso de acuerdo a la política y los requisitos. Además define el procedimiento de alta, baja y modificación o renovación/revocación de las claves de acceso a los activos y/o servicios de TI como email, BBDD, ficheros, aplicaciones.					
II.P07	¿Existen técnicas de cifrado establecidas para asegurar las claves de acceso de cada usuario? Ev: Técnicas y algoritmos que permiten el cifrado que asegure confidencialidad e integridad.					
FASE II. SP 2.2.	**Definir requisitos de terceros**					
II.P08	¿Existe un catálogo de requisitos de seguridad para los servicios TI que son provistos por terceras partes (proveedores)? Ev: Requisitos de seguridad legales, LOPD, normativas ISO 9001 y propios de la					

	organización, p.ej., requisitos establecidos en los umbrales de seguridad Web, SLAs relativos a la contratación de productos/servicios a terceros.					
II.P09	¿Existen acuerdos de nivel de servicio que reflejen criterios de disponibilidad e integridad? Ex: Existencia de SLAs que reflejen condiciones de disponibilidad y/o integridad de la información.					
II.P10	Contemplan los contratos las necesidades de revisión y cambio dependiendo de la criticidad del servicio/ aplicación que se provee? Ex: Registros de cambios motivados por situaciones críticas.					
FASE II. SP 2.3.	**Estructurar el catálogo de requisitos y planificar soluciones**					
II.P11	¿Existe un catálogo de requisitos de seguridad con alternativas de solución clasificadas atendiendo a los principios de seguridad (C/I/D) de la información, normativas y/o al activo que se quiera proteger (instalaciones, personas, equipos, comunicaciones, soportes de información)? Ex: Existe un registro de requisitos y activos de seguridad como alternativas de solución clasificadas de acuerdo al activo que se quiere proteger y el principio (C/I/D). Prioridad muy alta.					
II.P12	¿Se estudian las capacidades para la implantación de los nuevos servicios y soluciones? Ex: Documento con las capacidades que aseguran la viabilidad del proyecto y el funcionamiento del nuevo servicio de acuerdo a los requisitos, así como su aceptación por parte de la dirección.					
FASE II. A3	**Definición requisitos monitorización**					
FASE II. SP 3.1.	**Definir registros de monitorización del catálogo de requisitos**					
II.P13	¿Se definen los indicadores de cumplimiento de requisitos de seguridad atendiendo a (C/I/D) de la información y/o al activo que se quiera proteger (instalaciones, personas, equipos, comunicaciones, soportes de información)? Ex: Existe un registro con la definición de los indicadores de cumplimiento del requisito.					
II.P14	¿Se definen los indicadores de cumplimiento de requisitos de seguridad atendiendo a prevención y recuperación? Ex: Existe un documento con información de los requisitos (umbrales) de detección de fallos y recuperación del sistema.					
II.P15	¿Se definen los indicadores de cumplimiento de requisitos de seguridad acordes a las leyes y normas de obligado cumplimiento? Ex: Definición de controles y procedimientos de auditorías.					
II.P16	¿Existen controles de las técnicas que permiten la detección y protección contra software malicioso, ejecuciones de código no seguro descargado por parte del cliente? Ex: Soluciones para la detección y protección contra software malicioso, ejecuciones de código no seguro, etc.					
II.P17	¿Existen controles que permitan conocer cómo ha					

	sido gestionada y manipulada la información? Ev: Definición de procedimientos y técnicas de trazabilidad, gestión de incidencias, cambios, configuración, etc.					
II.P18	¿Existen controles que permitan supervisar el uso no autorizado de la información? Ev: Mecanismos de control del uso no autorizado de la información (control de acceso, auditorías, etc.).					
FASE III. A1	**Gestión de Riesgos**					
FASE III.SP 1.1.	**Diseñar el procedimiento de implantación de activos de seguridad**					
III.P01	¿Existe un proceso definido e implantado para la gestión de riesgos asociados a los proyectos de TI? Ev: Documento con el procedimiento definido para la gestión de riesgos identificados en la fase inicial de dirección, identificando activos y soluciones asociadas frente a los riesgos, identificando la reducción del impacto sobre los activos, coste asociado y posibles alternativas de solución.					
III.P02	¿Existe un procedimiento que describa cómo se realiza la custodia de los soportes de información (discos, pendrives, portátiles, móviles? Ev: Documento que describa las condiciones de C/I/D para los soportes de información (incluido la retirada o destrucción, total o parcial, de la información del soporte). Registro de cada soporte con los activos de información asociados y el requisito de C/I/D asociado a cada uno.					
III.P03	¿Existe un procedimiento que describa el borrado y destrucción de los activos (hardware, equipos, información...)? Ev: Documento que describa cómo se realiza el borrado y/o la destrucción de los activos (móviles, routers, servidor, impresoras, discos duros, discos cifrables...).					
III. SP 1.2.	**Diseño procedimientos transversales**					
IV.P04	¿Está diseñado un proceso de configuración de activos de seguridad para proyectos de TI? Ev: Documento con el diseño del procedimiento para definir una BBDD con activos clasificados de acuerdo a instalaciones, equipos, software, infraestructura, comunicaciones, soportes informáticos, información, servicios y productos de seguridad TI.					
III.P05	¿Existe un proceso de gestión de incidencias de seguridad en proyectos de TI? Ev: Documento que describe el procedimiento para la gestión de las incidencias de seguridad, desde su catalogación hasta su resolución y cierre.					
III.P06	¿Existe un proceso de gestión de cambios en proyectos de TI? Ev: Documento que describe el procedimiento para la gestión de cambios que refleje su aprobación y activos afectados.					
FASE III. A2	**Implementación de la solución**					
FASE III. SP 2.1.	**Implementar la BBDD de Configuración**					
III.P07	¿Está implantado algún proceso de configuración de					

	activos de seguridad para proyectos de TI? Ev: Procedimiento de gestión de una BBDD con activos de seguridad clasificados de acuerdo a instalaciones, equipos, software, infraestructura, comunicaciones, soportes informáticos, información, servicios y productos de seguridad TI.					
III.P08	¿Existe un proceso de configuración de activos de seguridad para proyectos de TI? Ev: Registro de los puntos de conexión con el exterior y estructura de cortafuegos definidas (cascada, redundantes...).					
FASE III. SP 2.2.	**Implementar la BBDD de Activos de Seguridad (SAL)**					
III.P09	¿Existe una BBDD con las soluciones asociadas a diferentes problemas de seguridad en los servicios/proyectos de TI? Ev: BBDD con soluciones asociadas a cifrados de información, firmas digitales, certificados, claves y su gestión, funciones hash, MAC relativas a la integridad, sellos de tiempo, aplicaciones limpieza software, protección de email, ...					
FASE III. SP 2.3.	**Implementar los Activos de Seguridad**					
III.P10	¿Existe un programa de formación para adquisición de competencias de seguridad en proyectos de TI que permite a los usuarios conocer el buen uso de los servicios de TI? Ev: Registros de formación, documentos asociados a la adquisición de competencias por roles.					
III.P11	¿Existe un procedimiento de implantación de cada activo de seguridad? Ev: Documento que describe el proceso de implantación de cada servicio producto, pruebas de cumplimiento de requisitos de confidencialidad, de aseguramiento de la integridad, disponibilidad, trazabilidad, etc.					
FASE III. A3	**Diseño del procedimiento de monitorización de la solución**					
FASE III. SP 3.1.	**Diseñar el cuadro de mando de seguridad**					
III.P12	¿Existe un cuadro de mando que permita conocer la traza desde los requisitos a los indicadores de éxito del proceso implantado? Ev: Cuadro de mando de gestión de seguridad de proyectos TI.					
III.P13	¿Existe un documento con la definición de la monitorización del diseño de la solución que permita identificar las desviaciones sobre el plan previsto? Ev: Documento que describa los procedimientos de control aplicados para la monitorización de la seguridad de los proyectos/servicios TI (p.ej., controles de incidencias relacionadas con C/I/D, control de costes asociados a la seguridad y la NO seguridad, mejoras sugeridas como consecuencia del plan de mejora, controles de registro de actividad de usuarios y procesos).					
III.P14	¿Existe un documento con las métricas de seguridad aplicadas en los proyectos de TI? Ev: Documento que					

	describa los procedimientos de medición aplicados para la monitorización de la seguridad de los proyectos/servicios TI (p.ej., métricas de incidencias relacionadas con C/ID/, métricas de costes asociados a la seguridad y la NO seguridad, mejoras sugeridas como consecuencia del plan de mejora, métricas de registro de actividad de usuarios y procesos).					
FASE IV. A1	**Definición del procedimiento monitorización y recuperación**					
FASE IV. SP 1.1.	**Monitorización de activos**					
IV.P01	¿Existe un proceso definido e implantado para la monitorización de la seguridad en los proyectos de TI? Ev: Documento con el procedimiento definido para la monitorización de la seguridad de los activos de TI, siguiendo la traza.					
IV.P02	¿Se aplican soluciones para la recuperación de los umbrales definidos en el documento de seguridad y relativos a las incidencias de C/I/D? Ev: Registro de las acciones realizadas y encaminadas a la recuperación de los umbrales de C/I/D previamente establecidos en el Documento de Seguridad.					
FASE IV. SP 1.2.	**Monitorización de cambio y continuidad**					
IV.P03	¿Existe un procedimiento definido e implantado que permita ejecutar el plan de contingencia? Ev: Existe un plan de contingencia implantado y actualizado, y existen registros de resultados de simulaciones y recuperación del sistema					
IV.P04	¿Existe un procedimiento definido e implantado para la activación del servidor de respaldo? E: El servidor no averiado puede tomar el control de la aplicación, bien de forma manual o automática.					
IV.P05	¿Existe un procedimiento definido e implantado para la gestión periódica de las copias de seguridad? Ev: Registros de versiones con copias de seguridad periódicas que son verificadas periódicamente.					
IV.P06	¿Existe un procedimiento definido e implantado para la recuperación del servicio TI y se registra la información de recuperación junto con el responsable y el motivo? Se hace restore y existe un registro con la información del responsable y el motivo.					
IV.P07	¿Se monitorizan las cláusulas de los contratos con los proveedores para garantizar la continuidad de los productos y servicios que proveen? Ev: Los contratos con proveedores y subcontratistas incluyen una cláusula en relación a la continuidad de los productos y servicios que proveen.					
FASE IV. A2	**Revisión de los controles de seguridad**					
FASE IV. SP 2.1.	**Revisión de controles relativos a la política de seguridad**					
IV.P08	¿Se revisa el control relativo al cumplimiento de las cláusulas definidas en el documento de seguridad: responsabilidades, umbrales de proyecto/servicio de TI? Ev1: registro de accesos, logs, e informes relativos					

	a uso. Ev2: Existen usuarios nominales. Se realiza revisión periódica de usuarios. Se cumple la política de contraseñas.					
IV.P09	¿Se revisa el control de actualización de la política adaptándose a nuevas necesidades organizativas? Ev: Registro de cambios producidos en la descripción de la política y del documento de seguridad					
FASE IV. SP 2.2.	**Revisión de controles relativos a los requisitos financieros de seguridad**					
IV.P10	¿Se revisa el control con la información referente al coste y/o beneficios económicos (ROI) de los recursos empleados en seguridad de los proyectos de TI? Ev: Registro beneficio por disminución del número de incidencias, tiempo de resolución de incidencias y recuperación del estado del servicio/proyecto.					
IV.P11	¿Se evalúan los daños producidos, sobre los procesos de negocio, por incidencias relacionadas con el no cumplimiento de los requisitos de seguridad? Ev: Registro de pérdida producida por una incidencia de seguridad (C/I/D) con información de los departamentos afectados.					
IV.P12	¿Se revisa el control con la información relativa a los costes de las incidencias de seguridad en los proyectos de TI? Ev: Documento con informe de coste de incidencias de C/I/D.					
FASE IV. SP 2.3.	**Revisión de controles relativos a la gestión de la seguridad**					
IV.P13	¿Se revisa el control con la información relativa a los costes de las incidencias de seguridad en los proyectos de TI? Ev: Documento con informe de coste de incidencias de C/I/D. Prioridad alta.					
IV.P14	¿Existe un procedimiento definido para la emisión de informes de seguimiento periódico del estado de los factores y de sus umbrales? EV: Existen documentos y registros resultados de auditoría o seguimiento de las cláusulas de seguridad definidas en el Documento de Seguridad. (Períodos de revisión, tiempos de implantación, tiempos de recuperación, plan de continuidad, etc.).					
IV.P15	¿Existe un procedimiento definido e implantado para la gestión de cambios de la configuración? EV: Registro de cambios de configuración, historiales, actualizaciones, copias de recuperación, etc.					
IV.P16	¿Se definen los controles asociados a las incidencias de C/I/D asociadas a cada activo y vulnerabilidad? EV: Existe registros de incidencias asociadas a los activos y clasificadas por tipo de principio que se ha vulnerado (C/I/D), vulnerabilidad del activo y coste asociado.					
FASE IV. A3	**Emisión de informes**					
FASE IV. SP 3.1.	**Emisión de informes de proceso**					
IV.P17	¿Existen informes de cambios de configuración motivados por requisitos o soluciones de seguridad?					

	EV: Documento con los informes relativos a los cambios producidos.					
IV.P18	¿Existe un procedimiento definido para la emisión de informes de seguimiento periódico del estado de los factores y de sus umbrales? EV: Existen documentos y registros resultados de auditoría o seguimiento de las cláusulas de seguridad definidas en el Documento de Seguridad.					
IV.P19	¿Se realiza un seguimiento de las tendencias (nuevas o resultado de monitorización) relativas a las necesidades de seguridad para los activos? EV: Registro de nuevas amenazas y vulnerabilidades.					
FASE V. A1	**Definición del plan de mejora**					
FASE V. SP 1.1.	**Revisión de estado seguro y resultados de monitorización**					
V.P01	¿Se realizan informes relativos a los resultados de revisión y auditoría? EV: Informes y actas de reunión de revisión de resultados de auditoría.					
V.P02	¿Se realizan informes relativos a los resultados de revisión y auditoría? EV: Informes y actas de reunión de revisión de resultados de auditoría.					
V.P03	¿Se realizan informes periódicamente sobre las necesidades de seguridad (C/I/D) de cada departamento o proveedor? EV: Documento con el acta de reuniones internas y/o de proveedores, con la revisión de las nuevas necesidades de C/I/D.					
V.P04	¿Proporciona el CIO información sobre los resultados de la evaluación del estado de la seguridad en sus proyectos de TI? EV: Documento, amoldado a cada rol, con los resultados de éxito/fracaso de los proyectos de seguridad implementados.					
FASE V. SP 1.2	**Comunicación de resultados de revisión**					
V.P05	¿Existe un procedimiento implantado para la comunicación de resultados de la revisión del estado de seguridad del proyecto/servicio? EV: Actas de reuniones, sitios web,...a los que se tenga acceso y se compruebe que se han entendido los resultados.					
V.P06	¿Existe un procedimiento que facilita la redacción de los resultados del estado de seguridad del proyecto/servicio, y acorde a cada rol y a cada responsabilidad definida en el documento de seguridad? EV: Se han definido las competencias y objetivos de seguridad para cada rol y responsable, y existe					
FASE V. A2	**Implantar y comunicar plan de mejora**					
FASE V. SP 2.1.	**Planificación del proceso de mejora**					
V.P07	¿Existe un plan de mejora continua para la gestión de seguridad en los proyectos de TI? EV: Documento que refleje en base a registros de monitorización e informes de auditoría y requisitos de seguridad, un plan de mejora de seguridad continua.					
V.P08	¿Se incluyen herramientas y técnicas más adecuadas					

	para la gestión de la seguridad en los proyectos de TI que se abordan? EV: Registro de nuevas herramientas y técnicas asociadas a soluciones y mejoras.					
V.P09	¿Existen registros de nuevas metas y objetivos para la seguridad de los proyectos/servicios de TI? EV: Documento que refleje en base a registros de monitorización e informes de auditoría, y requisitos de seguridad, los nuevos objetivos a cumplir en el plan de mejora.					
FASE V. SP 2.2.	**Gestión de decisiones de mejora**					
V.P10	¿Se utilizan los registros de monitorización de seguridad para la toma de decisiones en los proyectos de TI? EV: Registro de monitorización de los requisitos de seguridad definidos en el documento de seguridad vinculados con nuevas soluciones de mejora.					
V.P11	¿Se emplea la información de la monitorización para la implantación del plan de mejora de la seguridad de los activos (revisión de política, definición de nuevos requisitos, diseño e implantación de nuevas soluciones)? EV 1: Registros de monitorización asociados a cambios de políticas, requisitos, diseños e implantación de soluciones. EV 2: Los cambios de versión se hacen de manera controlada.					
V.P12	¿Se intercambia información con la gestión financiera de TI sobre el ROI del proceso y los ingresos totales, desglosados por área de negocio? EV: Registro de mejoras esperadas asociadas a costes de incidencias, ROI de soluciones.					
V.P13	¿Se intercambia información con gestión financiera, sobre la información pertinente a los costes de la seguridad y la NO seguridad de los servicios? EV: Registro de mejoras esperadas de asociadas a la estimación de coste de NO seguridad.					
V.P14	¿Se intercambia información con la gestión de la capacidad para prever y establecer los requisitos de nivel de disponibilidad? EV: Registro de mejoras esperadas asociadas a las nuevas capacidades de proceso y recuperación necesarias para asegurar disponibilidad definida en acuerdos, contratos y documento de seguridad.					
V.P15	¿Se intercambia información con la gestión del cambio con el fin de gestionar requisitos de seguridad asociados a cada cambio (control de versiones, parches, etc.)? EV 1: Registro con la descripción de los requisitos de seguridad del cambio aprobados por comité de cambio y responsable de seguridad, y las mejoras esperadas. EV 2: Existe un entorno separado de cambios y se sigue el procedimiento de gestión de cambios.					
V.P16	¿Se intercambia información con la gestión de la configuración relativa a la integridad y confidencialidad de la información de los elementos					

	adquiridos? EV: Registros con la información de las actualizaciones de los activos y sus relaciones.					
V.P17	¿Se intercambia información con la gestión de la configuración para monitorizar los requisitos de seguridad establecidos para cada elemento adquirido o desarrollado? EV: Registro de monitorización de los requisitos de seguridad definidos en el documento de seguridad.					
FASE V. SP 2.3.	**Comunicación de resultados de decisión**					
V.P18	¿Existe un procedimiento implantado para la comunicación de resultados de las decisiones de mejora? EV: Documento con las decisiones de mejora firmadas y comprometidas.					
V.P19	¿Existe un procedimiento que facilita la comunicación de las decisiones de seguridad del proyecto/servicio y acorde a cada rol y a cada responsabilidad definida en el documento de seguridad? EV: Se han definido las competencias y objetivos de seguridad para cada rol y responsable, y existe un registro de comunicación y aceptación.					

Anexo II. Resultados de validación inicial y final

II.I Cuestionario inicial Laboratorio de IICC

FASE I	Cuestionarios				Siempre	Usual mente	A veces	Rara vez	Nunca			
	RP1	RP2	RP3	RP4	#S	#U	#A	#R	#N	Cq	Medq	Devq
FASE I. A1												
FASE I. SP 1. 1												
I.P01	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P02	A	R	R	R	0	0	1	3	0	31%	1,25	0,4
					0%	0%	25%	75%	0%			
I.P03	S	U	S	U	2	2	0	0	0	88%	3,50	0,50
					50%	50%	0%	0%	0%			
I.P04	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P05	U	U	A	U	0	3	1	0	0			
					0%	75%	25%	0%	0%	69%	2,75	0,43
I.P06	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P07	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P08	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P09	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P10	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P11	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P12	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P13	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P14	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			
I.P15	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P16	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P17	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P18	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
FASE II												
II.P01	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			

II.P02	**R**	**N**	**R**	**R**	**0**	**0**	**0**	**3**	**1**	**19%**	**0,60**	**0,624**
					0%	**0%**	**0%**	**75%**	**25%**			
II.P03	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
II.P04	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
II.P05	**S**	**S**	**U**	**U**	**2**	**2**	**0**	**0**	**0**	**88%**	**3,50**	**0,50**
					50%	**50%**	**0%**	**0%**	**0%**			
II.P06	**A**	**A**	**A**	**A**	**0**	**0**	**4**	**0**	**0**	**50%**	**2,00**	**0,0**
					0%	**0%**	**100%**	**0%**	**0%**			
II.P07	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
II.P08	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
II.P09	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
II.P10	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
II.P11	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
II.P12	**A**	**A**	**A**	**A**	**0**	**0**	**4**	**0**	**0**	**50%**	**2,00**	**0,0**
					0%	**0%**	**100%**	**0%**	**0%**			
II.P13	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
II.P14	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
II.P15	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
II.P16	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
II.P17	**A**	**A**	**A**	**A**	**0**	**0**	**4**	**0**	**0**	**50%**	**2,00**	**0,0**
					0%	**0%**	**100%**	**0%**	**0%**			
II.P18	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
FASE III												
III.P01	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
III.P02	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
III.P03	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P04	**A**	**A**	**A**	**A**	**0**	**0**	**4**	**0**	**0**	**50%**	**2,00**	**0,0**
					0%	**0%**	**100%**	**0%**	**0%**			
III.P05	**R**	**R**	**R**	**R**	**0**	**0**	**0**	**4**	**0**	**25%**	**1,00**	**0,0**
					0%	**0%**	**0%**	**100%**	**0**			
III.P06	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
III.P07	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
III.P08	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
III.P09	**A**	**A**	**A**	**A**	**0**	**0**	**4**	**0**	**0**	**50%**	**2,00**	**0,0**
					0%	**0%**	**100%**	**0%**	**0%**			

III.P10	**U**	**U**	**U**	**U**	**0**	**4**	**0**	**0**	**0**	**75%**	**3,00**	**0,0**
					0%	**100%**	**0%**	**0%**	**0%**			
III.P11	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
III.P12	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
III.P13	**R**	**N**	**N**	**N**	**0**	**0**	**0**	**1**	**3**	**6%**	**0,25**	**0,433**
					0%	**0%**	**0%**	**25%**	**75%**			
III.P14	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
FASE IV												
IV.P01	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P02	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P03	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P04	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
IV.P05	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
IV.P06	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
IV.P07	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P08	**A**	**A**	**A**	**A**	**0**	**0**	**4**	**0**	**0**	**50%**	**2,00**	**0,0**
					0%	**0%**	**100%**	**0%**	**0%**			
IV.P09	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P10	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P11	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P12	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P13	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P14	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P15	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
IV.P16	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P17	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P18	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P19	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
FASE V												
V.P01	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P02	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**

					0%	0%	0%	0%	100%			
V.P03	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P04	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			
V.P05	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P06	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P07	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P08	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P09	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P10	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P11	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P12	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P13	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P14	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P15	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P16	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P17	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P18	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
V.P19	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			

II.II Cuestionario final Laboratorio de IICC

FASE I	Cuestionarios				Siempre	Usualmente	A veces	Rara vez	Nunca			
	RP1	RP2	RP3	RP4	#S	#U	#A	#R	#N	Cq	Medq	Devq
FASE I. A1												
FASE I. SP 1. 1												
I.P01	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P02	A	R	R	R	0	0	1	3	0	31%	1,25	0,4
					0%	0%	25%	75%	0%			
I.P03	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P04	N	N	N	N	0	0	0	0	4	0%	0,00	0,0

					0%	0%	0%	0%	100%			
I.P05	U	U	A	U	0	3	1	0	0	69%	2,75	0,43
					0%	75%	25%	0%	0%			
I.P06	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			
I.P07	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P08	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P09	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P10	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P11	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P12	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P13	S	S	U	U	2	2	0	0	0	88%	3,50	0,50
					50%	50%	0%	0%	0%			
I.P14	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P15	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
I.P16	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P17	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
I.P18	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
FASE II												
II.P01	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			
II.P02	R	N	R	R	0	0	0	3	1	19%	0,60	0,624
					0%	0%	0%	75%	25%			
II.P03	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
II.P04	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
II.P05	S	S	U	U	2	2	0	0	0	88%	3,50	0,50
					50%	50%	0%	0%	0%			
II.P06	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			
II.P07	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
II.P08	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
II.P09	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
II.P10	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
II.P11	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
II.P12	A	A	A	A	0	0	4	0	0	50%	2,00	0,0

					0%	0%	100%	0%	0%			
II.P13	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
II.P14	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
II.P15	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			
II.P16	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
II.P17	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			
II.P18	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
FASE III												
III.P01	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
III.P02	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
III.P03	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
IV.P04	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			
III.P05	R	R	R	R	0	0	0	4	0	25%	1,00	0,0
					0%	0%	0%	100%	0			
III.P06	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
III.P07	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
III.P08	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
III.P09	A	A	A	A	0	0	4	0	0	50%	2,00	0,0
					0%	0%	100%	0%	0%			
III.P10	U	U	U	U	0	4	0	0	0	75%	3,00	0,0
					0%	100%	0%	0%	0%			
III.P11	R	R	R	R	0	0	0	4	0	25%	1,00	0,0
					0%	0%	0%	100%	0			
III.P12	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
III.P13	R	N	N	N	0	0	0	1	3	6%	0,25	0,433
					0%	0%	0%	25%	75%			
III.P14	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
FASE IV												
IV.P01	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
IV.P02	R	R	R	R	0	0	0	4	0	25%	1,00	0,0
					0%	0%	0%	100%	0			
IV.P03	N	N	N	N	0	0	0	0	4	0%	0,00	0,0
					0%	0%	0%	0%	100%			
IV.P04	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			
IV.P05	S	S	S	S	4	0	0	0	0	100%	4,00	0,0
					100%	0%	0%	0%	0%			

IV.P06	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
IV.P07	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P08	**A**	**A**	**A**	**A**	**0**	**0**	**4**	**0**	**0**	**50%**	**2,00**	**0,0**
					0%	**0%**	**100%**	**0%**	**0%**			
IV.P09	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P10	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P11	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P12	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P13	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P14	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P15	**S**	**S**	**S**	**S**	**4**	**0**	**0**	**0**	**0**	**100%**	**4,00**	**0,0**
					100%	**0%**	**0%**	**0%**	**0%**			
IV.P16	**R**	**R**	**R**	**R**	**0**	**0**	**0**	**4**	**0**	**25%**	**1,00**	**0,0**
					0%	**0%**	**0%**	**100%**	**0**			
IV.P17	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P18	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
IV.P19	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
FASE V												
V.P01	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P02	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P03	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P04	**A**	**A**	**A**	**A**	**0**	**0**	**4**	**0**	**0**	**50%**	**2,00**	**0,0**
					0%	**0%**	**100%**	**0%**	**0%**			
V.P05	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P06	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P07	**R**	**R**	**R**	**R**	**0**	**0**	**0**	**4**	**0**	**25%**	**1,00**	**0,0**
					0%	**0%**	**0%**	**100%**	**0**			
V.P08	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P09	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P10	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P11	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P12	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			

V.P13	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P14	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P15	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P16	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P17	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P18	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			
V.P19	**N**	**N**	**N**	**N**	**0**	**0**	**0**	**0**	**4**	**0%**	**0,00**	**0,0**
					0%	**0%**	**0%**	**0%**	**100%**			

Anexo III. POLITICA DE SEGURIDAD

Referencia: ISO 27001:2013, 4.2.1 a-b)1,2,3-5 y 5.1.1
Elaborado : Responsable de Proyecto 1
Revisado : Responsable de Proyecto 2
Aprobado : Director
Versión: 2016-01

Nota: La versión válida y vigente en cada momento de este documento es la que está disponible en el sistema de gestión de recursos organizativos del LABORATORIO. En caso de versiones impresas asegúrese de que concuerda con la vigente antes de trabajar con ella.

El LABORATORIO es una entidad adscrita a la corporación X, cuya misión es aportar valor e innovación a sus usuarios y a la sociedad en general, a través del desarrollo de proyectos y servicios en el ámbito de los SCI.

Para que dichos servicios se presten con la debida eficacia, la Dirección del LABORATORIO está comprometida con el desarrollo de una gestión del mismo basada en un cumplimiento estricto de cualquier requisito legal que le afecte, y en la implantación de manera alineada con la estrategia, de una serie de sistemas de gestión basados en modelos de referencia internacional, que aseguran la buena praxis corporativa.

Uno de ellos es el SGSI, SlSTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, entendiendo como tal concepto el conjunto de medidas técnicas y organizativas que se integran en el marco de gestión común adoptado -Norma ISO/IEC 27001:2013, con objeto de analizar y tratar periódicamente los riesgos asociados a la seguridad.

Los objetivos en la materia se revisan periódicamente, fijándose en términos de alineamiento con la estrategia, búsqueda de la excelencia, garantía en la prestación de servicios, aportación de valor para los clientes y optimización de costes.

El alcance de la presente política comprende a todo el personal, sistemas informáticos y activos incluidos en los siguientes servicios del LABORATORIO:

- Servicios de análisis e investigación.
- Servicios de control industrial.
- Servicios organizativos, incluyendo la gestión de las áreas de Sistemas, Personal, Logística y Económico Financiera.

La prestación de estos servicios se realiza desde dos ubicaciones físicas incluidas en el alcance:

- Sede antigua localizada en XX.

- Nueva sede ubicada en YY.

Mediante el presente documento, la Dirección del LABORATORIO se compromete a velar por el mantenimiento y mejora constante del SGSI implantado, aportando para ello los recursos necesarios, compromiso que se hace extensivo a todos los usuarios, mediante el esfuerzo por mantener óptimos niveles reconocidos de seguridad y calidad. Los roles implicados directamente en este compromiso son los siguientes:

- Comité de Dirección.
- Comisión de Seguridad de la Información.
- Responsables y Usuarios de Activos.
- Auditores Internos.

Este documento se publica a la vista de todos los usuarios y existe una versión actualizada, a disposición de todos los miembros del LABORATORIO. Además, este documento no contiene información confidencial. Por lo tanto, puede ser puesto a disposición de terceras partes externas relevantes.

Anexo IV. Manual de Seguridad

Título : Manual de Seguridad		
Elaborado/modificado: Responsable de Proyecto 1		**Firma:**
Revisado : Responsable de Proyecto 2		**Firma:**
Aprobado : Director		**Firma**
Versión: 2016-01	**Revisión: 0**	**Fecha: 06/06/2016**

1. Introducción y objetivos del manual

La Dirección del LABORATORIO IICC, a través de la política de seguridad publicada en el documento ANEXO III Política de Seguridad, se ha comprometido a preservar la seguridad de la información (en adelante, SI) a través de sus tres parámetros de activos confidenciales, integros y disponibles, para todos los activos de información, física y electrónica, utilizados en todo el Lifecycle de los servicios/proyectos definidos dentro del Sist. de Gestión de Servicios de Tecnologías de la Información (SGSTI) con el fin de preservar su misión y objetivos organizativos.

2. Alcance

Este documento forma parte del compromiso de la dirección por establecer los mecanismos necesarios para garantizar la gestión de la SI en el SGSTI y por lo tanto, en los proyectos/servicios de TI que aborda el LABORATORIO.

Afecta a los usuarios con acceso al LABORATORIO y a los recursos protegidos (información, procesos, funciones, ficheros, procedimientos de administración de incidencias, backup de datos, así como a las medidas definidas para el transporte y manipulación de los soportes de información). Además, está alineada con las normas y estándares tales como LOPD, ISO 27001 e ISO/IEC 20000, así como la normativa aplicable en Seguridad TI en entornos de control industrial y de infraestructuras críticas.

El no cumplimiento de lo prescrito en este Manual permitirá encausar responsabilidades personales, eventualmente sancionables conforme la normativa establezca.

3. Beneficios

La aplicación de este documento beneficiará a todos los usuarios del Laboratorio, ya que se trabajará sobre la base de la confianza y disponibilidad de los procesos y la integridad de la información.

Estos beneficios pueden medirse de acuerdo a:

Beneficio	Medida
1. Máximo compromiso de todas las partes implicadas en la empresa con la seguridad de los servicios/proyectos de TI.	- Nº de cláusulas de confidencialidad incluidas en acuerdos y contratos con terceros. - Nº de cláusulas de disponibilidad en niveles de servicio/ total de acuerdos y contratos con terceros. - Presupuesto asignado a proyectos/servicios de seguridad de TI/ presupuesto de proyectos/servicios de TI.
2. Disminución de las incidencias relativas a los requisitos de seguridad establecidos tanto por las leyes como por las regulaciones de obligado cumplimiento establecidas por el LABORATORIO	-Nº de Incidencias de Seguridad/Nº Total de Incidencias TI detectadas.
3. El aumento del rendimiento en la gestión de los servicios/proyectos de TI.	- Disminución del tiempo medio de resolución de una incidencia de seguridad en el puesto de trabajo. - Disminución del tiempo medio de NO disponibilidad de aplicaciones y servicios en puesto de trabajo. - Disminución del Nº de accesos no permitidos/ Nº de accesos total.
4. Una mayor formación y concienciación de los usuarios implicadas en proyectos de tecnologías de información acerca de SI.	- Incremento del Nº participantes en actividades de formación y concienciación en ciberseguridad. - Incremento de la calificación obtenida por los asistentes a los programas de formación y concienciación en ciberseguridad.

4. Roles

La dirección del LABORATORIO ha definido las autoridades y responsabilidades en el SGSTI en dos tipos de rol:

- Rol básico, presente en cualquier tipo de organización.
- Rol de soporte, donde los roles básicos pueden delegar alguna de sus responsabilidades.

Todos los documentos generados por cada rol llevan la firma del responsable.

Roles	Tipo	Responsabilidad	Nombre/ Apellidos
Director	Básico	Máximo responsable de la dirección del LABORATORIO	
Responsable de proyecto	Básico	Persona representante de procesos del LABORATORIO responsable de las relaciones entre procesos/proyectos y TI	
Responsable TI	Básico	Persona con perfil informático, responsable de: - Las definiciones propias de la SI en la organización y de que estas	

		definiciones estén integradas con otras políticas de SI. - Información e infraestructura, - Solicitudes de revisiones y/o auditorías de seguridad en la organización. - Verificar que los controles de seguridad aplicados están orientados al cumplimiento de los requerimientos de SI del conjunto del Project Lifecycle. -Gestión de la SI del LABORATORIO -Administración de incidencias y continuidad de negocio.	

5. Usuarios de servicios TI

Los usuarios de activos y servicios TI se comprometen a respetar la confidencialidad de la información y de uso correcto de los recursos TI del LABORATORIO, así como el estricto cumplimiento del Manual de SI.

Todo usuario interno de nuevo ingreso (Analista, Técnico, Personal en formación o personal de soporte) deberá conocer el Manual de Políticas de SI del LABORATORIO, accesible en el portal web del LABORATORIO (hhtps://LABORATORIO.com) y que refleja las prácticas de necesario cumplimiento así como las acciones correctoras a aplicar en caso contrario.

Toda identificación de un incumplimiento del Manual de SI se registrará como una incidencia de "Incumplimiento en política de seguridad", observaciones y evidencias, para los efectos y acciones oportunas.

6. Seguridad física y del uso del entorno del LABORATORIO

Los procedimientos de control de accesos para los usuarios y terceras personas ajenas al Laboratorio facilitar el acceso físico a las dependencias y zonas de tipo restringido del LABORATORIO exclusivamente para personas con autorización.

El usuario deberá informar al Responsable TI, y en su ausencia al Director u otro Responsable de Proyecto, con una incidencia, de modo inmediato, en el mismo momento de la detección de posibles riesgos para los recursos de TI o comunicaciones tales como inundaciones o incendios u otros similares. Tampoco se deberán prácticas antihigiénicas que puedan dañar los equipamientos tales como tomar alimentos, ingenir líquidos que no estén en botellas de plástico cerradas en todo momento, ensuciar o taponar los conductos de ventilación de los equipos.

El usuario protegerá los dispositivos de almacenamiento de datos, independientemente del tipo, su utilización o no, o el carácter de los datos que puedan contener. Asimismo sólo podrá almacenar su información en los directorios facilitados y en ningún caso otros tales como los destinados a aplicaciones y sistemas operativos.

El usuario no realizará ni consentirá la fuga de datos sobre los que acceda y maneje contenidos desde su puesto de operaciones, respetando la información reservada y

confidencial ya sea en las redes internas y hacia el exterior, o pertenezca a terceras entidades.

Los usuarios del LABORATORIO deben respetar las buenas prácticas en materia de prevención de malware o spyware establecidas por el LABORATORIO:

a. Escaneado obligatorio por antivirus de cualquier dispositivo externo del Laboratorio antes de utilizarlo.
b. Análisis preventivo con antivirus de archivos adjuntos al email, incluyendo archivos comprimidos antes de su apertura.
   Prohibición de envío de predeterminados tipos de archivos por email.
   Restricciones de acceso para usuarios y determinación por el Responsable TI de los privilegios de administrador, en su caso.
c. Respeto por parte de cada usuario de la realización de actualizaciones automáticas y parches en el sistema operativo.
d. Utilización obligatoria del software antivirus, detección de spyware y utilidades de eliminación proporcionado por el Responsable de TI.
e. Restricción en el uso de dispositivos personales como móviles y tablets, previa autorización del Responsable de TI.
f. Consejos de navegación web segura entre los usuarios incluyendo la no apertura de ventanas emergentes sospechosas.
g. Prohibición de apertura de ficheros con extensiones .bat, .com, .exe, .pif, .vbs.
h. Consejos de custodia segura de contraseñas, claves personales y códigos de acceso en respuesta a emails o formularios web.

7. Entornos de desarrollo de servicio/proyecto

El desarrollo de los servicios/proyectos TI se debe considerar en todo su ciclo de vida. Por ello se consideran los servicios y las infraestructuras que los soportan en tres entornos diferentes: desarrollo, testeo y producción.

1. **Entorno de desarrollo**. El entorno de desarrollo se refiere al entorno en el que se desarrolla el software del proyecto/servicio. El responsable de mantener el buen entorno de desarrollo es el propietario del servicio/proyecto.
2. **Entorno de testeo**. El responsable de mantener el buen entorno de desarrollo es el Responsable de proyecto como gestor de seguridad, y si es posible junto con gestor de pruebas y verificación del servicio/proyecto.
3. **Separación de roles de entorno de desarrollo y de testeo**. Si es posible, el personal del desarrollo no debe gestionar el entorno de testeo.
4. **Responsable del entorno de operación**. El área de producción es el área operativa, en LA que el software desarrollado en el proyecto hace su función en la organización. El responsable de la gestión segura en este entorno es el Responsable del servicio/proyecto. El personal de desarrollo no debe gestionar el entorno de producción. En ningún caso se deben realizar pruebas en el entorno de producción.

Como referencia general de seguridad en la metodología de Ciclo de Vida del Desarrollo SW (SDLC), se recurrirá a la guía NIST 800-64.

8. Control de accesos

Cada acceso depende del perfil de cada usuario que se autentica. Corresponde al Responsable TI mantener el Registro de permisos de acceso a los usuarios del LABORATORIO.

Los protocolos de acceso a las listas de revocación serán del tipo HTTP u OCSP.

9. Control de cifrado

Para la protección de la información frente a posibles fallos de confidencialidad e integridad se utilizan sistemas y técnicas criptográficas que permiten la generación de claves para el cifrado de la información y la generación de números que facilitan verificar distintos aspectos de su integridad.

El LABORATORIO dispone de un procedimiento de gestión de claves que conlleva las siguientes tareas:

1. Diferenciar entre claves de sesión / intercambio de la firma digital.
2. Mantener la integridad de todas las claves secretas. Todas las claves son protegidas y cifradas evitando modificaciones o destrucción no deseada.
3. Generar y proteger el archivo de claves. Se proporciona una protección de cifrado a los equipos utilizados para crear y almacenar claves, catalogados como críticos o de alto riesgo.
4. Establecer período de validez de claves. Se someterán a un sistema de caducidad en plazos no superiores a 12 meses.
5. Protección de claves públicas. Se administrará sobre la base de certifiados de clave pública de confianza, mediante Autoridad de Certificación.

10. Seguridad de los archivos del SGSTI

Administrarlos archivos de forma segura resulta esencial para garantizar que el Project Lifecycle se desarrolla de modo seguro, principalmente mediante el control de accesos, para lo cual se establecen los procedimientos siguientes:

1. Control de acceso a archivos en el equipo o sistemas a los que accede un usuario, de modo que las aplicaciones no puedan acceder a aquellos de los que no sean propietarias, independientemente si se alojan en un servidor de aplicaciones o en el equipo/puesto del usuario.
2. Control del sw operativo. Cualquier aplicación que desarrolle el LABORATORIO o un tercero para éste, tendrá asignado un usuario que asumirá la responsabilidad informática por designación del Responsable del servicio/proyecto.
3. Protección de los datos en el entorno de protección, prohibiéndose el desarrollo de pruebas en el mismo, que se realizarán exclusivamente en el entorno de *testing*.
4. Control de cambios realizados a datos en entorno de producción. El procedimiento previene de modificaciones desreguladas sobre datos almacenados, archivos o bases de datos, que puedan arriesgar la integridad de la información. El procedimiento de control de cambios depende del Responsable de Proyecto.

5. Control de acceso a librerías de código fuente y ficheros de configuración. El procedimiento de control de cambios depende del Responsable de Proyecto y tiene aplicación al Equipo de Desarrollo del LABORATORIO.

11. Seguridad en las comunicaciones

El LABORATORIO IICC está enfocado en un entorno de seguridad industrial, por lo que constituyen sus metas principales preservar un adecuado aislamiento de las redes de datos que soportan los sistemas y procesos de control respecto al conjunto de red del Laboratorio.

12. Seguridad de los procesos de soporte y desarrollo

Estos procesos están fundamentados en la definición de requerimientos y condiciones de SI contemplando tres procedimientos:

1. *Control de Cambios*

- Verificación de que los solicitan usuarios autorizados.
- Registro de perfiles/niveles de autorización.
- Identificación de elementos de software, bases de datos, hardware que requieren modificación.
- Revisión de controles de datos que aseguren la integridad de los mismos por el cambio.
- Requerimiento de aprobación formal previa por parte del Responsable del Proyecto.
- Ejecución de cambios en entorno de desarrollo.
- Aprobación del usuario autorizado y del área de verificación mediante pruebas.
- Actualización de la documentación sobre los cambios en los manuales de usuario.
- Mantenimiento de un control de versiones para cada actualización SW.
- Información a usuarios.
- El Responsable de Proyecto en el equipo de Desarrollo aprueba el pase de los cambios a producción.

2. *Revisión de los cambios a nivel de SO Sistema Operativo*. La revisión en los cambios del sistema operativo debe aplicarse incluso en los cambios de versión:

- Revisar la integridad y los controles definidos para las aplicaciones garantizando que no se han comprometido por el cambio producido.
- Informar, con anterioridad a la implementación del cambio, a las partes implicadas.
- Asegurar que el Plan de Continuidad en la organización está actualizado.

3. *Revisión de los Canales Ocultos y Código Malicioso.*

- El procedimiento prevé la adquisición a proveedores de confianza y de productos testados, excepto en casos en el que el Equipo de Desarrollo actúe en coordinación con el Equipo de Investigación, con propósitos experimentales y de investigación, pruebas, etc, en cuyo caso el Responsable de Proyecto se asegurará de preservar el entorno de Desarrollo aislado del entorno de Pruebas. También se prevé el examen de requerimientos de SI de códigos fuente en aplicaciones externas al laboratorio si son de código abierto o accesible.
- Control de acceso y detección las alteraciones en el código instalado.
- Implantación de antivirus.

13. Auditoría y trazabilidad

Existe un procedimiento de registro de auditorías, accesos y controles a nivel central, mediante una aplicación específica SW que depende del Responsable TI, incluyendo como tareas las siguientes:

- Registro de métricas de uso de cada aplicación y el usuario
- Registro de trazas y tiempos de las aplicaciones y su funcionamiento.
- Registro del procedimiento y auditorías de administración de claves

14. Verificación de los requisitos de seguridad

Se prevé un procedimiento de verificación de los requerimientos de seguridad aplicables en los siguientes elementos:

1. En el código a nivel de desarrollo de programación durante y ex post.
2. En la caja negra de los componentes de aplicación
3. En las aplicaciones de modo general y particular.
4. En las aplicaciones en el entorno de producción.

1. *Verificación de la seguridad en el desarrollo de un componente*. Antes de que un componente se pase a producción, se verifica la seguridad del código. Es el propio desarrollador quien realiza este tipo de verificación. El procedimiento conlleva la aplicación de herramientas de verificación automática de código, y un registro documentado de verificaciones.

2. *Diseño de la seguridad de un elemento en producción*. Se prevén pruebas de verificación de la SI y las interacciones en un entorno de pruebas. En función del carácter crítico o no del elemento, el diseño de pruebas dependerá del desarrollador, o del Responsable de Proyecto.

3. *Verificación de la SI de la aplicación en producción*. Se prevén pruebas de verificación de la SI y las interacciones en un entorno de producción.

4. *Verificación de la seguridad de aplicaciones*. Debido a la interacción de los sistemas de aplicaciones se evaluan los requerimientos de seguridad en la interacción entre ellas y se diseñan pruebas de verificación que permitan garantizar el orden de ejecución, la

terminación automática en caso de fallo y la interrupción de proceso hasta la resolución del problema.

5. *Verificación del estado de la aplicación en producción*. Cuando un elemento o aplicación se encuentren en producción, se faciltan controles adecuados y verificados para los correspondientes requerimientos de SI, y se gestionan los incidentes de SI.

15. Seguridad en el diseño, desarrollo e implementación del software asociado al servicio/proyecto

Cada Responsable de proyecto tiene la obligación de conocer este manual completo y sus anexos. Las normas básicas en la administración de datos requieren la observación de buenas prácticas y respeto a los procedimientos de:

1. Validación de los datos de entrada.
2. Validación del procesamiento interno.
3. Autenticación de mensajes transferidos entre sistemas
4. Validación de los datos de salida.

Es obligatoria la utilización de modelos normativos de desarrollo seguro, atendiendo a los estándares identificados más comúnmente aceptados como C, C++, C#; C, y entornos de desarrollo y librerías como Visual C/C++.

Se aplica un procedimiento de prevención de fallos en la fase de diseño que incluye controles de validación de datos ex ante.

Se aplica un procedimiento de autenticación y cifrado de mensajes con información de tipo clasificado. El Responsable de Proyecto implementará controles criptográficos al efecto y validará el envío de datos.

Anexo V. Organigrama del Laboratorio IICC

Título : Organigrama del Laboratorio IICC		
Elaborado/modificado: Responsable de Proyecto 1		**Firma:**
Revisado : Responsable de Proyecto 2		**Firma:**
Aprobado : Director		**Firma**
Versión: 2016-01	**Revisión: 0**	**Fecha: 06/06/2016**

1. Organización

En esta apartado se definen: Responsabilidades, competencias y relaciones de la estructura organizativa del LABORATORIO.

2. Director

Es el responsable de impulsar, dirigir, coordinar y tomar decisiones sobre las actividades del LABORATORIO en sus distintas áreas.

- Analiza los resultados obtenidos por las distintas áreas y realiza las propuestas de mejora en todas ellas.
- Capacidad para firmar todos los documentos necesarios.
- Realiza el estudio de oportunidades de desarrollo para el LABORATORIO y análisis del entorno.
- Representación ante la dirección de la Corporación y los Servicios de Gestión (Personal, Administración General, Económico-Financiero y otros).

3. Responsables de proyecto

- Su misión es procesar todas las acciones relativas a servicios y Project management en el LABORATORIO. Sus actividades principales son:
    - Apoyo técnico a la Dirección para la definición de proyectos, actividades del Laboratorio.
    - Apoyo técnico a la Dirección para el liderazgo y coordinación de proyectos.

- Ejercer la supervisión directa del personal de los departamentos de análisis/investigación, desarrollo y del personal en formación.

4. Responsable TI

Es el responsable de seguridad TI, incluyendo los procedimientos de planificación, definición, operación, revisión, seguimiento y mantenimiento, siendo también de su responsabilidad las revisiones de estos planes, analizando las disconformidades y proponiendo las acciones correctivas y preventivas, si hubiera lugar, para el conjunto del Sistema de Gestión de Seguridad de las TI (SGSTI). Establece y comunica el alcance del SGSTI, la política y objetivos de la gestión del servicio.

Es responsable de gestionar las operaciones y actividades TI relacionadas con la parte productiva del LABORATORIO, y en concreto:

- Elabora y supervisa el sistema documental de Seguridad y Calidad del LABORATORIO.
- Planifica la Seguridad y Calidad, listas de verificación, hojas de control de proceso actuando como secretario de la Comisión de Seguridad.
- Realiza el seguimiento del *compliance* normativo del LABORATORIO elevando informes a la Dirección a efectos de revisión por esta, custodiando la documentación de archivo de calidad y SI.
- Control de documentación de Equipos de Inspección, Medida y Ensayo.
- Difusión de las Políticas de Seguridad y de Calidad

5. Técnicos.

Conjunto de técnicos que realizan tareas dentro de Proyectos de sector TIC: Investigación/análisis y Desarrollo, y personal en Formación.

6. Funciones y responsabilidades

Función	**Cargo**	**Nombre/ Apellidos**
Alta dirección	Director (D)	
Responsable de proyecto 1	Persona representante de procesos del LABORATORIO responsable de las relaciones entre procesos/proyectos y TI	
Responsable de proyecto 2	Persona representante de procesos del LABORATORIO responsable de las relaciones entre procesos/proyectos y TI	
Responsable TI	Persona con perfil informático, responsable de: - Las definiciones relativas a la SI - La SSII e infraestructura técnica - Procesos de revisión y/o auditoría de SI	

	- Verificar controles -Gestión del SGSI del LABORATORIO -Gestión de las incidencias así como de la continuidad de negocio.	

7. Funciones y firma

En la tabla siguiente se definen la asociación entre las funciones de la organización y la firma de la documentación del SGSTI:

Nombre/ Apellidos	**Función**	**Firma**	**Visado**
NOMBRE 1	Alta dirección		
NOMBRE 2	Responsable de proyecto 1		
NOMBRE 3	Responsable de proyecto 2		
NOMBRE 4	Responsable TI		

8. Comunicación Interna

Independientemente de los canales de comunicación utilizados, la información transmitida será clara, adecuada a los conocimientos del receptor, contrastable, así como, verídica. Los Métodos para transmitir esta comunicación dentro del LABORATORIO serán:

- Oral
- Correo informático interno
- Reuniones

9. Comité de dirección.

La comisión de Seguridad de LABORATORIO IICC, está constituida por:

- El director del LABORATORIO
- Responsables de Proyecto
- Responsable de TI, que actuará como coordinador de las acciones aprobadas por el Comité.

Dicha Comisión de Seguridad le compete el control del ciclo PDCA de mejora y se reunirá al menos una vez cada dos meses y, a propuesta de uno de sus miembros, y cuando se produzca una situación de riesgo considerada grave o muy grave que requiera la

adopción de medidas. En todo caso, el Responsable de TI llevará custodia del Registro de Convocatorias y Actas de reunión y seguimiento de acuerdos.

Anexo VI. Catálogo de activos de seguridad

Título : Catálogo de activos de seguridad		
Elaborado/modificado: Responsable de TI		**Firma:**
Revisado : Responsable de Proyecto 2		**Firma:**
Aprobado : Director		**Firma**
Versión: 2016-01	**Revisión: 0**	**Fecha: 06/06/2016**

	NOMBRE ACTIVO DE SEGURIDAD	**DESCRIPCIÓN**	**EFECTO SOBRE EL RIESGO**	**DOCUMENTO EN EL QUE SE DESCRIBE EL DETALLE DEL CONTROL**
1	PROCESO DE CONTROL y SEGUIMIENTO	Revisiones globales del sistema de gestión que pretenden mostrar los no cumplimientos con los procedimientos establecidos en el SGSTI	Se reduce	Manual de Seguridad
2	PROCESO DE RECONOCIMIENTO DE USUARIO	Responsable de proyecto 1	Se reduce	Se incorporarán como parte del proceso de acogida en la organización, los documentos base del SGSTI que deberá conocer cada nuevo empleado
4	PROCESO DE GESTION DE CAPACIDAD	Realizar análisis con periodicidad mensual de la capacidad de la infraestructura que soportan el servicio: servidores y comunicaciones. Que se alertará a través de la generación de una actividad hacia el responsable para la realización del análisis.	Se reduce	Plan de capacidad
5	PLAN DE CONTINUIDAD	Se debe disponer de un sistema de monitorización que alerte a los técnicos sobre cualquier problema que surja en los equipos, como pueden ser perdidas de conectividad, equipos saturados, fallo en discos Implantado. Se	Se reduce	Plan de continuidad y disponibilidad

		utiliza los sistemas propios del servidor para monitorizar los equipos y servicios alojados en el CPD.		
6	DEFINICIÓN DE POLITICA Y MANUAL DE SEGURIDAD	Cada vez que se realizan cambios importantes en la infraestructura de los equipos o tras un cambio organizativo importante se revisa la política para comprobar si es necesario actualizarla. Adicionalmente se revisa de forma anual.	Se controla	Política de seguridad
7	RESPALDO DE DIRECCIÓN DOCUMENTADO	La dirección del LABORATORIO brinda su apoyo al proceso de la seguridad como se puede observar en la política de seguridad, la cual está firmada por el Director.	Se elimina	Política de seguridad
8	PROCESO DE GESTION DE SOLICITUDES Y CAMBIOS	Al realizar cambios significativos, si gestión de cambios lo considera oportuno, se solicita asesoramiento al área de seguridad.	Se elimina	Manual de seguridad
9	PROCESO DE GESTION DE INCIDENTES DE SEGURIDAD	Revisión continua: Se revisarán mensualmente las incidencias de los servicios para determinar los errores más comunes y los operadores con más errores de registro. Con las conclusiones extraídas se dará formación personalizada y se creará un documento de formación a disposición de todos los usuarios del LABORATORIO. Esto se realizará, al menos, durante un año.	Se reduce	Proceso de gestión de incidentes
10	PROCESO DE CONFIGURACIÓN DE BBDD	Las auditorías de la BBDD , incidentes, problemas y cambios obligarán a la adecuación del alcance de la BBDD.	Se reduce	Proceso de gestión de incidentes
11	Servicio EXTERNO - ADSL	Se tienen contratadas líneas en el Laboratorio adicionales al servicio de red propio de la corporación.	Se reduce	Manual de Seguridad Plan de continuidad y disponibilidad
12	Servicio EXTERNO - Suministro eléctrico	Se dispone de un SAI que solucionaría un caso de corte de suministro eléctrico temporal	Se reduce	Plan de continuidad y disponibilidad
13	Servicio EXTERNO - Suministro eléctrico	Con un fallo de larga duración, la continuidad del servicio, se realizaría desde instalaciones centrales corporativas	Se reduce	Plan de continuidad y disponibilidad
14	INFRAESTRUCTURA - Servidor fisicos y lógicos	Se asegura con la política de contraseñas. Se auditan los intentos de LOGON	Se controla	Manual de seguridad

15	INFRAESTRUCTURA - Servidor fisicos y lógicos	No existe acceso Remoto al servidor	Se reduce	Manual de seguridad
16	INFRAESTRUCTURA - Punto de acceso Inalambrico	Ante un fallo, los usuarios conectarán a través de la LAN corporativa	Se reduce	Plan de continuidad y disponibilidad
17	INFORMACIÓN_Datos en Servidor	Proceso de copias de seguridad. Copia diarias en disco duro que se guarda en Servidor de Backup. Copia Semanal que se guarda en instalaciones de CENTRAL CORPORATIVA	Se controla	Política de seguridad
18	INFORMACIÓN_Configuraciones del router/Switch	Procedimiento de reconfiguración de Router / Switch.	Se controla	Política de seguridad
19	INFORMACIÓN_CMDB	Copias diaria completa. Copia antes de realizar cualquier actualización. Se asume la pérdida y el tiempo de recuperación	Se controla	Política de seguridad
20	INFORMACIÓN	Se considera razonable, dado la baja probabilidad de que ocurra una catástrofe, que se perdieran todos los datos de un día	Se asume	Política de seguridad
21	INFORMACIÓN	Se debe disponer de un sistema de copias de seguridad automatizadas con el fin de poder restaurar la información crítica en caso de perdida por cualquier motivo (virus, fallos software, fallos hardware, errores humanos...)	Se controla	Política de seguridad
22	INFORMACIÓN	Se considera razonable la copia diaria de todos los archivos del servidor	Se elimina	Política de seguridad
23	INFORMACIÓN	Las copias se realizan internamente en el servidor.	Se reduce	Política de seguridad
24	INFORMACIÓN	Se realizarán simulacros periódicos para comprobar la integridad de las copias de seguridad creadas. Restauraciones Anuales	Se reduce	Política de seguridad
25	SOFTWARE – ANTIVIRUS	Monitorización diaria de los servidores	Se reduce	Plan de continuidad y disponibilidad
26	SOFTWARE	Sin acceso desde el exterior al servidor interno	Se elimina	Política de seguridad
27	SOFTWARE	Con el fin de evitar infecciones víricas propagadas internamente se han de mantener todos los equipos actualizados, parcheados y con sistemas antivirus. Periódicamente se revisa el estado de actualización de los antivirus del servidor.	Se reduce	Política de seguridad

28	INSTALACIONES	Sólo el personal interno puede acceder a las dependencias de la organización. Cualquier persona ajena deberá ir acompañada de personal interno.	Se reduce	Política de seguridad
29	INSTALACIONES – Salas de servidores	Existe un extintor para intentar controlar un fuego en caso de producirse.	Se controla	Política de seguridad
30	INSTALACIONES	La vigilancia 24x7 del edificio avisaría en caso de incendio al director de sistemas y bomberos.	Se reduce	Política de seguridad
31	INSTALACIONES	Revisar periódicamente la asignación de perfiles y los permisos de acceso concedidos.	Se reduce	Política de seguridad
32	RRHH – Responsables	Todos los roles de importancia en la organización tienen siempre un responsable y un coordinador de respaldo	Se elimina	Plan de continuidad y disponibilidad
33	RRHH	Documentación de los conocimientos que han de tener. Plan de formación para nuevos usuarios.	Se reduce	Competencia, concienciación y formación
34	RRHH - Backup de conocimientos	Poner los medios para asegurar que existe un backup de conocimientos, por puesto, para casos de baja en el LABORATORIO. En la mayoría de las áreas técnicas se trabaja por "pools", esto es, varias personas con conocimientos similares haciendo tareas de proyectos varios. Para mitigar el impacto de posibles bajas, se dispone de una base de conocimiento, se define procedimiento de actuación y se generan instrucciones de trabajo específicas para tareas de detalle.	Se reduce	Plan de continuidad y disponibilidad
35	SOPORTE DEL SERVICIO (Infraestructura y personal)	Definición de un Plan de contingencias	Se controla	Plan de continuidad y disponibilidad

Anexo VII. Plan de Contingencia y Disponibilidad

1. Introducción y requisitos

La definición del plan de contingencia y recuperación de la disponibilidad, necesita que el LABORATORIO haya evaluado y documentado las amenazas, riesgo en impacto sobre sus activos definidos en el alcance de los servicios/proyectos del SGSTI. Una contingencia comienza cuando el desarrollo normal de la actividad organizativa se ve afectado negativamente, poniendo en peligro la continuidad de las actividades del LABORATORIO, y termina cuando se restablece la situación original y normal de las actividades.

2. Introducción y requisitos

El propósito del plan de contingencia es "gaantizar la continuidad y disponibilidad de los activos críticos del LABORATORIO. Estos activos de los que su falta de disponibilidad puede depender la existencia del servicio/proyecto o, incluso, Del LABORATORIO.

3. Alcance

Los servicios cubiertos por este plan son los que figuran en el alcance del ANEXO Manual de Seguridad del LABORATORIOy que se prestan desde las instalaciones sitas en sus dos sedes de DIRECCION COMPLETA.

4. Contexto del plan de continuidad y recuperación de disponibilidad

Rol: Gestor de continuidad. Corresponde al Responsable TI del LABORATORIO. Las funciones desempeñadas y la asignación de dicho role son aprobados por el Director. Es el responsable de asegurar que este plan se mantiene, de que se ejecutan las pruebas de acuerdo a la programación establecida y que se actualiza de acuerdo a los requisitos de continuidad del servicio establecidos en la Política de Seguridad.

- Herramienta de soporte: La gestión de la continuidad y recuperación de la disponibilidad se realizará mediante la monitorización directa de los activos y la observación de sus umbrales establecidos de disponibilidad para el servicio/proyecto.
- Comunicación del plan. Este plan se distribuye a los usuarios del LABORATORIO que puedan verse afectados por alguna acción definida en el plan de continuidad.
- Almacenamiento. Las copias digitales de este plan están almacenadas en el servidor de datos.
- Revisión. El plan se revisará cada dos meses al menos, y se actualizará, si procede, a partir de los resultados de las pruebas realizadas de acuerdo a la programación

establecida en la tabla de continuidad. Además, trimestralmente se revisarán teléfonos de contacto, direcciones de las partes implicadas y se actualizarán las modificaciones, quedando registrado el cambio.

- Ejecución de las pruebas. Este plan es probado y ejecutado con la periodicidad que figura en la programación acordada con las partes implicadas. Las modificaciones resultantes del plan de pruebas y/o de la programación de las mismas se incorporan al plan de mejora.

5. Fase de activación

Este plan se activa en respuesta a incidencias que causen un nivel de impacto muy alto en el servicio o actividad del Laboratorio, especialmente si afectan a actividades críticas del mismo.

Las causas que darían lugar a la activación parcial o total del plan deben acordarse. Se proponen:

- Imposibilidad continuada de conexión a los servidores en los que se alojen aplicativos y datos de usuarios.
- Imposibilidad de acceso al edificio desde donde se presta normalmente el servicio, por incendio, inundación, explosión.
- Falta prolongada del suministro eléctrico en las instalaciones del LABORATORIO.

El/los usuario/s administradores del servicio/s afectado/s serán los encargados de activar total o parcialmente el plan. Serán ellos mismos los responsables de decidir cuándo, una vez recuperado el servicio dentro de sus parámetros normales, se puede desactivar la ejecución del plan. La siguiente tabla recoge los responsables:

Nombre/ Apellidos	**Rol**	**Nº de Extensión**	**Nº Tf. Móvil**
NOMBRE RESPONSABLE SERVICIO PROYECTO	Propietario del servicio	5551	555 66 66 66
RESPONSABLE TI	Responsable TI	5555	555 66 66 55
...			

El Responsable de TI, como responsable de Continuidad, y en su ausencia el Director o Responsable de Proyecto disponible deben ser siempre informados de la activación del Plan de Contingencia. La naturaleza y gravedad de la incidencia determinará a quién y cómo derivar de nuevo la información. El propietario del servicio será quien realice la acción de informarles y comunicarles de la incidencia y de la activación total o parcial del plan de continuidad.

6. Fase de Continuidad de Negocio

El plan de continuidad permite mantener el servicio operativo frente a eventos críticos y minimizar el impacto negativo sobre el mismo, consiguiendo que los usuarios no se vean afectados por los fallos potenciales. La metodología práctica comprende la identificación del riesgo, la resolución propuesta y el tiempo que lleva aplicar dicha resolución y la realización de pruebas periódicas para certificar el funcionamiento de la solución a la contingencia.

El objetivo de esta fase del plan de contingencia es asegurar que las actividades críticas se reanuden lo antes posible y / o continúan dándose durante la interrupción.

- *Actividades críticas*. Se han identificado las siguientes actividades críticas:
    - Provisión de las condiciones ambientales adecuadas para proveer el Servicio de "Gestión Técnica y de Operaciones TI de Redes de Telecomunicaciones y Sistemas"
    - Disponer de las comunicaciones adecuadas en la ubicación alternativa para la provisión del servicio.
    - Proveer del equipamiento adecuado para disponer de puestos de trabajo en la ubicación alternativa
    - Cargar las BBDD y aplicativos del SGSTI para poder usar el sistema en condiciones normales hasta la recuperación de la ubicación habitual.
- *Actividades NO críticas.* Se han identificado las siguientes actividades NO críticas, que son actividades secundarias que se recuperan una vez que las actividades críticas se hayan reanudado:
    - Actividades administrativas habituales del *backend*.
    - Actividades del LABORATORIO habituales.

7. Fase de recuperación y reanudación

El objetivo de la fase de recuperación y reanudación es reiniciar las actividades normales de trabajo de los servicios/proyectos. Si se prolongara la duración de la incidencia, es posible que las operaciones normales de prestación del servicio tuvieran que ser realizadas desde una ubicación alternativa del LABORATORIO.

Acciones de recuperación y reanudación. Detalladas para cada uno de los escenarios en la siguiente Tabla:

INCIDENCIA	RESOLUCIÓN	TIEMPO	PRUEBAS	PERIODO
Se estropea un PC de puesto de trabajo	Se dispone de un PC de Backup	10 min.	Prueba del correcto funcionamiento y actualización del PC de Backup de puesto de trabajo	Mensual
Se estropea un servidor	Se dispone de un PC de Backup	10 min	Prueba del correcto funcionamiento del Servidor	Mensual

Caída de línea ADSL	Se dispone de un balanceo para que salgan por la línea de la Sede 2	Inmediato	Tirar la línea de la Sede 2 y verificar que se sigue trabajando por la línea de la Sede 1	Mensual
Se estropea el switch de la Lan	Conectar a través de la Wifi	5 min.	Probar a desconectar el cable de LAN y salir por la wifi	Mensual
Se pierde el suministro eléctrico en el edificio (>2 horas)	Desplazamiento a centro de trabajo alternativo en Nube, trabajo en domicilios con móviles y portátiles	Tiempo de Desplazamiento al edificio de Sede 2	Llamar al Servicio de Infraestructuras corporativo	Mensual

Se registrarán todos los gastos que incurran como resultado de la incidencia.

8. Plan de disponibilidad del servicio

El Plan de Disponibilidad tiene como objetivo mejorar la disponibilidad general de la Infraestructura TI para cerciorarse de que se pueden alcanzar, de forma segura, los niveles de disponibilidad actuales y futuros de una manera eficiente. Se revisa de manera continua. Las actividades que forman parte de la monitorización y mejora de la disponibilidad son:

- Medir la disponibilidad de aplicativos y datos para diferentes usuarios. Para ello se mide las tasas de disponibilidad / NO disponibilidad en términos de las métricas establecidas.
- Monitorizar y evaluar hacia dónde se comporta la disponibilidad (cuellos de botella), confiabilidad y el mantenimiento de los activos TI.
- Realizar informes de monitorización y oportunidades de mejora.

Fecha última actualización	Fecha próxima actualización
Firma Director	Firma Responsable TI

Bibliografía

Ahern, D. M., Armstrong, J., Clouse, A., Ferguson, J. R., Hayes, W., & & Nidiffer, K. E. (2005). CMMI SCAMPI Distilled: Appraisals for Process Improvement. Boston: Addison-Wesley.

Alcaraz, Cristina; Fernández, Gerardo and Carvajal, Fernando (2012). Security Aspects of SCADA and DCS Environments, in J. Lopez et al. (Eds.): Critical Information Infrastructure Protection, LNCS 7130, pp. 120–149.

Álvarez Fernández, César (Coord.) (2016). *El modelo de Protección de Infraestructuras Críticas en España. Guía PIC*. Madrid: Fundación Borredá.

Arboleda, H., Paz, A., & Casallas, R. (2013). Metodología para implantar el Modelo Integrado de Capacidad de Madurezen grupos pequeños y emergentes. Estudios Gerenciales 29 , 177–188.

Arcilla, M. (2013). *Metamodelo para la implantación de la gestión financiera de servicios TIC en las MPMES*. Madrid: UNED.

Arcilla, M., Calvo-Manzano, J., & San Feliu, T. (2013). Building an IT service catalog in a small company as the main input for the IT financial management. Computer Standards & Interfaces 36, 42–53.

Arnold, M. (1998). Recursos para la investigación sistémico/constructivista. Cinta moebio 3, 31-39.

Bahsi, H. and Maennel, O. M. (2009). A Conceptual Nationwide Cyber Situational Awareness Framework for Critical Infrastructures. In S. Buchegger and M. Dam (Eds.): NordSec 2015, LNCS 9417, Switzerland: Springer, pp. 3–10, 2015.

Baina, A., Abou El Kalam, A., Deswarte, Y., Ka°aniche, M. (2008). A Collaborative Access Control Framework for Critical Infrastructures. In: IFIP 11.10 Conference on Critical Infrastructure Protection, ITCIP 2008, Washington, DC, USA, March 16-19.

Baker, S., Waterman, S. & Ivanov, G. (2010). In the Crossfire: Critical Infrastructure in the Age of Cyber War. McAffee, Recuperado de http://resources.mcafee.com/content/NACIPReport.

Barrio, Félix A. y Ramos, Antonio (Coords.) (2012). Protección de infraestructuras críticas guía para la elaboración de planes de seguridad del operador y planes de protección específica. León: Agrupación empresarial innovadora para la seguridad de las redes y los sistemas de información. Recuperado de www.seguritecnia.es/content/download/4506/59827/file/GuiaPIC.pdf

Bayona, S., Calvo-Manzano, J., & San Feliu, T. (2012). Critical Success Factors in Software Process Improvement: A Systematic Review. SPICE, CCIS 290, pp 1-12.

Biolchini, Jorge; Gomes, Paula; Cruz, Ana C. and Horta, Guilherme (2005). *Systematic Review in Software Engineering*. Technical Report. RT-ES 679/05. Rio de Janeiro: Systems Engineering and Computer Science Departmente COPPE/UFRJ Recuperado de http://disciplinas.stoa.usp.br/pluginfile.php/92788/course/section/27982/Biolchini2005_Systematic_Review_in_Software_Engineering.pdf

Blangenois, Jonathan; Guemkam, Guy; Feltus, Christophe; Khadraoui, Djamel (2013) *Organizational Security Architecture for Critical Infrastructure*, In Proceedings of 8th FARES 2013 IEEE, Germany.

Calder, A. (2008). *IT Governance: Implementing Frameworks and Standards for the Corporate Governance of IT*. London: Kogan Page Publishers.

Calvo-Manzano, J., Cuevas, G., Gasca, G., San Feliu, T., & Vega, V. (2009). State of the art for risk management in software acquisition. ACM SIGSOFT Software.

Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W. and Young, Lisa R. (2010). *CERT® Resilience Management Model, Version 1.0. Improving Operational Resilience Processes.* Pittsburgh, PA: SEI- Carnegie Mellon University. Recuperado de http://sei.cmu.edu/reports/10tr012.pdf

Chandra, Pravir (Project Lead) (2006). CLASP -Comprehensive, Lightweight Application Security Process, Version 1.2, Version Date: 31 march 2006. Recuperado de http://www.owasp.org/index.php/Category: OWASP_CLASP_Project.

Chen, Zhongqiang; Zhang, Yuan and Chen, Zhongrong (2009). A Categorization Framework for Common Computer Vulnerabilities and Exposures. *The Computer Journal Advance Access*. Recuperado de http://comjnl.oxfordjournals.org/content/53/5/551.abstract

Chiaradonna, Silvano; Di Giandomenico, Felicita and Lollini, Paolo (2008). Evaluation of Critical Infrastructures: Challenges and Viable Approaches, In R. de Lemos et al. (Eds.): Architecting Dependable Systems V, LNCS 5135, pp. 52–77.

Chien, Eric (2010). Stuxnet: A Breakthrough. Recuperado de http://www.symantec.com/connect/blogs/stuxnet-breakthrough

Choi, WoongChul & Yoo, DaeHun (2009). Software Assurance Towards Better IT Service, Journal of Service Science (2009) 1:31-56

Coppolino, Luigi; D'Antonio, Salvatore ; Formicola, Valerio and Romano, Luigi (2007). Enhancing SIEM Technology to Protect Critical Infrastructures. In López, J & Hämmerli, B. M. (eds.). CRITIS 2012, LNCS, vol. 7722, Berlín-Heidelberg.: Springer, pp. 10-21.

CSAE. (2012). MAGERIT–versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Ministerio de Hacienda y Administraciones Públicas.

Cuevas Agustín, Gonzalo, Coordinador (2002). Gestión del proceso software. Madrid: Centro de Estudios Ramón Areces.

Curphey, M. (2009). The Ten Best Practices for Secure Software Development. ISC2.

De la Cámara Delgado, Mercedes (2016). *GPS-PYMEs: Marco de Gestión de Proyectos para el desarrollo Seguro en PYMEs*. Tesis doctoral. Madrid: Universidad Politécnica de Madrid.

De la Camara, M., Sáenz, F., Calvo-Manzano, J., & Arcilla, M. (2015). Security by design factors for developing and evaluating secure software. 2015 *10th Iberian Conference on Information Systems and Technologies (CISTI),* (pp. 1 - 6). Aveiro (Portugal): IEEE.

Deming, W. (1989). Calidad, productividad y competitividad: la salida de la crisis. Madrid: Diaz de Santos.

Deswarte, Y. (2011). Protecting Critical Infrastructures While Preserving Each Organization's Autonomy. In R. Natarajan and A. Ojo (Eds.): ICDCIT 2011, LNCS 6536, pp. 15–34, 2011.

Dougherty, Chad; Sayre, Kirk; Seacord, Robert C.; Svoboda, David and Togashi, Kazuya (2009). *Secure Design Patterns. Technical Report*, CMU/SEI-2009-TR-010, ESC-TR-2009-010.

Dunn, M. & Abele-Wigert, I. (2006): The International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations (Vol. I) (Zurich, Center for Security Studies, 2006).

El Kalam, Anas Abou & Deswarte, Yves (2009). Critical Infrastructures Security Modeling, Enforcement and Runtime Checking, In R. Setola and S. Geretshuber (Eds.): CRITIS 2008, LNCS 5508, Berlin Heidelberg: Springer-Verlag, pp. 95–108.

Falessi, Nicole; Gavrila, Razvan; Klejnstrup, Maj Ritter, Moulinos, Konstantinos (2012). *National Cyber Security Strategies. Practical Guide on Development and Execution*. Heraklion, Greece: European Network and Information Security Agency (ENISA)

Falk, Laura; Prakash, Atul and Borders, Kevin (2008). Analyzing websites for user-visible security design flaws. *ACM International Conference Proceeding Series*; Vol. 337, pp. 117-126.

Falliere, Nicolas, Murchu, Liam O., y Chien, Eric (2011). W32.Stuxnet Dossier. Symantec. Recuperado de http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Feitosa, Daniel (2014). An Architecture Design Method for Critical Embedded Systems. In Proceedings of the *WICSA'14*, April 7–11, 2014, Sydney, New South Wales, Australia. Vol. 15.

Feltus, Christophe & Khadraoui, Djamel (2013). On designing automatic reaction strategy for critical infrastructure SCADA system. In Proceedings of the 6th International Conference on Security of Information and Networks SIN '13, Nov 26-28 2013, Aksaray, Turkey, pp. 444-445.

Firvida, Daniel (2016). Familias de malware en la industria. Instituto Nacional de Ciberseguridad, 2016. Recuperado de https://www.incibe.es/blog/BlogSeguridad/ultimos_articulos/?postAction=getBlogHome&blogID=1000077536&p=0

Forrester, E. B. (2011). *CMMI for services: Guidelines for superior service. 2nd Edition*. Boston: Addison-Wesley.

Gregoire, Johan; Buyens, Koen; De Win, Bart; Scandariato, Riccardo and Joosen, Wouter (2007): On the Secure Software Development Process: CLASP and SDL Compared. In the proceedings of the Third IEEE International Workshop on Software Engineering for Secure Systems, 2007.

Grossi, L., & Calvo-Manzano, J. (2008). Análisis de Decisiones en la Selección de Proveedores de Tecnologías de la Información: Una Revisión Sistemática. RISTI, 67-79.

Hadavi, M.A.; Sangchi, H. M.; Hamishagi, V. S. and Shirazi, H. (2008): Software Security; A Vulnerability Activity Revisit. In the Third International Conference on Availability, Reliability and Security, IEEE.

Harp, Derek and Gregory-Brown, Bengt (2015). *The State of Security in Control Systems Today*. Swansea: SANS Institute. InfoSec Reading Room, Recuperado de https://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042

Hefley, B. (2010). ESourcing Capability Model for Service Providers – ESCM-SP. van Haren Publishing.

Hefley, B., & Loesche, E. (2010). ESourcing Capability Model for Client Organizations – ESCM-CL. van Haren Publishing.

Humphrey, W. S. (1989). *Managing the Software Process*. Boston, MA: Addison-Wesley.

Humphrey, W. S. (1997). *Introduction to the personal software process. SEI Series in Software Engineering*, Reading, MA: Addison-Wesley.

Humphrey, W. S. (2002). Introduction to the team software process. SEI Series in Software Engineering, Reading, MA: Addison-Wesley.

IBM Corporation, A Strategic Approach to Protecting SCADA and Process Control Systems (2007). Recuperado de http://documents.iss.net/whitepapers/SCADA.pdf

IEEE. (1999). IEEE Guide - Adoption of PMI Standard - a Guide to the Project Management Body of Knowledge. IEEE Std 1490-1998.

INCIBE (2016). *Tendencias en el mercado de la ciberseguridad*. León: Instituto Nacional de Ciberseguridad. MINETUR. Recuperado de https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf

ISACA. (2009). An Introduction to the Business Model for Information Security. Meadows, IL 60008 USA: ISACA.

ISACA (2014). ITAF: A Professional Practices Framework for IS Audit/ Assurance, 3rd Edition. Rolling Meadows, IL: ISACA.

Ismail, Suhaila; Sitnikova, Elena & Slay, Jill (2014). Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks. In N. Cuppens-Boulahia et al. (Eds.): SEC 2014, IFIP International Federation for Information Processing, AICT 428, pp. 242–249, 2014.

ISO (2004). ISO/IEC 15504-3:2004,Information technology -- Process assessment (All parts). Geneve: ISO.

ISO (2008). ISO/IEC 38500:2008 Corporate governance of information technology. Geneve: ISO.

ISO (2008b). ISO/IEC 12207:2008 Systems and software engineering – Software life cycle processes. Geneve: ISO.

ISO (2013). ISO/IEC 27002, Information Technology. Security Techniques. Code of Practice for Information Security Management. Geneve: ISO.

ISO (2015). ISO/IEC 20000-1:2011. Information technology -- Service management -- Part 1: Service management system requirements. Geneve: ISO.

ISO (2015b). ISO/IEC 27040:2015. Information technology -- Security techniques -- Storage security. Geneve: ISO.

ITGI (2009). *An Introduction to the Business Model for Information Security*. Rolling Meadows, IL: ISACA.

ITGI (2012). *COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. Rolling Meadows, IL: ISACA.

Juristo, Natalia and Moreno, Ana M. (2001). *Basics of Software Engineering Experimentation*. Dordrecht (The Netherlands): Kluwer.

Kaufmann, H., Hutter, R., Skopik, F., Mantere, M. (2015). A structural design for a pan-european early warning system for critical infrastructures. e & i. Elektrotechnik und Informationstechnik 132, pp. 117–121.

Kitchenham, B. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering Version 2.3. Durham: Technical Report EBSE-2007-01, Software Engineering Group, School of Computer Science and Mathematics, Keele University, and Department of Computer Science.

Kobashi, T., Kaiya, H., Yoshioka, N., Washizaki, H., Okubo, T., & Fukazawa, Y. (2011). Validating Security Design Pattern Applications Using Model Testing. Badgers'11, 70-77.

López, Javier & Hämmerli, Bernhard M. (Eds.) (2007). *Critical Information Infrastructures Security*, Second International Workshop, CRITIS 2007, Málaga (Spain). Berlín: Springer.

Luallen, Matthew E. (2013). *SANS SCADA and Process Control Security Survey*. Swansea: SANS Institute. InfoSec Reading Room.

MAP (2001). *Métrica v.3.* Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html#.V7iRU_mLTIV

Meland, Per Håkon and Jensen, Jostein (2008). Secure Software Design in Practice. In the Third International Conference on Availability, Reliability and Security, IEEE.

Mesquida, A., Mas, A., Amengual, E., & Calvo-Manzano, J. (2012). IT Service Management Process Improvement based on ISO/IEC 15504: A systematic review. Information and Software Technology 54, 239-247.

Ministerio del Interior (2011). *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*. Recuperado de http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630

Mouratidis, Haralambos and Giorgini, Paolo (2007). Secure Tropos: a Security-Oriented Extension of the Tropos Methodology, *International Journal of Software Engineering and Knowledge Engineerin*g , Volume 17, 2007, pp.285-309.

Mouratidis, Haralambos; Jürjens, Jan and Fox, Jorge (2006). Towards a Comprehensive Framework for Secure Systems Development. *Advanced Information Systems Engineering*, pp. 48-62.

NIST (2008). 2 NIST 800-82 – Guide to Industrial Control Systems (ICS) Security – U.S. Department of Commerce –September 2008.

NIST (2009) *NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations Access Control (AC) family* - U.S. Department of Commerce - August 2009. Recuperado de http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2- final.pdf

NIST (2009b). *NIST 800-82 Guide to Industrial Control Systems* (ICS) Security - U.S Department of Commerce - September. Recuperado de http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

OCDE (2004). Principios de Gobierno Corporativo de la OCDE. París: Organización para la Cooperación y el Desarrollo Económicos. Recuperado de https://www.oecd.org/daf/ca/corporategovernanceprinciples/37191543.pdf

OGC (2009). Éxito en la gestión de proyectos con PRINCE2. Reino Unido: TSO.

ONTSI (2016). *Informe e-Pyme 2015 de análisis sectorial de la implantación y uso de las TIC en las empresas españolas*. Madrid: Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información-MINETUR.

Paganini, Pierluigi (2014). Cyber attack on German steel factory caused severe damage. Recuperado de http://securityaffairs.co/wordpress/31368/cyber-crime/cyber-attack-german-steel-factory.html

Palacio, Juan (2015). *Gestión de proyectos Scrum Manager*. Zaragoza: Lubaris Info 4 Media S.L.

Palacio, Juan y Ruata, Claudia (2011). Scrum Manager Gestión de Proyectos. Safe Creative Recuperado de http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/Gesti%C3%B3n%20de%20proyectos.pdf

Paulk, M. C., Charles, V., Curtis, B., & Chrissis, M. B. (1995). *The Capability Maturity Model: Guidelines for improving the software process*. Boston: Addison-Wesley.

PMI. (2009). *Project Management Institute. A guide to the project management body of knowledge (PMBOK guide)*. 4th Edition. Newton Square: Project Management Institute.

PMI. (2014). Guía de los Fundamentos Para la Dirección de Proyectos (Guía del PMBOK®)–Quinta Edición. Newton Square: Project Management Institute.

Poulsen, Kevin (2003). Slammer worm crashed Ohio nuke plant net. Recuperado de http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/

Rehman, S. and Mustafa, K. (2009). Research on Software Design Level Security Vulnerabilities, ACM SIGSOFT Software Engineering Notes,Volume 34 Number 6.

Rodríguez Penin, Aquilino (2007). *Sistemas SCADA*. 2ª edición. MARCOMBO 2007

Rodríguez, J. V. G., Carmona, R. M., Carrasco, Y. V., & Contreras, B. M. G. (2013). Análisis-Evaluación de riesgos, aplicando la metodología Mosler en las pymes de Tlaxcala, México.

Sanders, William H. (2012). *Assuring the trustworthiness of the smarter electric grid*. April 2012 ICPE '12: Proceedings of the 3rd ACM/SPEC International Conference on Performance Engineering, p. 19.

Sarriegi, J., Torres, J., & Santos, J. (2005). Explaining Security Management Evolution through the Analysis of CIOs' Mental Models. The 23rd International Conference of the System Dynamics Society.

Scarfone, K., Souppaya, M., & Cody, A. &. (2008). Technical Guide to Information Security Testing and Assessment. Gaithersburg, MD 20899-8930: NIST.

Schaberreiter, T., Kittilä, K., Halunen, K., Röning, J., Khadraoui, D.: Risk assessment in critical infrastructure security modelling based on dependency analysis (short paper). In: 6th International Conference on Critical Information Infrastructure Security, CRITIS 2011 (2011)

Schaberreiter, T.; Varrette, S.; Bouvry, P.; Röning, J and Khadraoui, D. (2013). Dependency Analysis for Critical Infrastructure Security Modelling: A Case Study within the Grid'5000 Project. In A. Cuzzocrea et al. (Eds.): CD-ARES 2013 Workshops, LNCS 8128, pp. 269–287, 2013.

Schmitz, W.: Simulation and test: Instruments for Critical Infrastructure Protection (CIP). Information Security Technical Report 12, 2–15 (2007)

SEI. (2007). *+SAFE. A Safety Extension to CMMI-DEV, V1.2. Software Engineering Process Management Program.* Pittsburgh (PA): SEI-CMU.

SEI. (2010). *CMMI® for Services Version 1.3. CMMI-SVC, V1.3*, November 2010. Pittsburgh (PA): SEI-CMU.

SEI (2013). *CMMI para Servicios, Versión 1.3*. Pittsburgh (PA): SEI-CMU Recuperado de http://www.sei.cmu.edu/library/assets/whitepapers/Spanish%20Technical%20Report%20CMMI%20V%201%203.pdf.

Siemens, A. (2013). Security by design with CMMI for development. An Application Guide for Improving Processes for Secure Products. Pittsburgh (PA): SEI-CMU.

Solomon, Dan (2011) *Critical National Infrastructure Security Investment in Europe*. Brochure, February. Hawk ISM Security, Consulting & Risk Group [Recuperado de http://www.authorstream.com/Presentation/dansolo1967-864668-hawk-cni-security-investment-europe-2011-brochure/]

Trendmicro (2016). Utility Provider in Michigan Hit by Ransomware Attack. Recuperado de http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/electricity-utility-in-michigan-downed-by-ransomware-attack

Van Caenegem, Bart and·Skordas, Thomas (2007). Community research activities in secure and trustworthy ICT infrastructures, Telecommun Syst (2007) 35: 89–97.

Villalón, Antonio; Holguín, José Miguel; Belda, Nelo; Vila, José (2011). Protección de Infraestructuras Críticas 2011. Valencia: S2 Grupo.

Wang, J. A. and Guo, Minzhe (2009). *OVM: An Ontology for Vulnerability Management. In Proceedings of CSIIRW'09.* Tennessee.

Wohlin, C. , Runeson, P., Höst, M., Ohlsson, M., Regnell, B., Wesslén, A. (2000): *Experimentation in Software Engineering: An Introduction*, Dordrecht (The Netherlands): Kluwer Academic Publishers.

Wohlin,, C.; Höst, M. and Henningsson, W. (2003). Empirical Research Methods in Software Engineering, In *Lecture Notes in Computer Science: Empirical Methods and Studies in Software Engineering: Experiences from ESERNET*, edited by A. I. Wang and R. Conradi, Springer Verlag, Germany, LNCS 2765.

Zambon, E.; Etalle, S.; Wieringa, R. J. & Hartel, P. (2009). Model-based qualitative risk assessment for availability of IT infrastructures, Softw Syst Model (2011) 10:553–580.

Índice de Figuras

FIGURA 1.1. NÚMERO DE EMPRESAS POR SUBSECTOR INDUSTRIAL EN ESPAÑA, 2015. EN ROJO LOS 11 SUBSECTORES AFECTADOS POR LA CLASIFICACIÓN DE IICC EN UN GRADO SIGNIFICATIVO. FUENTE: ELABORACIÓN PROPIA EN BASE A DIRCE 2015, INE (ONTSI, 2016) **10**

FIGURA 1.2. ESQUEMA DE FUNCIONAMIENTO DE UN SISTEMA SCADA (FUENTE: BARRIO Y RAMOS, 2012) **13**

FIGURA 1.3. CORRELACIÓN ENTRE LA DEPENDENCIA DE LAS TIC Y LA VULNERABILIDAD MOSTRADA POR LOS PRINCIPALES SECTORES DE IICC 2011-2012 (FUENTE: SOLOMON, 2011) **17**

FIGURA 1.4. PRINCIPALES ESTÁNDARES UTILIZADOS POR LOS OPERADORES DE IICC EN ESTADOS UNIDOS (FUENTE: LUELLEN, 2013: P. 11) **20**

FIGURA 2.1 ISO/IEC 20.000. ESTRUCTURA DE PROCESOS. **34**

FIGURA 2.2. ÁREAS DE PROCESO CUBIERTAS POR EL CERT RESILIENCE MANAGEMENT MODEL (CERT-RMM) (FUENTE: SEI-CMU) **37**

FIGURA 2.3 MARCO DE TRABAJO PMBOK (FUENTE: PMI, 2009) **41**

FIGURA 2.4. ESQUEMA DE PROCESOS DE PSP (FUENTE: HUMPHREY, 1997) **42**

FIGURA 2.5 FLUJO DE PROCESOS CON TSP (FUENTE: HUMPHREY, 2002) **43**

FIGURA 2.6. ESQUEMA TÍPICO DE DIAGRAMA SCRUM (FUENTE: PALACIO Y RUATA, 2011) **44**

FIGURA 2.7. DOMINIOS ISO 27002:2013 ..... **57**

FIGURA 2.8. ACTIVIDADES DEL SGSI EN ISO/IEC 27001. ..... **58**

FIGURA 2.9. ELEMENTOS COMUNES DE LAS METODOLOGÍAS DE ANÁLISIS DE RIESGOS (FUENTE: BARRIO Y RAMOS (2012: P. 14): **59**

FIGURA 2.10. RESULTADOS DE LAS INVESTIGACIONES PRIMARIAS SOBRE IICC **69**

FIGURA 4.1. FASES DEL MARCO GPS-IICC **79**

FIGURA 5.1. FASES DEL MARCO GPS-IICC **103**

FIGURA 5.2. ACTIVIDADES DEL PATRÓN APLICADAS (FONDO RELLENO) **104**

FIGURA 5.3. RESULTADOS COMPARADOS DE LAS LÍNEAS INICIAL Y FINAL **119**

Índice de Tablas

TABLA 1.1 ESTRUCTURA DEL TRABAJO FIN DE MASTER 23

TABLA 2.1 MARCOS Y NORMAS INVOLUCRADOS EN LA ADMINISTRACIÓN SEGURA DE PROYECTOS DE DESARROLLO 24

TABLA 2.2. ELEMENTOS DE ESTUDIO PARA EL ANÁLISIS DE LAS GUÍAS, NORMAS Y MODELOS DE LA GOBERNANZA TI EN IICC 30

TABLA 2.3. ELEMENTOS DE ESTUDIO PARA EL ANÁLISIS DE LAS GUÍAS, NORMAS Y MODELOS DE GESTIÓN DE SERVICIOS TI EN IICC. 35

TABLA 2.4. ELEMENTOS DE ANÁLISIS DE LAS GUÍAS, NORMAS Y MODELOS DE MEJORA DE PROCESOS TI EN IICC 40

TABLA 2.5. ELEMENTOS DE ANÁLISIS DE LAS GUÍAS, NORMAS Y MODELOS DE GESTIÓN DE PROYECTOS TI APLICABLES EN IICC 44

TABLA 2.6. REVISIÓN SISTEMÁTICA. BBDD. 64

TABLA 2.7. REVISIÓN SISTEMÁTICA. RESULTADOS DE BÚSQUEDA. 65

TABLA 2.8 CRITERIOS A REVISAR. 65

TABLA 2.9. TENDENCIA ANUAL DE PUBLICACIONES RELEVANTES. 65

TABLA 2.10. INSTITUCIONES DE TRABAJO DE LAS FUENTES PRIMARIAS 66

TABLA 2.11. CLASIFICACIÓN EN LA EXTRACCIÓN DE DATOS. RESULTADOS. 68

TABLA 4.1. PRÁCTICAS ESPECÍFICAS PARA ESTABLECER LA POLÍTICA DE SEGURIDAD 80

TABLA 4.2. DEFINICIÓN DE PRERREQUISITOS DE SEGURIDAD 82

TABLA 4.3. PLANIFICACIÓN Y COMUNICACIÓN 83

TABLA 4.4. CLASIFICACIÓN DE ACTIVOS 84

TABLA 4.5. DEFINICIÓN DE LOS REQUISITOS DE ACCESO 85

TABLA 4.6. DEFINIR REQUISITOS DE SEGURIDAD DE TERCEROS 85

TABLA 4.7. ESTRUCTURAR EL CATÁLOGO DE REQUISITOS DE SEGURIDAD 86

TABLA 4.8. DEFINICIÓN DE REQUISITOS DE MONITORIZACIÓN DEL CATÁLOGO 87

TABLA 4.9. DISEÑO DEL PROCEDIMIENTO DE IMPLANTACIÓN DE ACTIVOS DE SEGURIDAD 88

TABLA 4.10. DISEÑO DE LOS PROCEDIMIENTOS TRANSVERSALES 88

TABLA 4.11. IMPLEMENTACIÓN DE LA SOLUCIÓN 89

TABLA 4.12. DISEÑAR EL CUADRO DE MANDO DE SEGURIDAD (CMS) 90

TABLA 4.13. DEFINICIÓN DE LAS MÉTRICAS Y CONTROLES DE MONITORIZACIÓN DE ACTIVOS 91

TABLA 4.14. MONITORIZACIÓN DE LA RECUPERACIÓN Y LA CONTINUIDAD 91

TABLA 4.15. REVISIÓN DE LOS ACTIVOS DE SEGURIDAD 92

TABLA 4.16. EMISIÓN DE INFORMES 93

TABLA 4.17. REVISIÓN DEL ESTADO ACTUAL 94

TABLA 4.18. PLANIFICAR Y COMUNICAR EL PLAN DE MEJORA 95

TABLA 5.1. DISTRIBUCIÓN DE CUESTIONES POR FASE 99
TABLA 5.2. LÍNEA BASE INICIAL. RESULTADO DE LA EVALUACIÓN DE LAS PREGUNTAS 100
TABLA 5.3. ROLES DE LA ORGANIZACIÓN 107
TABLA 5.4. NIVELES DEL CATÁLOGO DE REQUISITOS DE SEGURIDAD 108
TABLA 5.5. ESTRUCTURA DEL REGISTRO DE REQUISITO DE SEGURIDAD 109
TABLA 5.6. REGISTRO DE ACTIVOS DE SEGURIDAD 111
TABLA 5.7. ACTIVOS DE TI CRÍTICOS 113
TABLA 5.8. LÍNEA BASE FINAL. RESULTADO DE LA EVALUACIÓN DE LAS PREGUNTAS 116