ISACA
Trust in, and value from, information systems
Barcelona Chapter

CONGRÉS
2017

Integrando la norma ISO 27001, o el Esquema Nacional de Seguridad (ENS), con el Reglamento General de Protección de Datos (RGPD/UE)

Sr. José Luis Colom Planas

Director Técnico (Auditoría y Cumplimiento Normativo)
en el Organismo de Certificación **AUDERTIS Audit Services.**

- Colaborador como Auditor Jefe de Certificación ISO 27001 en **British Standards (BSI).**
- Formador de Auditores Jefe en las normas ISO 27001 e ISO 22301 para cursos oficiales del **International Register of Certificated Auditors (IRCA).**
- Miembro de la Junta Directiva (Comisión de Certificación) en **INBLAC.**
- Instructor acreditado respecto al Esquema Nacional de Seguridad (ENS) en la **Diputació de Barcelona (DIBA).**
- Múltiples certificaciones: CISA, CDPP, LA ISO27001, ISO 22301, ISO 20000 PMI, Esquema Cloud CSA-STAR…

AUDERTIS

- Introducción al RGPD(UE)
- Las Evaluaciones de Impacto en la Protección de Datos (EIPD)
- Comparativa entre la norma ISO 27001 y el Esquema Nacional de Seguridad (ENS)
- Sistemas de Gestión y su integración con el RGPD.

Introducción al RGPD

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, **RGPD**

LOPD actual
LO 15/1999

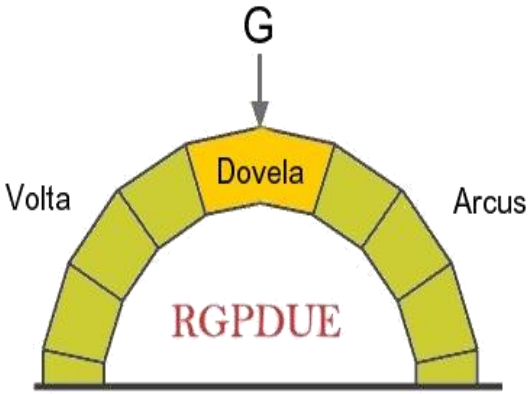
Nueva LOPD
LO 15/1999

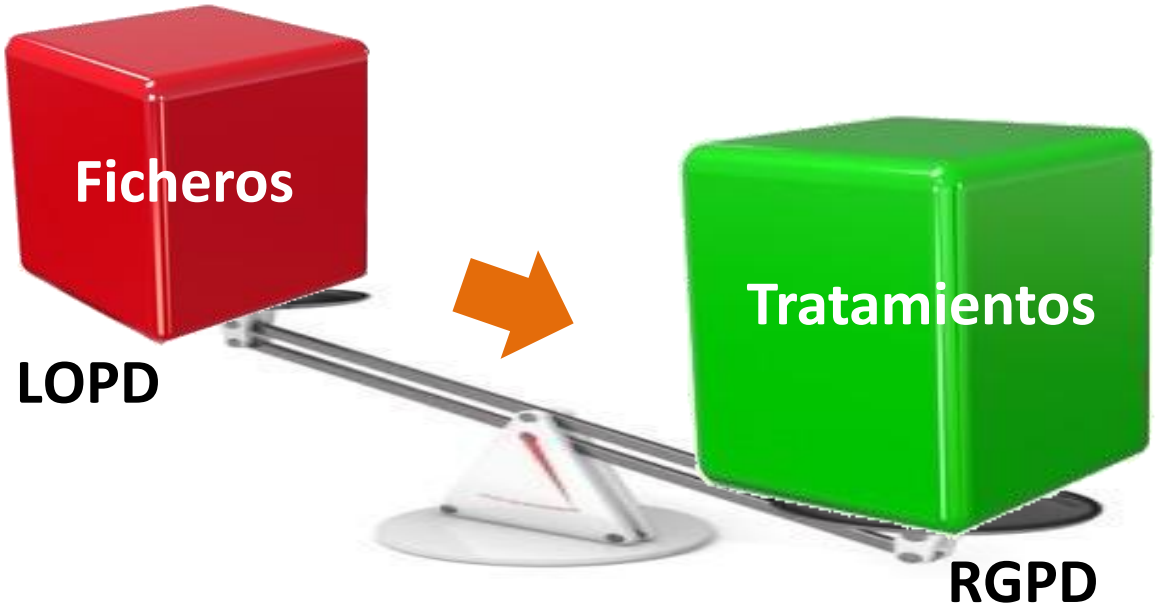
~~**RLOPD**~~
~~**RD 1720/2007**~~

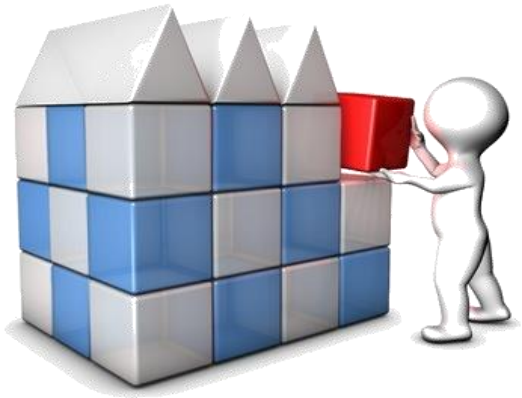
sábado, 24 de septiembre de 2016

La dovela central del Reglamento Europeo de Protección de Datos (RGPDUE)

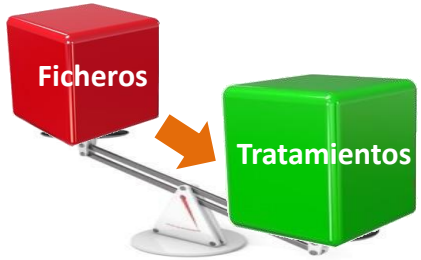
www.aspectosprofesionales.info





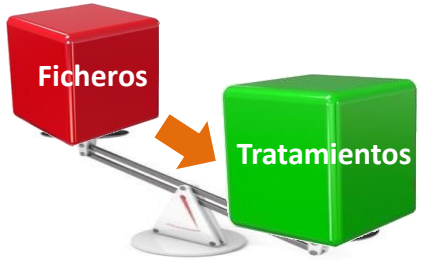


- Desaparecen los **niveles de seguridad** de los ficheros de datos.
- Desaparecen las **medidas de seguridad tasadas**.



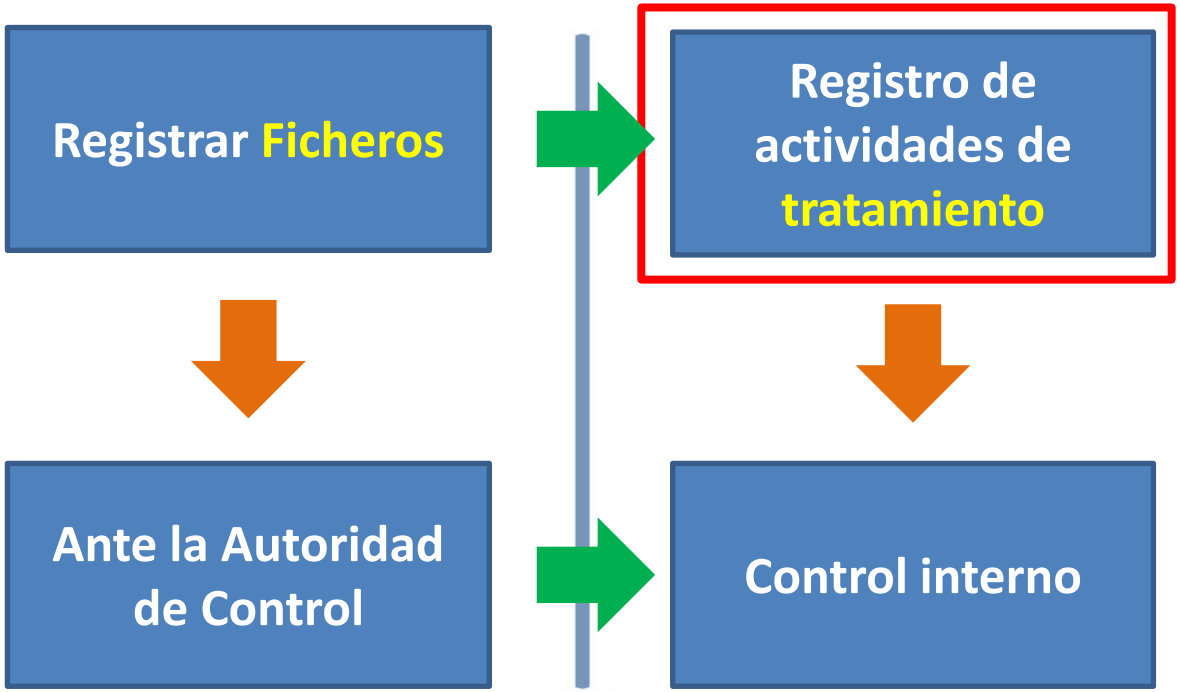
Categorías especiales de datos: origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

- Desaparecen los **niveles de seguridad** de los ficheros de datos.
- Desaparecen las **medidas de seguridad tasadas** como existían en el Capítulo III, del Título VIII, del RD 1720/2007.



Art. 32.1 RGPD sobre Seguridad del tratamiento: "*1.Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como <u>riesgos de probabilidad y gravedad variables</u> para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán <u>medidas técnicas y organizativas apropiadas</u> para garantizar un nivel de seguridad adecuado al riesgo*".

Principio de Rendición de Cuentas



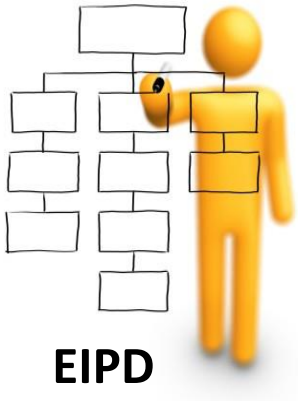
Artículo 30 RGPD. Registro de las actividades de tratamiento

- Nombre del tratamiento.
- La finalidad del tratamiento.
- La licitud (interés legítimo u otro).
- Los colectivos afectados y las categorías de datos personales.
- Datos personales tratados
- El origen de los datos
- Ficheros empleados
- Las categorías de destinatarios a quienes se comunicarán los datos personales.
- Externalización en terceros (Encargados del tratamiento)
- TID y documentos de garantía.
- Plazos previstos para la supresión.
- Descripción general de las medidas de seguridad.
- Tecnologías utilizadas, si procede:
  - Equipos que intervienen en el tratamiento.
  - Propios o de terceros.

Las Evaluaciones de Impacto en la Protección de Datos (EIPD)

Evaluaciones de Impacto en la Protección de Datos (EIPD)

REGISTRO DE ACTIVIDADES DE TRATAMIENTO (de datos personales)



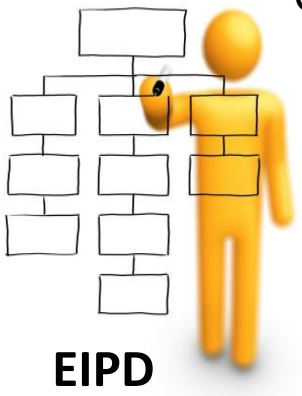
EIPD

ACCIONES DE TRATAMIENTO (mitigar riesgos evaluados como inaceptables)

Evaluaciones de Impacto en la Protección de Datos (EIPD)

REGISTRO DE ACTIVIDADES DE TRATAMIENTO (de datos personales)

Gestión de Riesgos



EIPD

ACCIONES DE TRATAMIENTO (mitigar riesgos evaluados como inaceptables)

Evaluaciones de Impacto en la Protección de Datos (EIPD)

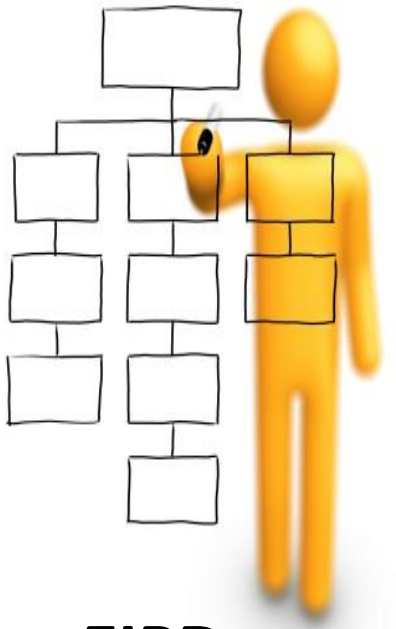
ACTIVIDAD DE TRATAMIENTO #01 X

ACTIVIDAD DE TRATAMIENTO #02 →

ACTIVIDAD DE TRATAMIENTO #03 X

ACTIVIDAD DE TRATAMIENTO #04 X

ACTIVIDAD DE TRATAMIENTO #05 →



EIPD

Gestión de Riesgos según la norma ISO 31000:2009

SandaS GRC | ElevenPaths | Sandas GRC | SandaS GRC

Evaluación Impacto
- Listado de Evaluaciones

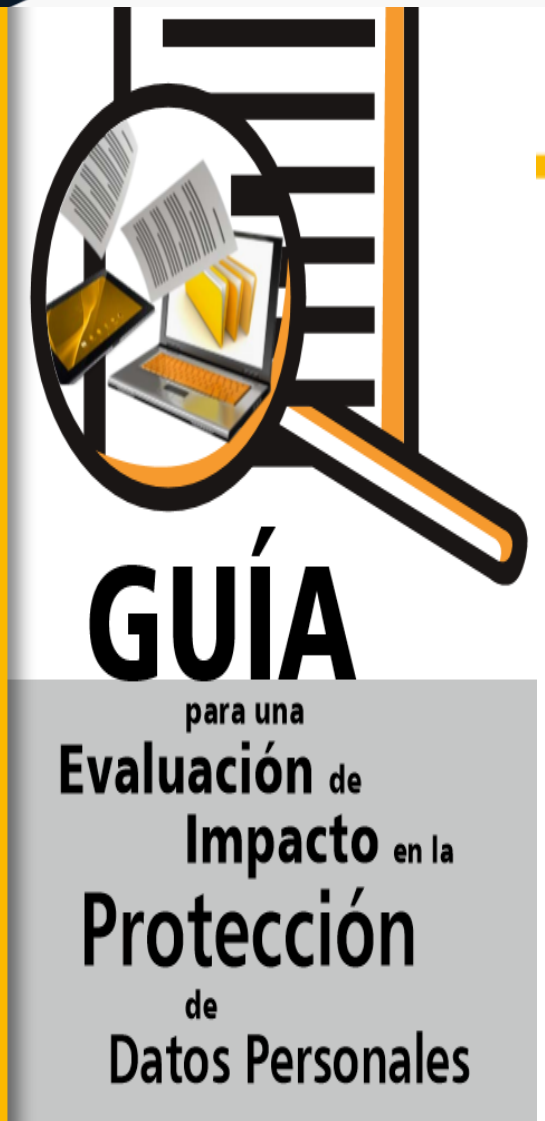
Personalización
- Escalas
- Criterios de Impacto
- Matrices de Riesgo

Resumen

Evaluaciones de Impacto en Protección de Datos. Tratamiento del Riesgo

1. Datos Generales | 2. Tratamientos Incluidos | 3. Comité de Gestión del Riesgo | 4. Flujos de Datos | 5. Identificación de Escenarios de Riesgo | 6. Análisis del Riesgo | 7. Consultas | 8. Tratamiento del Riesgo | 9. Informe | 10. Consultas Autoridad de Control | 11. Revisión y Auditoría

Código	Escenario de Riesgo	Frecuencia Inicial	Impacto Inicial	Riesgo Inicial	Frecuencia Residual	Impacto Residual	Riesgo Residual	Acción
RGPDUE-GEN.R.UE.28.3.1.	El tratamiento de datos por encargado no se rige por contrato u otro acto jurídico con arreglo a Derecho de la Unión de Estados Miembros	>= 100 veces al año	Muy Alto	Muy Alto	>= 100 veces al año	Muy Alto	Muy Alto	Mitigar
RGPDUE-GEN.R.UE.28.2.1.	El encargado de tratamiento ha nombrado otro encargado sin autorización del responsable	>= 10 veces al año	Alto	Alto	>= 10 veces al año	Alto	Alto	Evitar
RGPDUE-GEN.R.UE.13.2.a - GEN	No informar del plazo de conservación de los datos o, cuando no sea posible los criterios utilizados para determinar ese plazo	>= 1 vez al año	Muy Alto	Alto	>= 1 vez al año	Muy Alto	Alto	Aceptar
RGPDUE-GEN.R.UE.28.1.1.	El responsable del tratamiento no ha elegido un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas	>= 1 vez al año	Medio	Medio	>= 1 vez al año	Medio	Medio	Mitigar
RGPDUE-GEN.R.UE.06.01	Tratamiento ilícito (incumpliendo las	<= 1 vez			<= 1 vez			Aceptar



17. ANEXO III. MODELO DE INFORME FINAL DE UNA EIPD

[1] a [5]

[6] Identificación y gestión de riesgos

III. **Gestión de los riesgos**: decisión adoptada para cada riesgo, objetivos de control, controles y medidas propuestas.

[7] Análisis de cumplimiento normativo

[8] Conclusiones

III. **Medidas técnicas** que deben adoptarse en el diseño del proyecto para eliminar o evitar, mitigar, transferir o aceptar los riesgos para la privacidad

IV. **Medidas organizativas** que deben adoptarse en el diseño del proyecto para eliminar o evitar, mitigar, transferir o aceptar los riesgos para la privacidad.

Comparativa entre la norma ISO 27001:2013 y el Esquema Nacional de Seguridad (ENS)

ISO 27001:2013

- Cláusulas
- Anexo A
  - Dominios de Control
    - Objetivos de Control
      - Controles (114)

RD 3/2010 (ENS)

- Artículos
- Anexo II
  - Grupos: Marco organizativo, marco operacional y medidas de protección)
    - Subgrupos
      - Medidas de seguridad (75)

ISO 27001

Anexo A: 14 Dominios, 35 objetivos de control y 114 controles

- A.5 Políticas de seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad relativa a los recursos humanos
- A.8 Gestión de activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y del entorno
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas de información
- A.15 Relación con proveedores
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio
- A.18 Cumplimiento

ENS RD 3/2010

Anexo II: 3 Grupos, 14 subgrupos y 75 medidas de seguridad

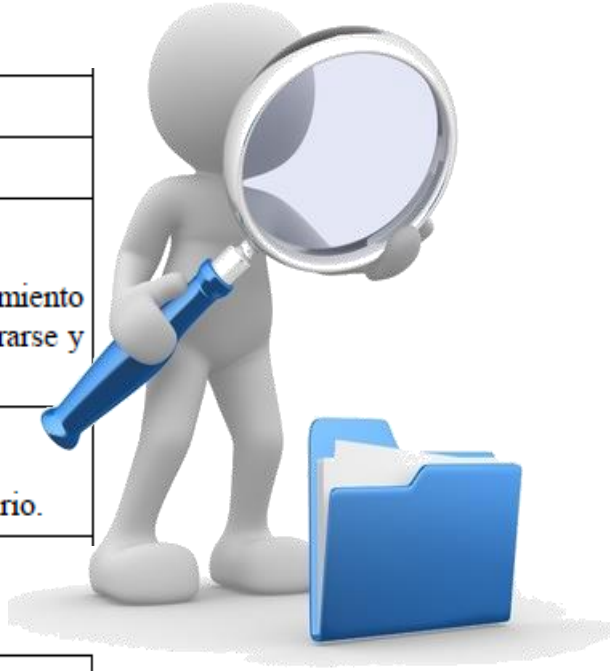
- **MARCO ORGANIZATIVO**

- **MARCO OPERACIONAL**
  - Planificación
  - Control de acceso
  - Explotación
  - Servicios externos
  - Continuidad del servicio
  - Monitorización del sistema

- **MEDIDAS DE PROTECCIÓN**
  - Protección de las instalaciones e infraestructuras
  - Gestión del personal
  - Protección de los equipos
  - Protección de las comunicaciones
  - Protección de los soportes de información
  - Protección de las aplicaciones informáticas
  - Protección de la información
  - Protección de los servicios

Anexo A de la ISO 27001 (114 controles):

A.8.1 Responsabilidad sobre los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		
A.8.1.1	Inventario de activos	*Control* Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
A.8.1.2	Propiedad de los activos	*Control* Todos los activos que figuran en el inventario deben tener un propietario.



Anexo II del ENS (75 medidas de seguridad):

Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidentes
T	aplica	+	++	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidentes
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad

Análisis de riesgos ISO 27001 / ENS

SandaS GRC

Apreciación de Riesgos | Global | Crear Apreciación de Riesgos | Informes

Configuración | Cuadros de Mando | Identificación | Análisis | Evaluación | Tratamiento

Modo | Edición | Mostrar Taxonomía | 1 / 15 | Resultados 10

Activo	Código	Evento	Probabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Riesgo
Active Directory	A.07.01	Por personal interno	MA	M-	B	B	B	B	(1)
Alfresco	A.17.02	A beneficio del atacante	MR	B	B	B	B	B	(0)
Alfresco	A.18.02	A beneficio del atacante	MR	MA	M	B	B	B	(3)
Alfresco	A.19.02	A contratistas que no necesitan conocerlo	CS	MA	MA	B	B	B	(7)
Alfresco	E.14.02	A contratistas que no necesitan conocerlo	CS	MA	A	T	M	B	(9)
Almacenamiento	A.18.02	A beneficio del atacante	CS	MA	MA	MA	A	A	(6)
Almacenamiento	A.04.02	A beneficio del atacante	MR	B	B	B	B	B	(0)
Almacenamiento	E.14.02	A contratistas que no necesitan conocerlo	CS	A	MA	B	B	B	(6)
Almacenamiento	E.19.02	A contratistas que no necesitan conocerlo	MR	B	B	B	B	B	(0)

Concepto	ISO/IEC 27001:2013	ENS
Tipo de norma	Norma de adscripción **voluntaria**	Norma jurídica de **obligado cumplimiento** (RD 3/2010) para AAPP
Alcance	**Elegible por la organización**: Geográfico, departamental, procesos de negocio, servicios… (+ exclusiones).	**Predefinido**: Todos los servicios prestados a la ciudadanía que se apoyen en medios electrónicos.
Categorización	**NO** **3** dimensiones de la seguridad	**SI**, de los sistemas : BASICA, MEDIA y ALTA. **5** dimensiones de la seguridad
"Risk Approach"	**SI** Cláusulas 6.1 (Acciones para tratar los riesgos y oportunidades)	**SI** Medida de seguridad op.pl.1 (Análisis de riesgos)
Sistema de Gestión	**SI** explícito en la cláusula 4.4	**SI** según op.pl.2 (Arquitectura de seguridad) para categorías MEDIA y ALTA.
Controles	**114** controles de seguridad Anexo A	**75** medidas de seguridad Anexo II

Guía comparativa entre ISO 27001 y ENS

SIN CLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC 825)

ESQUEMA NACIONAL DE SEGURIDAD
CERTIFICACIONES 27001

NOVIEMBRE 2013

nivel	comentario
0	cubierto siempre conviene validar que se contemplan los detalles específicos del ENS
1	probablemente cubierto hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea marginal
2	probablemente se necesite completar hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea significativo
3	no cubierto son aspectos que no se cubren en los controles de la norma 27002 ni en los requisitos de la norma 27001, por lo que deberán ser objeto de una auditoría específica

Medidas de Seguridad ENS → Controles ISO 27001:2013

mp.si	Protección de los soportes de información	
mp.si.1	Etiquetado	0
mp.si.2	Criptografía	1
mp.si.3	Custodia	0
mp.si.4	Transporte	0
mp.si.5	Borrado y destrucción	0
mp.sw	Protección de las aplicaciones informáticas	
mp.sw.1	Desarrollo	0
mp.sw.2	Aceptación y puesta en servicio	1
mp.info	Protección de la información	
mp.info.1	Datos de carácter personal	0
mp.info.2	Calificación de la información	0
mp.info.3	Cifrado de la información	2
mp.info.4	Firma electrónica	3
mp.info.5	Sellos de tiempo	3
mp.info.6	Limpieza de documentos	3
mp.info.9	Copias de seguridad (backup)	0
mp.s	Protección de los servicios	
mp.s.1	Protección del correo electrónico	0
mp.s.2	Protección de servicios y aplicaciones web	3
mp.s.8	Protección frente a la denegación de servicio	3
mp.s.9	Medios alternativos	2

El concepto de Sistema de Gestión y su integración con el RGPD (Seguridad Activa)

Sistema de Gestión de la Seguridad de la Información (SGSI)

Un SGSI es aquel que permite establecer políticas, normas, procedimientos, instrucciones operativas y controles de seguridad, **alineados con los objetivos de la organización**, con el fin de mantener el riesgo de la información, de forma adaptativa, por debajo del nivel asumible.

Sistema de Gestión de la Seguridad de la Información (SGSI)

Gestión de Riesgos

Seguimiento de Acciones

Declaración de Aplicabilidad

CONTEXTO DE LA ORGANIZACIÓN

Sistema de Gestión de la Seguridad de la Información (SGSI)

Cualquier Sistema de Gestión

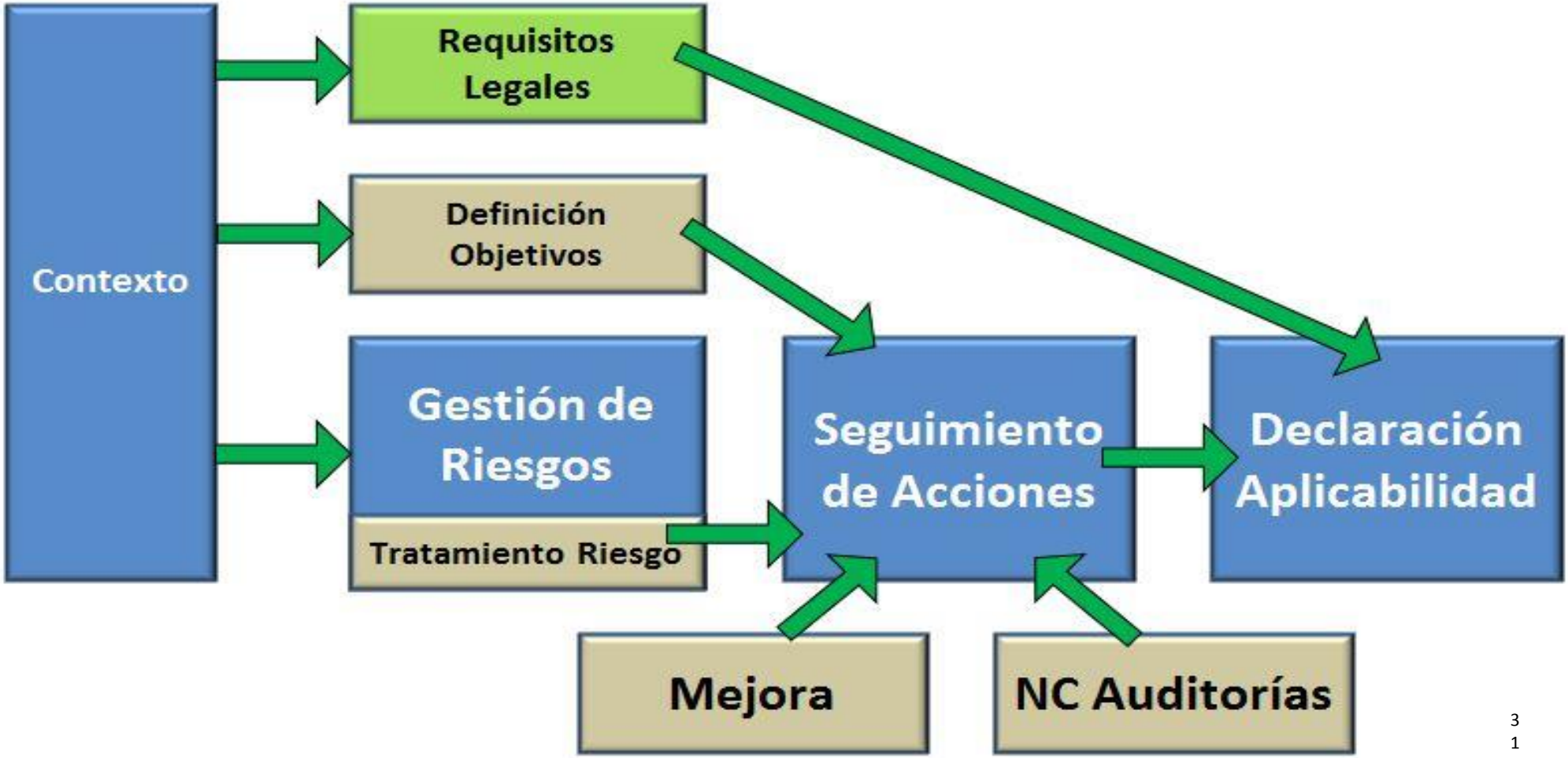
Gestión de Riesgos

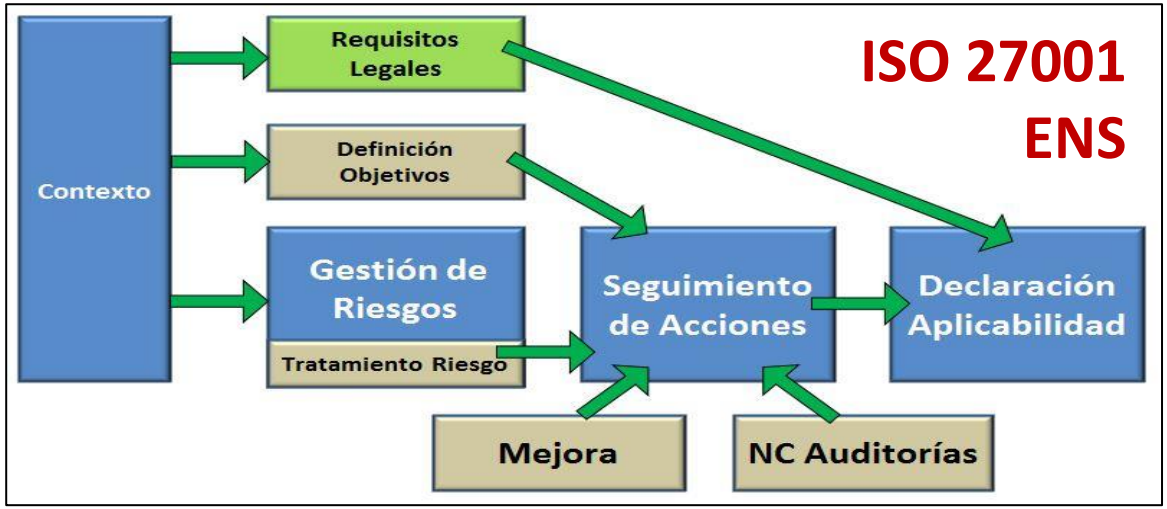
Seguimiento de Acciones

Declaración de Aplicabilidad

CONTEXTO DE LA ORGANIZACIÓN

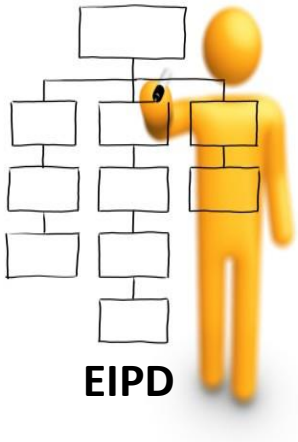
Sistema de Gestión de la Seguridad de la Información (SGSI)



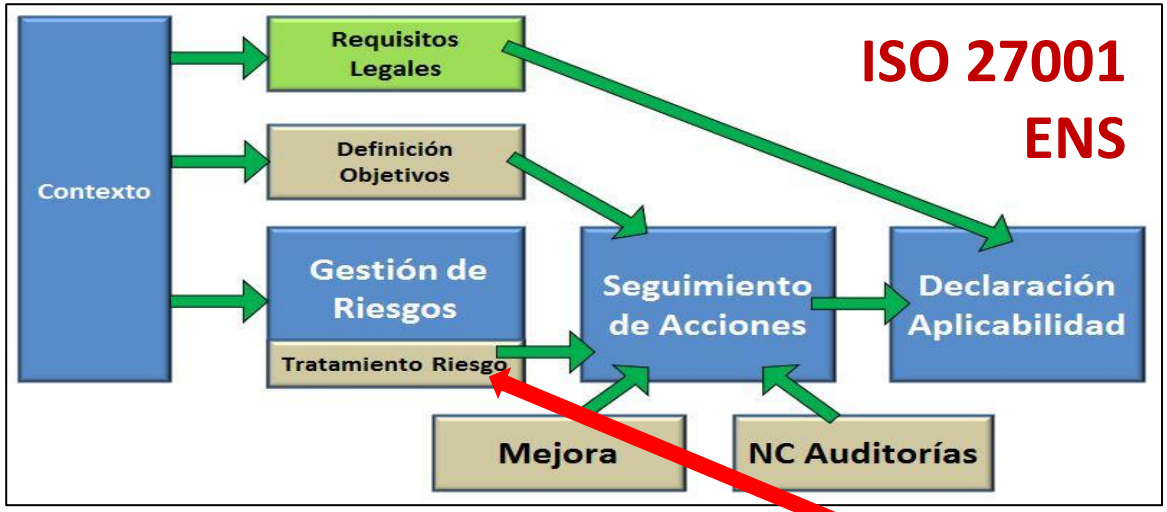


RGPD

REGISTRO DE ACTIVIDADES DE TRATAMIENTO (de datos personales)

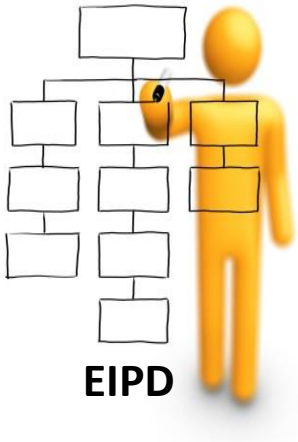


ACCIONES DE TRATAMIENTO (de los riesgos evaluados como inaceptables)



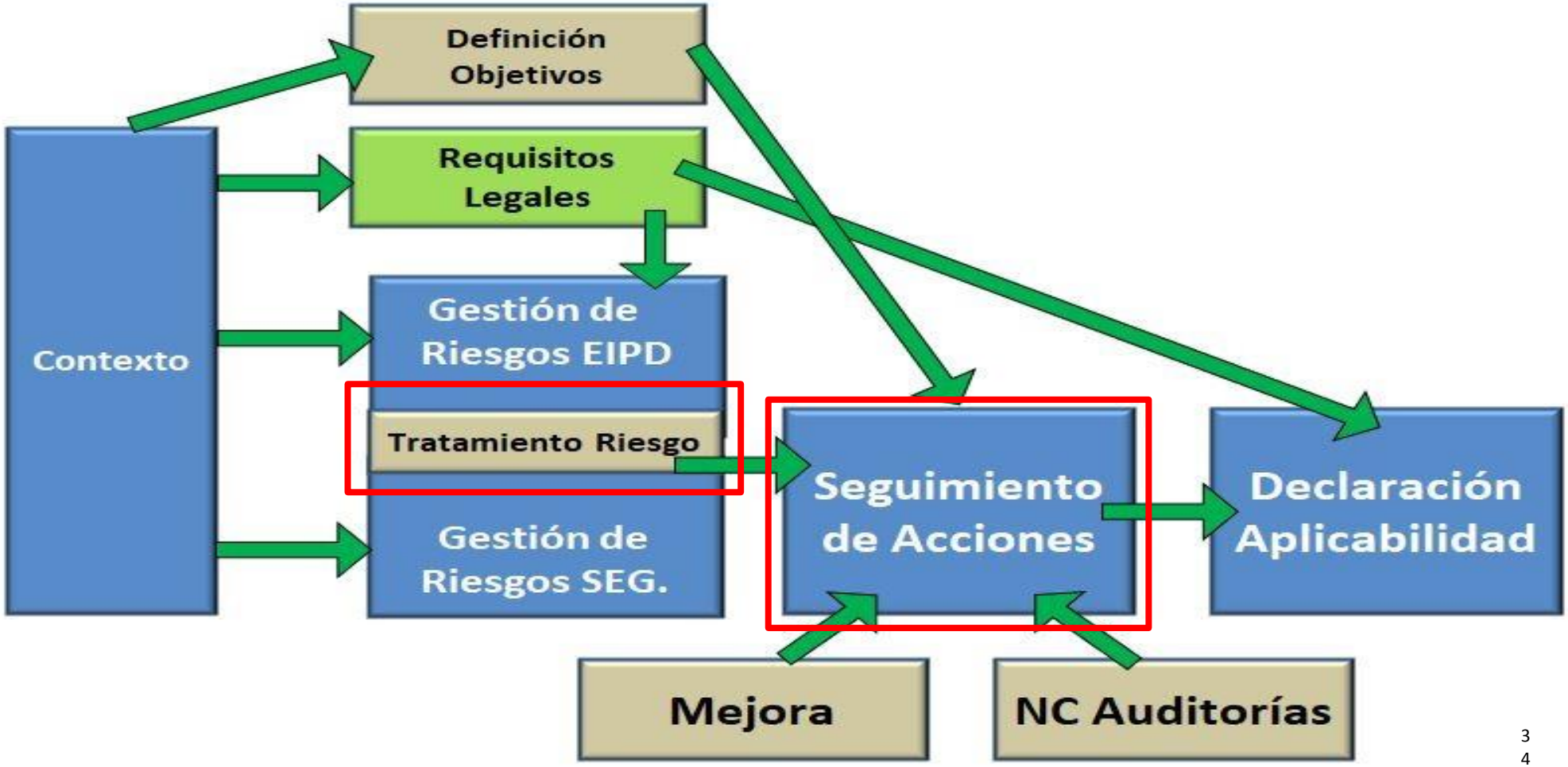
RGPD

REGISTRO DE ACTIVIDADES DE TRATAMIENTO
(de datos personales)

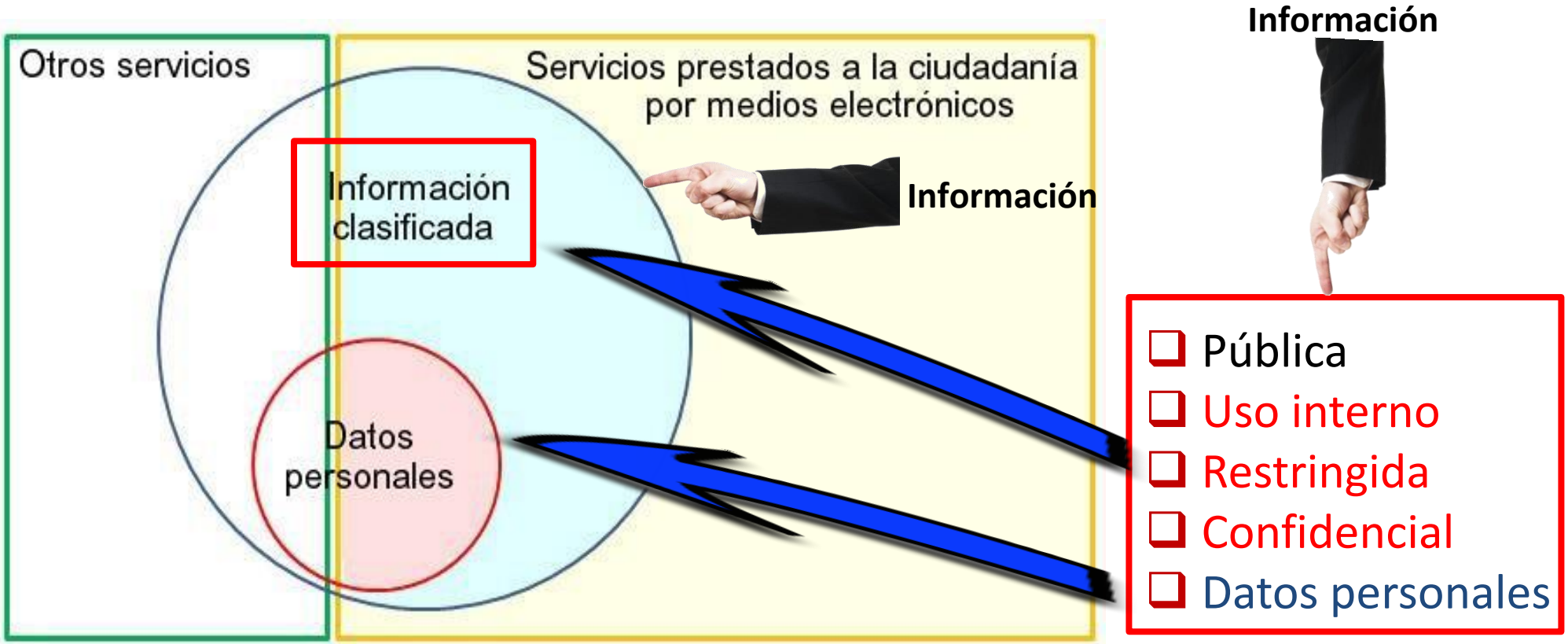


ACCIONES DE TRATAMIENTO
(de los riesgos evaluados como inaceptables)

Sistema Integrado de Gestión de Seguridad de la Información y Privacidad



Los Datos Personales son un subconjunto de la información



CONGRÉS 2017

ISACA
Trust in, and value from, information systems
Barcelona Chapter

Seguimiento de acciones del SGSI-ENS (Incluye PTR)

	A	B	C	D	E	F	G	H	I
1	Registro inicial							Evaluación de las causas y determinación de las acciones	
2–3	SG	Fecha registro	Origen	Desencadenante de la acción		Ámbito	Art./Cláusula	Identificación de la causa de la NC o de la elección del objetivo	Acciones necesarias
				Referencia	Descripción				
4	COMUN	13/10/2016	No conformidad menor	NCm01/16	Las acciones formativas que aparecen en el programa anual de formación, no tienen en cuenta los cambios en la estructura organizativa.	Formación	Art. 39.1.a) RGPD 7.2 ISO 27001 mp.per.4 ENS	Únicamente se hace una programación de la formación a principios de año, y no se revisa teniendo en cuenta los cambios en la organización que afecten a necesidades formativas de la plantilla, especialmente las nuevas incorporaciones a lo largo del año.	El área de formación formará parte del circuito de notificaciones de altas y modificaciones de la situación y funciones laborales asignadas a los empleados, para que pueda planificar sin dilación las acciones formativas y de concienciación correspondientes a cargo del DPD y del Responsable de Seguridad ENS.
5	RGPD	16/10/2017	Tratamiento de Riesgos	TR001/17	Riesgo de solicitar datos o categorías de datos innecesarios para las finalidades del nuevo Servicio según EIPD #132.	Minimización de datos	5.1.d) RGPD	No se ha estudiado detenidamente la necesidad de los datos recabados en finción de los fines del Servicio y sus tratamientos asociados.	Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso
6	SGSI-ENS	17/10/2017	No conformidad menor	NCm01/17	No se revisan informalmente los registros de actividad buscando patrones anormales.	Registro actividad de los usuarios (LOGS)	op.exp.8 ENS A.12.4.1 ISO27001	Al no disponerse de un correlacionador de eventos (SIEM) es una árdua tarea que acaba no haciéndose.	Adquirir y configurar un SIEM, definiendo alertas automáticas.
7									
8									
9									

Registro de acciones del SGSI-ENS (Incluye PTR)

	A	B	C	D	E	F	G	H	I
1	Registro inicial							Evaluación de las causas y determinación de las acciones	
2–3	SG	Fecha registro	Origen	Desencadenante de la acción		Ámbito	Art./Cláusula	Identificación de la causa de la NC o de la elección del objetivo	Acciones necesarias
				Referencia	Descripción				
4	COMUN	13/10/2016	No conformidad menor	NCm01/16	acciones formativas que en en el programa anual de ción, no tienen en cuenta los	Formación	Art. 39.1.a) RGPD 7.2 ISO 27001 mp.per.4 ENS	Únicamente se hace una programación de la formación a principios de año, y no se revisa teniendo en cuenta los cambios en la dades te las ño.	El área de formación formará parte del circuito de notificaciones de altas y modificaciones de la situación y funciones laborales asignadas a los empleados, para que pueda planificar sin dilación las acciones formativas y de concienciación correspondientes a cargo del DPD y del Responsable de Seguridad ENS.
5	RGPD	16/10/2017	Tratamiento de Riesgos	TR001/17				e la nción entos	Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso
6	SGSI-ENS	17/10/2017	No conformidad menor	NCm01/17	patrones anormales.	usuarios (LOGS)		de caba no haciendose.	Adquirir y configurar un SIEM, definiendo alertas automáticas.
7									
8									
9									

- **Lo que se va a hacer.**
- Qué recursos se requerirán.
- Quién será el responsable.
- Cuando se empezará.
- Cuando se finalizará.
- Cómo se evaluarán los resultados.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN DE APLICABILIDAD (SOA) ISO 27001:2013

	A	B	C	D	E	F	G	H	I	J
4	ISO 27001:2013 6.1.3.d)	DECLARACIÓN DE APLICABILIDAD (SOA)								
5	Dominio / Control	Descripción del Control / Objetivo de Control	Aplica	Status	Descripción y referencias documentales	Origen del control				
6	A.5	Política de seguridad de la Información				origen del contro			RGPD	TRAT. RIESGOS
7						TR	RL	BP	Detalle	Detalle
139	*A.15.2*	*Gestión de la provisión de servicios del proveedor*								
140	A.15.2.1 Control y revisión de la provisión de servicios del proveedor	Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor.	SI	⇧	Consultar el documento "SGSI-PRO-021-VxRx-Cadena de Suministro". Se reciben rapports mensuales de actividades de los proveedores más relevantes y se realiza una evaluación una vez al año.	X			[OP.EXT.2] GESTIÓN DIARIA	TR013/2017
141	A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor	Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los	SI	⇨	Consultar el documento "SGSI-PRO-021-VxRx-Cadena de Suministro" y el documento "SGSI-PRO-012-VxRx-Gestion de Cambios".			X	[OP.EXT.2] GESTIÓN DIARIA	
142	A.16	Gestión de incidentes de seguridad de la información								
143	*A.16.1*	*Gestión de incidentes de seguridad de la información y mejo*								
144	A.16.1.1 Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	SI	⇧	Consultar el procedimiento "SGSI-PRO-003-VxRx-Gestion y Respuesta a Incidentes de Seguridad de la Informacion".	X			[ORG.2] NORMATIVA DE SEGURIDAD [ORG.3] PROCEDIMIENTOS DE SEGURIDAD	NCm02/2017
	A.16.1.2 Notificación de los eventos	Los eventos de seguridad de la información se			Consultar el procedimiento "SGSI-PRO-003-VxRx-Gestion					

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN DE APLICABILIDAD (SOA) ISO 27001:2013

ISO 27001:2013 6.1.3.d)	DECLARACIÓN DE APLICABILIDAD (SOA)								
Dominio / Control	Descripción del Control / Objetivo de Control	Aplica	Status	Descripción y referencias documentales	Origen del control				
					origen del contro			RGPD	TRAT. RIESGOS
					TR	RL	BP	Detalle	Detalle
RGPD	Medida / Control								
Recabado	*Medidas en el recabado de datos*								
RGPD 0501 Minimización de datos	Solicitar únicamente los datos necesarios para la finalidad del servicio y los tratamientos asociados.	SI	⇧	Se repasan exhaustivamente los flujos de informción de las acciones de tratamieento para detectar si se recaban dato personales que después no son utilizados en ningún proceso. Se describe en el documento "SGSI-PRO-024-VxRx-ProcedimientoDe RevisiónDeFlujos".	X	X		5.1.d) RGPD	TR001/17

Resumen final de conceptos

- El RGPD pone el foco en TRATAMIENTOS más que en FICHEROS.
- El **Registro de Actividades de Tratamiento**, pieza clave en el RGPD.
- Las **EIPD** son una Gestión de Riesgos aplicada a determinadas actividades de tratamiento.
- Las EIPD se integran con la **Gestión de Riesgos** del SGSI-ENS.
- El **seguimiento de acciones** de mitigación derivadas de las EIPD puede ser común con el de las acciones generales determinadas para el SGSI-ENS.
- La **declaración de Aplicabilidad** (SOA), ampliada con controles jurídico-organizativos permiten compartir la estructura entre el RGPD y el SGSI-ENS.

Detalls Contacte

AUDERTIS

Nom del ponent
José Luis Colom Planas

Adreça Correu
jl.colom@audertis.es

Telèfon Contacte
609 861 073

Twitter
@JLColomPlanas

Integrando la norma ISO 27001, o el ENS, con el RGPD

*Agradecimiento a **Carlos GALÁN CORDERO** por haber iniciado la temática de esta ponencia en Marzo de 2017.*