

# IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

## Conformidad con el ENS ¿algo imposible?



CENTRO CRIPTOLÓGICO NACIONAL



## Certificado de Conformidad Esquema Nacional de Seguridad



Esquema Nacional de Seguridad

ENS-0004/2015

AENOR, Asociación Española de Normalización y Certificación, certifica que la organización

### **JUNTA DE COMUNIDADES DE CASTILLA LA MANCHA** **Consejería de Hacienda y Administraciones Públicas** **Dirección General de Función Pública**

dispone de un sistema de seguridad de la información conforme con la Norma UNE-ISO/IEC 27001:2014 que cumple con los requisitos establecidos en el ANEXO II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

para las actividades: La prestación de servicios comunes de Tecnología de la Información y Comunicaciones (TIC) a la Administración regional y al ciudadano, en infraestructura software, gestión de contenidos, infraestructura CPD y comunicaciones, así como los activos en los que se soportan, de acuerdo con la categorización del sistema vigente.

que se realizan: CONSEJERÍA DE FOMENTO  
DIRECCIÓN GENERAL DE TELECOMUNICACIONES Y NUEVAS TECNOLOGÍAS  
AVDA. RÍO ESTENILLA, S/N  
45071 TOLEDO

Fecha de primera emisión: 2015-07-30

Fecha de expiración: 2018-07-30

AENOR Asociación Española de Normalización y Certificación  
Avenida BBDO MARQUINA  
Director General de AENOR

**AENOR**

Asociación Española de Normalización y Certificación

Ciudad, 6. 28004 Madrid, España  
Tel. 902 102 201 - www.aenor.es

# IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

## Cómo conseguir la conformidad con el ENS

## Índice

- 1. Introducción**
- 2. Características del proyecto**
- 3. Sistema de Gestión Certificado SERTIC**
- 4. Claves de éxito**
- 5. Siguietes pasos**

# Introducción

## Marco legal



### LEGISLACIÓN EUROPEA

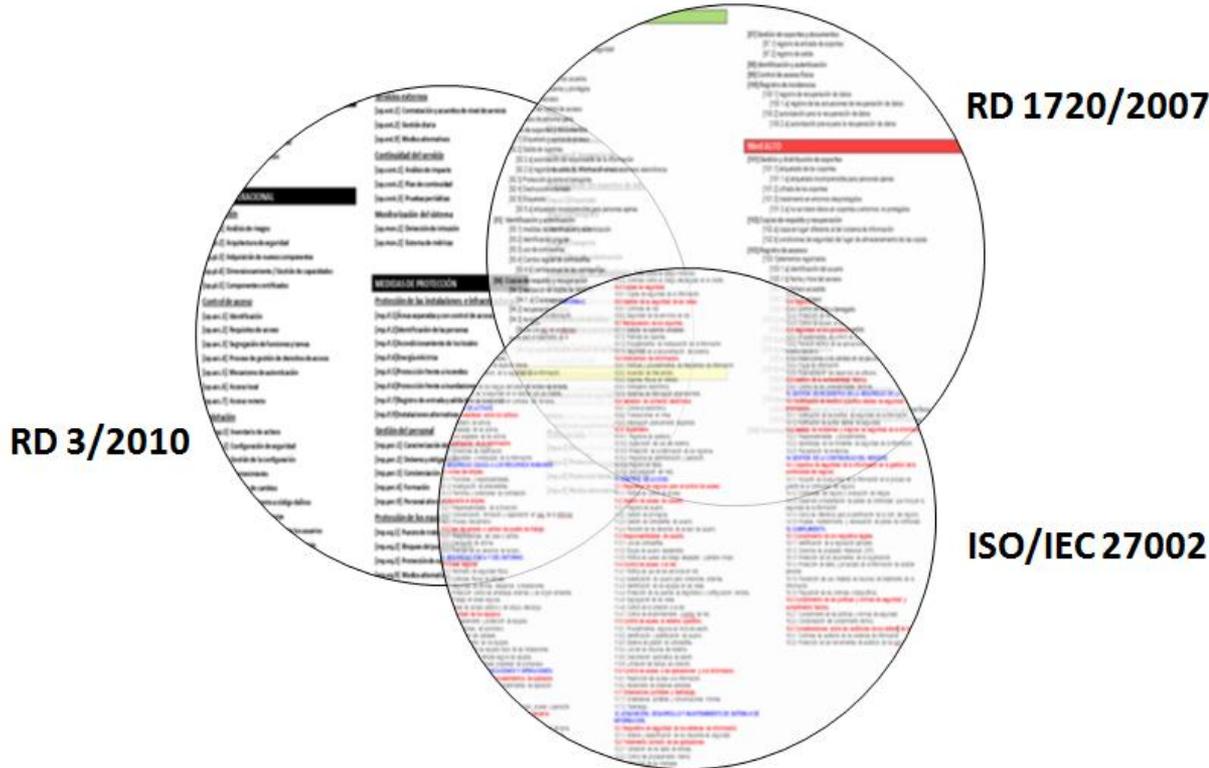
- **DIRECTIVA 95/46/CE** DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- **Reglamento (CE) 885/2006** por el que se establecen las disposiciones de aplicación del Reglamento (CE) no 1290/2005 del Consejo en lo que se refiere a la autorización de los organismos pagadores y otros órganos y a la liquidación de cuentas del FEAGA y del FEADER. (BSI, COBIT, ISO 27002)
- **Reglamento Delegado (UE) n ° 907/2014** de la Comisión, de 11 de marzo de 2014 , que completa el Reglamento (UE) n° 1306/2013 del Parlamento Europeo y del Consejo en lo relativo a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro (ISO/IEC 27001)



### LEGISLACIÓN NACIONAL

- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal y su reglamento de desarrollo (**RD 1720/2007**)
- **Real Decreto 3/2010**, de 8 de enero, por el que se aprueba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

# Introducción



# Introducción

## Antecedentes

- **Enero de 2008:** Certificación en Seguridad de la Información (27001) + Certificación en Calidad (9001) del Servicio de Internet de JCCM (Sistema de Gestión Unificado, SGU):
  - Alcance: Seguridad Perimetral, Correo electrónico, infraestructura del portal institucional.
- **Enero de 2010:** Estudio del ENS y elaboración de normas con mayor alcance
  - Decreto 57/2012, de 23 de febrero, por el que se establece la política de seguridad de la Información en la Administración de la Junta de Comunidades de Castilla-La Mancha
  - Orden de 11 de julio de 2012, de la Consejería de Presidencia y Administraciones Públicas y de la Consejería de Fomento por la que se aprueba la Instrucción sobre el uso aceptable de medios tecnológicos en la Administración de la Junta de Comunidades de Castilla-La Mancha
- **Mediados de 2012:** Comienza el proyecto de consolidación de servicios TIC en JCCM
  - Servicios comunes en la Dirección General de Telecomunicaciones y Nuevas Tecnologías (DGTNT)
  - Centro de Soluciones TIC, desarrollo y mantenimiento de aplicaciones (DGTNT)
  - Desarrollo y mantenimiento de aplicaciones en Organismo Pagador
  - Servicio de Salud (SESCAM)

# Introducción

## Organización TIC



## Introducción

**Enero de 2014:** Comienza el proyecto de redefinición del Modelo de Seguridad de la Información en JCCM

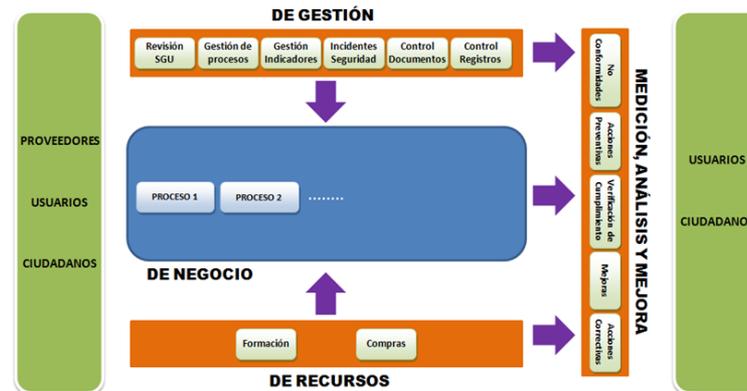
- Definir distintos Sistemas de Gestión en base a las competencias en materia TIC
- Ampliación de la certificación existente a la totalidad de los servicios comunes
- Adecuación a las normas **ISO/IEC 27001: 2013** y **ISO/IEC 27002:2013**
- Integración del **Esquema Nacional de Seguridad (ENS)**

**Objetivo:** Obtener una **TRIPLE CERTIFICACIÓN** en cada uno de los Sistemas de Gestión Unificados.

- Seguridad de la Información (ISO/IEC 27001)
- Conformidad con el Esquema Nacional de Seguridad
- Calidad (ISO 9001)

## Características del proyecto

- Definición del proyecto
- Identificación de la estructura de un SGU
- Análisis de los requisitos de gestión y de seguridad
  - Requisitos de la norma ISO/IEC 27001:2013
  - Requisitos de la norma ISO/IEC 27002:2013
  - Requisitos de la norma UNE-EN ISO 9001:2008
  - Requisitos del ENS
  - Requisitos de la LOPD
- Establecimiento de los alcances de cada SGU
- Definición de la documentación necesaria
  - Identificación de la documentación requerida
  - Identificación de la documentación existente
  - Identificación de los documentos a crear/modificar/borrar
- Elaboración de los documentos (comunes y particulares)
- Implantación de cada SGU
- Certificación de cada SGU



## Características del proyecto

### CUESTIONES EXTERNAS

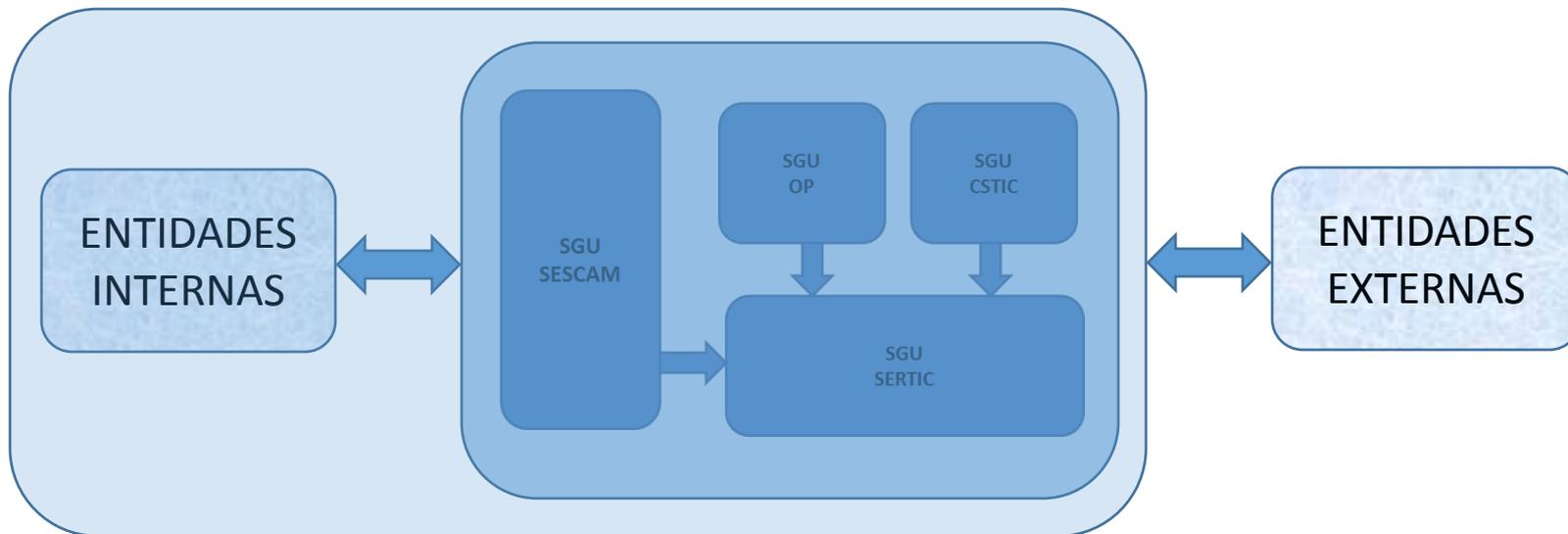
- Crisis económica
- Consolidación de servicios TIC (implantar SGU en un entorno **MUY cambiante**)
- Muchos órganos gestores implicados
- Resistencia al cambio

### CUESTIONES INTERNAS

- Comité Técnico de Seguridad de la Información: personal del Servicio de Seguridad y Protección de Datos, Organismo Pagador, DGTNT y SESCOAM: **Recursos internos**
- Marco de controles seleccionado: **ENS** (obligado cumplimiento).
- Sistema de Gestión sencillo y mantenible
- Calendario: 2014-2017

## Características del proyecto

Relaciones entre SGUs y con terceros (internos y externos)



# Características del proyecto

## Declaraciones de aplicabilidad

Declaración de aplicabilidad del SGU de .....			
COD	CONTROL	APLICA	COMPETENCIA
org.1	Política de seguridad	-	-
org.2	Normativa de seguridad	-	-
org.3	Procedimientos de seguridad	-	-
org.4	Proceso de autorización	-	-
op.pl.1	Análisis de riesgos	-	-
op.pl.2	Arquitectura de seguridad	-	-
op.pl.3	Adquisición de nuevos componentes	-	-
op.pl.4	Dimensionamiento/Gestión de capacidades	-	-
op.aoc.1	Identificación	-	-
op.aoc.2	Requisitos de acceso	-	-
op.aoc.3	Segregación de funciones y tareas	-	-
op.aoc.4	Proceso de gestión de derechos de acceso	-	-
op.aoc.5	Mecanismo de autenticación	-	-
op.aoc.6	Acceso local	-	-
op.aoc.7	Acceso remoto	-	-
op.exp.1	Inventario de activos	-	-
op.exp.2	Configuración de seguridad	-	-
op.exp.3	Gestión de la configuración	-	-
op.exp.4	Mantenimiento	-	-
op.exp.5	Gestión de cambios	-	-
op.exp.6	Protección frente a código dañinos	-	-
op.exp.7	Gestión de incidencias	-	-
op.exp.8	Registro de la actividad de los usuarios	-	-
op.exp.9	Registro de la gestión de incidencias	-	-
op.exp.10	Protección de los registro de actividad	-	-

Declaración de aplicabilidad del SGU de .....			
COD	CONTROL	APLICA	COMPETENCIA
org.1	Política de seguridad	-	-
org.2	Normativa de seguridad	-	-
org.3	Procedimientos de seguridad	-	-
org.4	Proceso de autorización	-	-
op.pl.1	Análisis de riesgos	-	-
op.pl.2	Arquitectura de seguridad	-	-
op.pl.3	Adquisición de nuevos componentes	-	-
op.pl.4	Dimensionamiento/Gestión de capacidades	-	-
op.aoc.1	Identificación	-	-
op.aoc.2	Requisitos de acceso	-	-
op.aoc.3	Segregación de funciones y tareas	-	-
op.aoc.4	Proceso de gestión de derechos de acceso	-	-
op.aoc.5	Mecanismo de autenticación	-	-
op.aoc.6	Acceso local	-	-
op.aoc.7	Acceso remoto	-	-
op.exp.1	Inventario de activos	-	-
op.exp.2	Configuración de seguridad	-	-
op.exp.3	Gestión de la configuración	-	-
op.exp.4	Mantenimiento	-	-
op.exp.5	Gestión de cambios	-	-
op.exp.6	Protección frente a código dañinos	-	-
op.exp.7	Gestión de incidencias	-	-
op.exp.8	Registro de la actividad de los usuarios	-	-
op.exp.9	Registro de la gestión de incidencias	-	-
op.exp.10	Protección de los registro de actividad	-	-

Declaración de aplicabilidad del SGU de .....			
COD	CONTROL	APLICA	COMPETENCIA
org.1	Política de seguridad	-	-
org.2	Normativa de seguridad	-	-
org.3	Procedimientos de seguridad	-	-
org.4	Proceso de autorización	-	-
op.pl.1	Análisis de riesgos	-	-
op.pl.2	Arquitectura de seguridad	-	-
op.pl.3	Adquisición de nuevos componentes	-	-
op.pl.4	Dimensionamiento/Gestión de capacidades	-	-
op.aoc.1	Identificación	-	-
op.aoc.2	Requisitos de acceso	-	-
op.aoc.3	Segregación de funciones y tareas	-	-
op.aoc.4	Proceso de gestión de derechos de acceso	-	-
op.aoc.5	Mecanismo de autenticación	-	-
op.aoc.6	Acceso local	-	-
op.aoc.7	Acceso remoto	-	-
op.exp.1	Inventario de activos	-	-
op.exp.2	Configuración de seguridad	-	-
op.exp.3	Gestión de la configuración	-	-
op.exp.4	Mantenimiento	-	-
op.exp.5	Gestión de cambios	-	-
op.exp.6	Protección frente a código dañinos	-	-
op.exp.7	Gestión de incidencias	-	-
op.exp.8	Registro de la actividad de los usuarios	-	-
op.exp.9	Registro de la gestión de incidencias	-	-
op.exp.10	Protección de los registro de actividad	-	-
op.exp.11	Protección de claves criptográficas	-	-
op.ext.1	Contratación y acuerdos de nivel de servicio	-	-
op.ext.2	Gestión diaria	-	-

## Características del proyecto

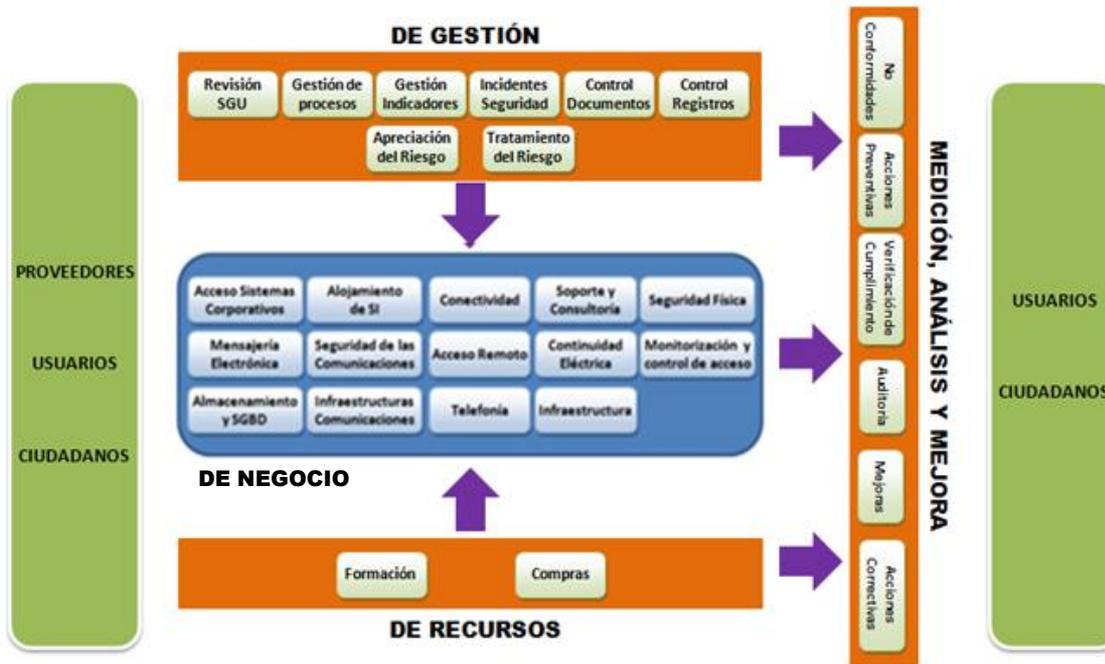
### Declaración de aplicabilidad

Declaración de aplicabilidad del Sistema de Gestión Unificado de SERTIC			
COD	CONTROL	APLICA	COMPETENCIA
org.1	Política de seguridad	S	S
org.2	Normativa de seguridad	S	N

- S / S:
  - Solo competencia del órgano gestor: implementar control
  - Competencia de varios órganos gestores: implementar control y establecer acuerdo interno
- S / N: identificar al órgano competente y establecer acuerdo interno

# Sistema de Gestión certificado

Esquema del Sistema de Gestión Seguridad de la Información y Calidad de SERTIC



## Sistema de Gestión certificado

### DOCUMENTACIÓN EXTERNA:

#### Legislación aplicable

- Decreto 57/2012, de 23 de febrero de 2012, por el que se establece la **Política de Seguridad** de la Información en la Administración de la Junta de Comunidades de Castilla-La Mancha
- Decreto 69/2012, de 29/03/2012, por el que se regulan las actuaciones sobre **Calidad de los Servicios** públicos en la Junta de Comunidades de Castilla-La Mancha
- Orden 11/07/2012, de la Consejería de Presidencia y Administraciones Públicas y de la Consejería de Fomento, por la que se aprueba la instrucción sobre el **uso aceptable de medios tecnológicos** en la Administración de la Junta de Comunidades de Castilla-La Mancha

.....

#### Normativas de la Dirección General de Función Pública

- Directrices de Seguridad de la Información
- Normas de Clasificación de la Información
- Normativa de Desarrollo Seguro de aplicaciones
- Creación y Uso de Contraseñas de usuarios
- Seguridad de la Información y la protección de datos en la prestación de servicios por terceros
- Normas de Seguridad y Protección de Datos para usuarios de Teletrabajo

.....

# Sistema de Gestión certificado

## DOCUMENTACIÓN INTERNA:

### Por requisito de la Norma ISO/IEC27001

- Proceso de apreciación del riesgo
- Proceso de tratamiento de riesgos
- Objetivos de seguridad y Calidad
- Proceso de auditoría
- Proceso de revisión del SGU

.....

### Por requisito de la Norma ISO 9001

- Listado de documentación del SGU
- Objetivos de calidad
- Mapa de procesos
- Procedimiento de control de documentos
- Procedimiento de control de registros
- Procedimiento de no conformidades
- Procedimiento de acciones correctivas

.....

MANUAL		EDICIÓN UNIFICADA
Sistema de Gestión Unificado del SERTEC		Código: SGC-SGU-UNIF-001 Versión: 01 Fecha: 15/09/2015
<b>ÍNDICE</b>		
<b>1. INTRODUCCIÓN</b> .....		6
1.1 Objeto.....		6
1.2 Alcance.....		6
1.3 Referencias: Acrónimos.....		6
1.3.1 Definiciones.....		6
1.3.2 Acrónimos.....		7
<b>2. REFERENCIAS</b> .....		8
<b>3. CONSIDERACIONES GENERALES</b> .....		9
3.1 Confidencialidad del Manual.....		9
3.2 Normas de referencia.....		9
3.3 Gestión del Manual.....		10
3.4 Mapa de procesos del SGU.....		10
<b>4. SISTEMA DE GESTIÓN UNIFICADO</b> .....		12
4.1 Requisitos generales.....		12
4.2 Contexto del sistema de gestión.....		12
4.2.1 Comprensión de la organización y su contexto.....		12
4.2.1.1 Entorno interno.....		13
4.2.1.2 Entorno externo.....		13
4.2.2 Comprensión de las necesidades y expectativas de las partes interesadas.....		14
4.2.3 Determinación del alcance del sistema de gestión de seguridad de la información.....		15
4.2.3.1 Relaciones con órganos internos y la Administración.....		16
4.2.3.2 Relaciones con órganos externos y la Administración.....		16
4.3 Requisitos del sistema de gestión.....		16
4.3.1 Generalidades.....		16
4.3.2 Manual del SGU.....		17
4.3.3 Control de los documentos.....		17
4.3.4 Control de los registros.....		19
<b>5. RESPONSABILIDADES DE LA DIRECCIÓN</b> .....		19
5.1 Compromiso de la Dirección.....		19
5.2 Política del riesgo.....		19
5.3 Partes interesadas más relevantes.....		19
5.3.1 Usuarios.....		19
5.3.2 Empresas externas.....		20
5.3.3 Clientes.....		20
5.4 Políticas.....		20
5.5 Planificación.....		21
5.5.1 Objetivos de la Calidad y de la Seguridad.....		21
5.5.2 Planificación del SGU.....		21
5.6 Recursos, autoridad y comunicación.....		21
5.6.1 Responsabilidad y autoridad.....		21
5.6.1.1 Responsabilidad.....		21
5.6.1.2 Responsabilidad en el SISTEMA DE GESTIÓN UNIFICADO.....		21

# Sistema de Gestión certificado

## DOCUMENTACIÓN INTERNA:

### Marco de controles seleccionados (ENS + ISO/IEC 27002)

- Política de seguridad
- Procedimiento de gestión de incidencias
- Procedimiento de desarrollo de aplicaciones
- Procedimiento de gestión de cambios
- Procedimiento de gestión de usuarios
- Procedimiento de auditoria

.....



# Sistema de Gestión certificado

## Declaración de aplicabilidad de SERTIC

COD	Control	A	C	Documentación	Relación con ISO 27000
org.1	Política de seguridad	S	S	- Decreto 57/2012, Política de Seguridad de la Información JCCM - SPD-SBG-SGOP-MAN-001 Manual del Sistema de Gestión Unificado	[27001] 4 Contexto de la organización 5.2 Política 5.3 Roles, responsabilidades y autoridad
				- Decreto 57/2012, Política de Seguridad de la Información JCCM - SPD-SBG-SGOP-MAN-001 Manual del Sistema de Gestión Unificado - DPS003-Estructura y Funciones SIOP	6.1.1 Roles y responsabilidades en seguridad de la información
				- SPD-SBG-SGU-PRO-008 Identificación de Legislación aplicable - SPD-SBG-SGOP-DO C-006 Listado de documentación del SGU	18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
org.2	Normativa de seguridad	S	S	- Decreto 57/2012, Política de Seguridad de la Información JCCM - SPD-SBG-SGOP-MAN-01 Manual del Sistema de Gestión Unificado - SPD-SBG-NOR-002 Directrices de Seguridad de la Información	5.1.1 Políticas para la seguridad de la información
				- Decreto 57/2012, Política de Seguridad de la Información JCCM - SPD-SBG-NOR-002 Directrices de Seguridad de la Información - SPD-SBG-SGOP-MAN-001 Manual del Sistema de Gestión Unificado - SPD-SBG-SGU-FRR-006 Verificación de Cumplimiento - SPD-AUD-PRO-001 Auditoría Interna	5.1.2 Revisión de las políticas para la seguridad de la información
				- SCPO23 Procedimiento para el conocimiento y actualización en temas de seguridad - Contacto con grupos de Interés	6.1.4 Contacto con grupos de interés especial
				- Decreto 57/2012, Política de Seguridad de la Información JCCM - SPD-SBG-SGOP-MAN-001 Manual del Sistema de Gestión Unificado - SPD-SBG-NOR-002 Directrices de Seguridad de la Información - Orden de 11/07/2012, sobre el uso aceptable de medios tecnológicos en la JCCM	8.1.3 Uso aceptable de los activos
				- Orden de 11/07/2012, sobre el uso aceptable de medios tecnológicos en la JCCM - SPD-SBG-NOR-002 Directrices de Seguridad de la Información	9.1.2 Política de uso de los servicios de red
				- Decreto 57/2012, Política de Seguridad de la Información JCCM - SPD-SBG-SGOP-MAN-001 Manual del Sistema de Gestión Unificado - SPD-SBG-NOR-002 Directrices de Seguridad de la Información - Orden de 11/07/2012, sobre el uso aceptable de medios tecnológicos en la JCCM - SPD-GEN-INS-001 Seguridad y Protección de Datos en la prestación de servicios con terceros	13.2.1 Políticas y procedimientos de intercambio de información
				- Decreto 57/2012, Política de Seguridad de la Información JCCM - SPD-SBG-SGOP-MAN-001 Manual del Sistema de Gestión Unificado - SPD-GEN-INS-001 Seguridad y Protección de Datos en la prestación de servicios con terceros - SPD-SBG-NOR-002 Directrices de Seguridad de la Información	15.1.1 Política de seguridad de la información en las relaciones con los proveedores

# Sistema de Gestión certificado

## Comprobación de la no omisión de controles

Controles ISO 27002		Relación ENS	Observaciones
<b>5 Políticas de seguridad</b>			
<b>5.1 Directrices de gestión de la seguridad de la información</b>			
Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas pertinentes.			
5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	<ul style="list-style-type: none"> <li>• [org.1] Política de seguridad</li> <li>• [org.2] Normativa de seguridad</li> </ul>
5.1.2	Revisión de las políticas de seguridad de la información	Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	• Las políticas/normativas se revisan acorde a lo establecido en los Sistemas de Gestión correspondientes.
<b>6 Organización de la seguridad de la información</b>			
<b>6.1 Organización interna</b>			
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			
6.1.1	Roles y responsabilidades en seguridad de la información	Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	<ul style="list-style-type: none"> <li>• [org.1] Política de seguridad</li> <li>• [org.4] Proceso de autorización</li> </ul>
6.1.2	Segregación de tareas	Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	• [op.acc.3] Segregación de funciones y tareas
6.1.3	Contacto con las autoridades	Deben mantenerse los contactos apropiados con las autoridades pertinentes.	<ul style="list-style-type: none"> <li>• [org.3] Procedimientos de seguridad</li> <li>• [op.exp.7] Gestión de incidencias</li> </ul>
6.1.4	Contacto con grupos de interés especial	Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros, y asociaciones profesionales especializadas en seguridad.	<ul style="list-style-type: none"> <li>• [org.2] Normativa de seguridad de seguridad</li> <li>• [op.exp.7] Gestión de incidencias</li> </ul>
6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe tratarse en la gestión de proyectos, independientemente de la naturaleza del proyecto.	Se refiere la norma a que todos los proyectos acometidos por la organización tengan en cuenta la seguridad de la información. Puede decirse que en el ENS este aspecto aparece de forma implícita al ser obligatoria su aplicación a toda información y servicio relacionado con la Ley 11/2007.
<b>6.2 Los dispositivos móviles y el teletrabajo</b>			
Objetivo: Garantizar la seguridad en el teletrabajo y en el uso seguro de dispositivos móviles.			
6.2.1	Política de dispositivos móviles	Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	<ul style="list-style-type: none"> <li>• [org.4] Proceso de autorización</li> <li>• [mp.eq.3] Protección de equipos portátiles</li> </ul>

### Certificado del Sistema de Gestión de la Calidad



**ER-0276/2008**

AENOR, Asociación Española de Normalización y Certificación, certifica que la organización

#### JUNTA DE COMUNIDADES DE CASTILLA LA MANCHA

Consejería de Hacienda y Administraciones Públicas - Dirección General de Función Pública

dispone de un sistema de gestión de la calidad conforme con la Norma ISO 9001:2008

para las actividades: la prestación de servicios comunes de Tecnología de la Información y Comunicaciones (TIC) a la Administración Regional y al ciudadano en infraestructura software, gestión de contenidos, infraestructura cpd y comunicaciones, así como los activos en los que se soportan.

que se realizan en: CONSEJERÍA DE FOMENTO, Dirección General de Telecomunicaciones y Nuevas Tecnologías. AVDA ESTERILLA, S/N. 45071 - TOLEDO

Fecha de primera emisión: 2008-01-15  
Fecha de última emisión: 2015-07-30  
Fecha de expiración: 2016-09-08



Aurora ESPIDO MARQUENA  
Directora General de AENOR



Asociación Española de Normalización y Certificación



ENTIDAD NACIONAL DE ACREDITACIÓN



INSTITUTO COOPERATIVO DE NORMALIZACIÓN

### Certificado del Sistema de Gestión de Seguridad de la Información



**SI-0025/2008**

AENOR, Asociación Española de Normalización y Certificación, certifica que la organización

#### JUNTA DE COMUNIDADES DE CASTILLA LA MANCHA

Consejería de Hacienda y Administraciones Públicas - Dirección General de Función Pública

dispone de un sistema de gestión de seguridad de la información conforme con la Norma UNE-AENOR 27001:2011

para las actividades: Los sistemas de información que soportan los procesos de registro de servicios comunes de tecnología de la información y comunicaciones (TIC) a la Administración Regional y al ciudadano, en infraestructura software, gestión de contenidos, infraestructura cpd y comunicaciones, así como los activos en los que se soportan, de acuerdo al documento de aplicabilidad vigente.

que se realizan en: CONSEJERÍA DE FOMENTO, Dirección General de Telecomunicaciones y Nuevas Tecnologías. AVDA ESTERILLA, S/N. 45071 - TOLEDO

Fecha de primera emisión: 2008-01-15  
Fecha de última emisión: 2015-07-30  
Fecha de expiración: 2016-09-08



Aurora ESPIDO MARQUENA  
Directora General de AENOR



Asociación Española de Normalización y Certificación



ENTIDAD NACIONAL DE ACREDITACIÓN



INSTITUTO COOPERATIVO DE NORMALIZACIÓN

### Certificado de Conformidad Esquema Nacional de Seguridad



**ENS-0004/2015**

AENOR, Asociación Española de Normalización y Certificación, certifica que la organización

#### JUNTA DE COMUNIDADES DE CASTILLA LA MANCHA

Consejería de Hacienda y Administraciones Públicas  
Dirección General de Función Pública

dispone de un sistema de seguridad de la información conforme con la Norma UNE-ISO/IEC 27002:2014 que cumple con los requisitos establecidos en el ANEXO II del Real Decreto 1631/2010, de 8 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

para las actividades: La prestación de servicios comunes de Tecnología de la Información y Comunicaciones (TIC) a la Administración regional y al ciudadano, en infraestructura software, gestión de contenidos, infraestructura CPD y comunicaciones, así como los activos en los que se soportan, de acuerdo con la categorización del sistema vigente.

que se realizan: CONSEJERÍA DE FOMENTO, DIRECCIÓN GENERAL DE TELECOMUNICACIONES Y NUEVAS TECNOLOGÍAS, AVDA. RIO ESTERILLA, S/N. 45071 TOLEDO

Fecha de primera emisión: 2015-07-30  
Fecha de expiración: 2016-07-30



Aurora ESPIDO MARQUENA  
Directora General de AENOR



Asociación Española de Normalización y Certificación



ENTIDAD NACIONAL DE ACREDITACIÓN



INSTITUTO COOPERATIVO DE NORMALIZACIÓN

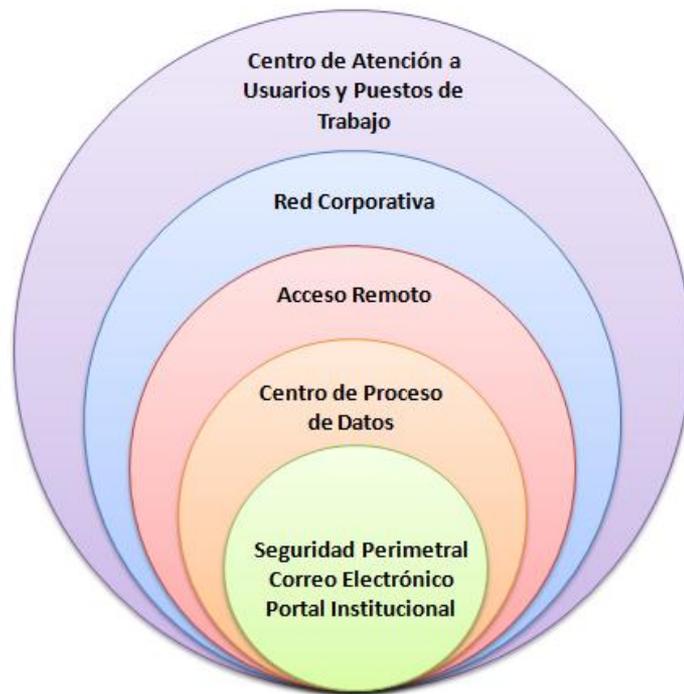
Equipo Humano

**Claves de éxito**



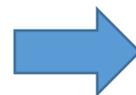
## Claves de éxito

Ampliación progresiva de alcances



## Claves de éxito

### Plan de formación de la Escuela de Administración Regional



**11.985 empleados públicos**

### Concienciación sobre Seguridad de la Información



## Siguientes pasos

### Certificación del Sistema de Gestión de Organismo Pagador

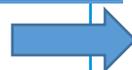
L 255/18 ES Diario Oficial de la Unión Europea 28.8.2014

---

**REGLAMENTO DELEGADO (UE) Nº 907/2014 DE LA COMISIÓN**  
de 11 de marzo de 2014

que completa el Reglamento (UE) nº 1306/2013 del Parlamento Europeo y del Consejo en lo relativo a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro

LA COMISIÓN EUROPEA,



#### 3. INFORMACIÓN Y COMUNICACIÓN

##### A) Comunicación

El organismo pagador adoptará los procedimientos necesarios para garantizar que las modificaciones de la normativa de la Unión, y en especial las que afecten al importe de las ayudas aplicables, sean registradas y que las instrucciones, bases de datos y listas de control se actualicen a su debido tiempo.

##### B) Seguridad de los sistemas de información

i) Sin perjuicio del inciso ii) siguiente, la seguridad de los sistemas de información estará basada en los criterios fijados en una versión aplicable en el ejercicio financiero considerado de una de las siguientes normas:

- International Standards Organisation 27002: Code of practice for Information Security management (Organización internacional de normalización 27002: Código de prácticas para la gestión de la seguridad de la información) (ISO),
- Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch/IT Baseline Protection Manual (Manual de protección informática de base) (BSI),
- Information Systems Audit and Control Association: Control objectives for Information and related Technology (Asociación para la auditoría y el control de los sistemas de información: Objetivos de control para la información y tecnologías afines) (COBIT).

ii) A partir del 16 de octubre de 2016, la seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO 27001: Information Security management systems – Requirements (ISO) (Sistemas de gestión de la seguridad de la información-Requisitos) (ISO).

La Comisión podrá autorizar a los Estados miembros para certificar la seguridad de sus sistemas de información de conformidad con otras normas aceptadas si estas normas garantizan un nivel de seguridad equivalente, como mínimo, al previsto en la norma ISO 27001.

En el caso de los organismos pagadores responsables de la gestión y control de un gasto de la Unión anual superior a 400 millones EUR, el Estado miembro podrá decidir no aplicar lo dispuesto en el párrafo primero. Dichos Estados miembros seguirán aplicando las disposiciones del inciso i). Informarán a la Comisión de su decisión.

## Siguientes pasos

### Certificación del Sistema de Gestión de Organismo Pagador

**Octubre de 2015:** Decisión de la Dirección de Organismo Pagador de gestionar la Seguridad de la Información de los Sistemas de Información del Organismo Pagador mediante SGSI

#### Tareas realizadas:

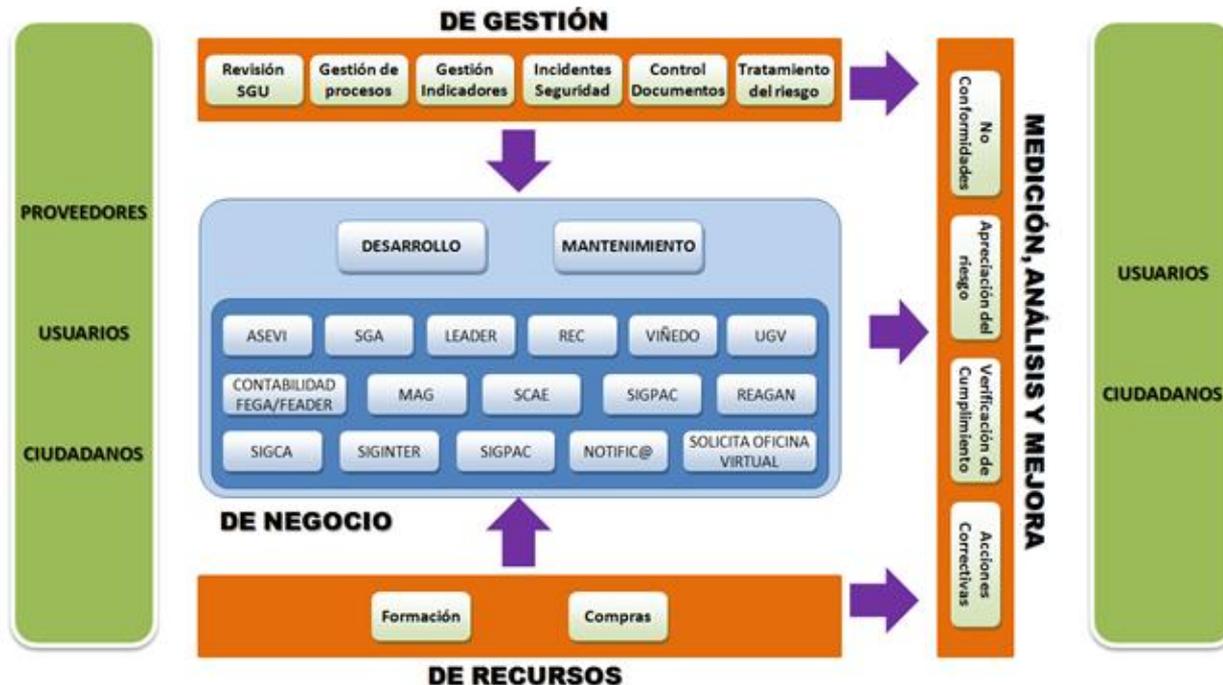
- Manual del Sistema de Gestión
- Análisis de riesgos
- Nivel de aceptación del riesgo
- Plan de Tratamiento del riesgo
- Definición de objetivos de Seguridad
- Declaración de aplicabilidad extendida
- Fichas de proceso
- Auditoria interna

.....



## Siguientes pasos

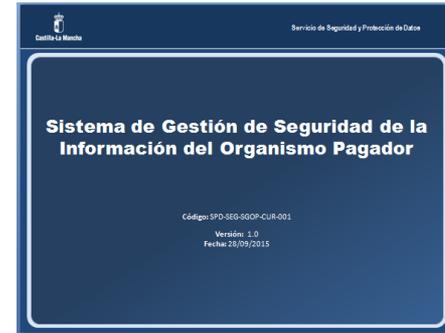
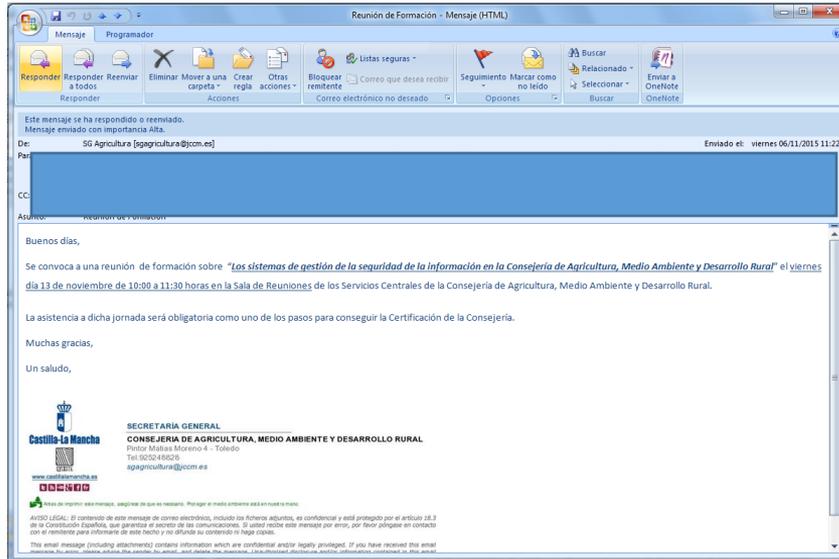
### Certificación del Sistema de Gestión de Organismo Pagador



# Siguientes pasos

Certificación del Sistema de Gestión de Organismo Pagador

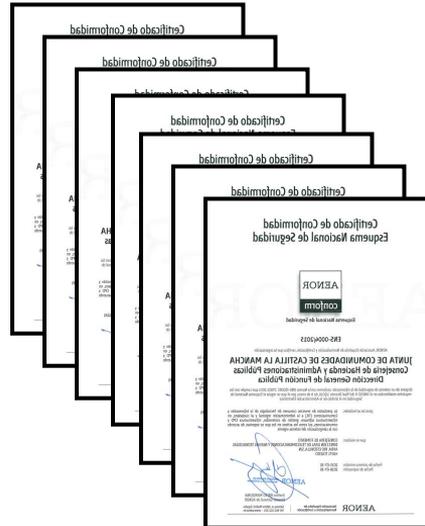
Formación sobre SGSI a jefes de área/servicio



## Sigüientes pasos

Certificación del Sistema de Gestión de Organismo Pagador

**Marzo de 2016:** Auditoria de certificación en ISO/IEC 27001 y certificado de conformidad con ENS



## ➤ E-Mails

- [info@ccn-cert.cni.es](mailto:info@ccn-cert.cni.es)
- [ccn@cni.es](mailto:ccn@cni.es)
- [sondas@ccn-cert.cni.es](mailto:sondas@ccn-cert.cni.es)
- [redsara@ccn-cert.cni.es](mailto:redsara@ccn-cert.cni.es)
- [organismo.certificacion@cni.es](mailto:organismo.certificacion@cni.es)

## ➤ Websites

- [www.ccn.cni.es](http://www.ccn.cni.es)
- [www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)
- [www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)



Síguenos en Linked in

