Cumplimiento integral del RGPD y ENS

Telefónica

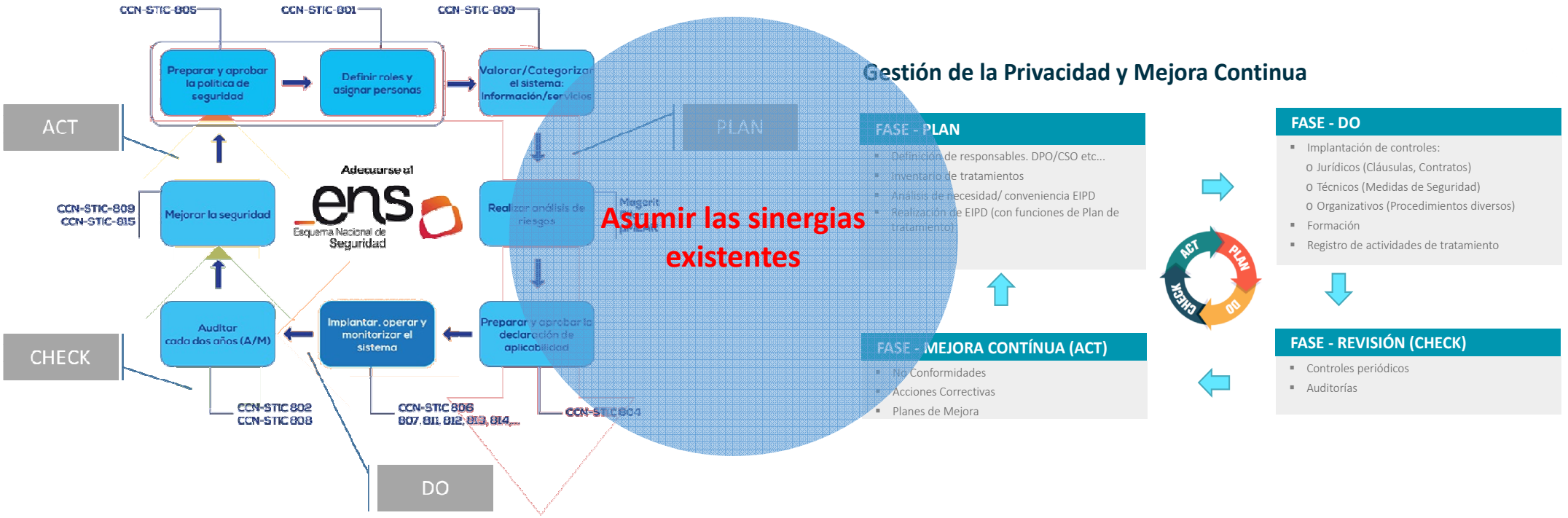
AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

1. VISIÓN GENERAL DEL CUMPLIMIENTO INTEGRADO ENS y RGPD

Planteamiento metodológico

- Simultanear el proceso de mejora continua en el contexto ENS+RGPD.



Telefónica

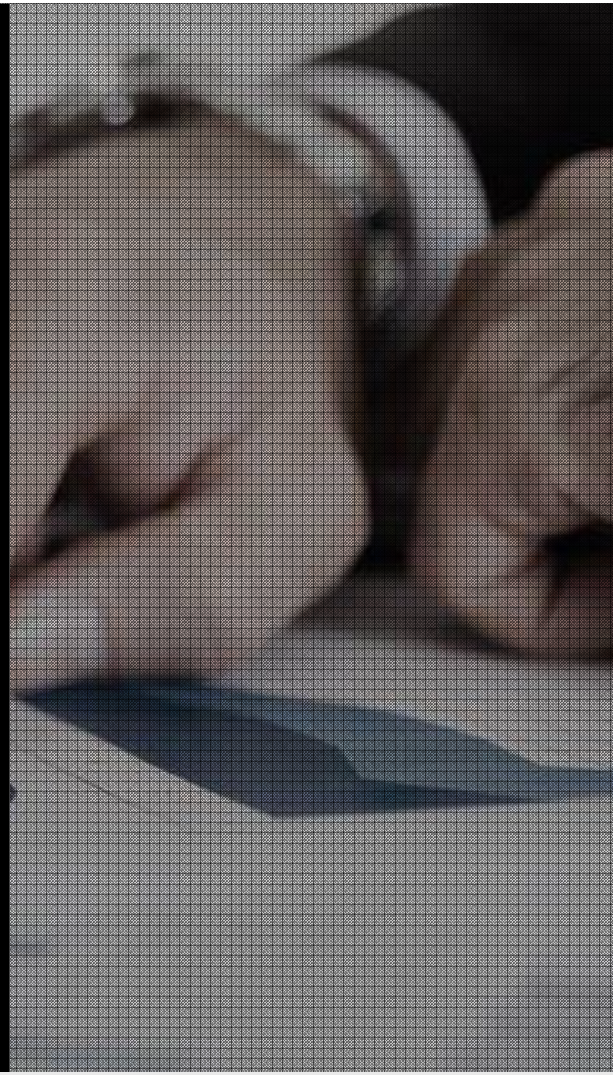
AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

2. PLAN DE PROYECTO: FASES Y ACTIVIDADES

GOVERTIS
Advisory Services

FASE PLAN



Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Roles y Responsabilidades: Planificación RGPD y ENS

RGPD

Asesor-Supervisor

Delegado de protección de datos

Supervisión

Responsable de seguridad

ENS

Responsable de la información

Responsable del servicio

Operación sistemas de información

Responsable del sistema de información

Roles y Responsabilidades: Relación

GUÍA CCN-STIC 801 ACTUALIZADA

FUNCIONES: INFORMAR, ASESORAR Y SUPERVISAR.

CARACTERÍSTICAS: INDEPENDENCIA, EVITANDO CONFLICTO DE INTERESES. PARTICIPANDO CON VOZ PERO SIN VOTO.

Niveles de la estructura de seguridad

Roles y Responsabilidades: Cuestiones frecuentes

CISO - Responsable de la seguridad de la información

DPO - Responsable de la privacidad

¿Pueden ser la misma persona?

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

con lo que se garantiza su independencia y se evita cualquier tipo de conflicto de intereses en el ejercicio de sus funciones.

V

En conclusión, es criterio de este Gabinete Jurídico que, con carácter general, debe existir la necesaria separación entre el delgado de protección de datos regulado en el RGPD y el responsable de seguridad del ENS, sin que sus funciones puedan recaer en la misma persona u órgano colegiado.

¿Y el Responsable de Seguridad ENS podría ser misma persona que el Responsable de Seguridad LOPD?

4.5 ¿El Responsable de Seguridad del ENS puede ser la misma persona que el Responsable de Seguridad de la LOPD?

Formalmente nada lo impide.

Debemos hacer constar que ambos perfiles requieren una formación muy específica y diferenciada. (Por ejemplo, el Responsable de Seguridad ENS es un perfil eminentemente tecnológico, mientras que el Responsable de Seguridad LOPD debe poseer, además, el conocimiento jurídico pertinente). Por tanto, dándose la circunstancia de que la persona designada goce de la formación adecuada en ambas responsabilidades, no existe inconveniente.

Independientemente de lo anterior, sobre todo en organizaciones de tamaño significativo, debe entenderse como más conveniente que ambos responsables (en el caso de personas físicas) sean distintos, pudiendo formar parte, eso sí, de un Comité de Seguridad de amplio espectro y cuyo titular será el Responsable formal de ambas funciones.

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Roles y Responsabilidades: Cuestiones frecuentes

¿Se pueden ejercer estas funciones de manera colegiada?

SÍ

9. COMITÉS

68. Como hemos señalado con anterioridad, algunas responsabilidades pueden instrumentalizarse por medio de Comités, que se constituirán como órganos colegiados, de conformidad con lo señalado en la Ley 40/2015. Estos Comités, que estarán formados por miembros de todas las partes implicadas, facilitan el desenvolvimiento de la organización y suelen ser habituales en entidades de tamaño mediano o grande.

69. Son habituales los siguientes:

- **Comité de Seguridad Corporativa**, que se responsabiliza de alinear todas las actividades de la organización en materia de seguridad, destacándose los aspectos de seguridad física y patrimonial (seguridad de las instalaciones), seguridad de la información, Compliance (seguridad y conformidad legal) y planes de contingencia.
- **Comité de Seguridad de la Información**, dependiente del anterior, que se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información.

Siendo el más común el segundo de ellos, tanto en RGPD como e ENS, estando habitualmente formado por las responsabilidades anteriormente enunciadas, así como por cualquier persona adicional que se considere oportuna.

El Responsable de Seguridad actuará como Secretario.

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Política de Seguridad: ENS y RGPD

GUÍA DE SEGURIDAD
(CCN-STIC-805)

ESQUEMA NACIONAL DE SEGURIDAD
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ENERO 2011

CONTENIDO

Clave: No sólo dedicar un apartado para hablar sobre la interrelación de normas, si no también incorporar la figura del DPD a la estructura de roles

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Advisory Services

Identificación de activos: ENS

METODOLOGÍA MAGERIT

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]

En un sistema de información hay 2 activos esenciales (la **información** que maneja y los **servicios** que presta), considerándose el resto como activos de soporte:

Importante para su modelado:

- Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema **transmitiéndoles su valor**.
- En cambio, estos activos esenciales son susceptibles **al riesgo transmitido por los activos de soporte**.

Telefónica AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD GOVERTIS Advisory Services

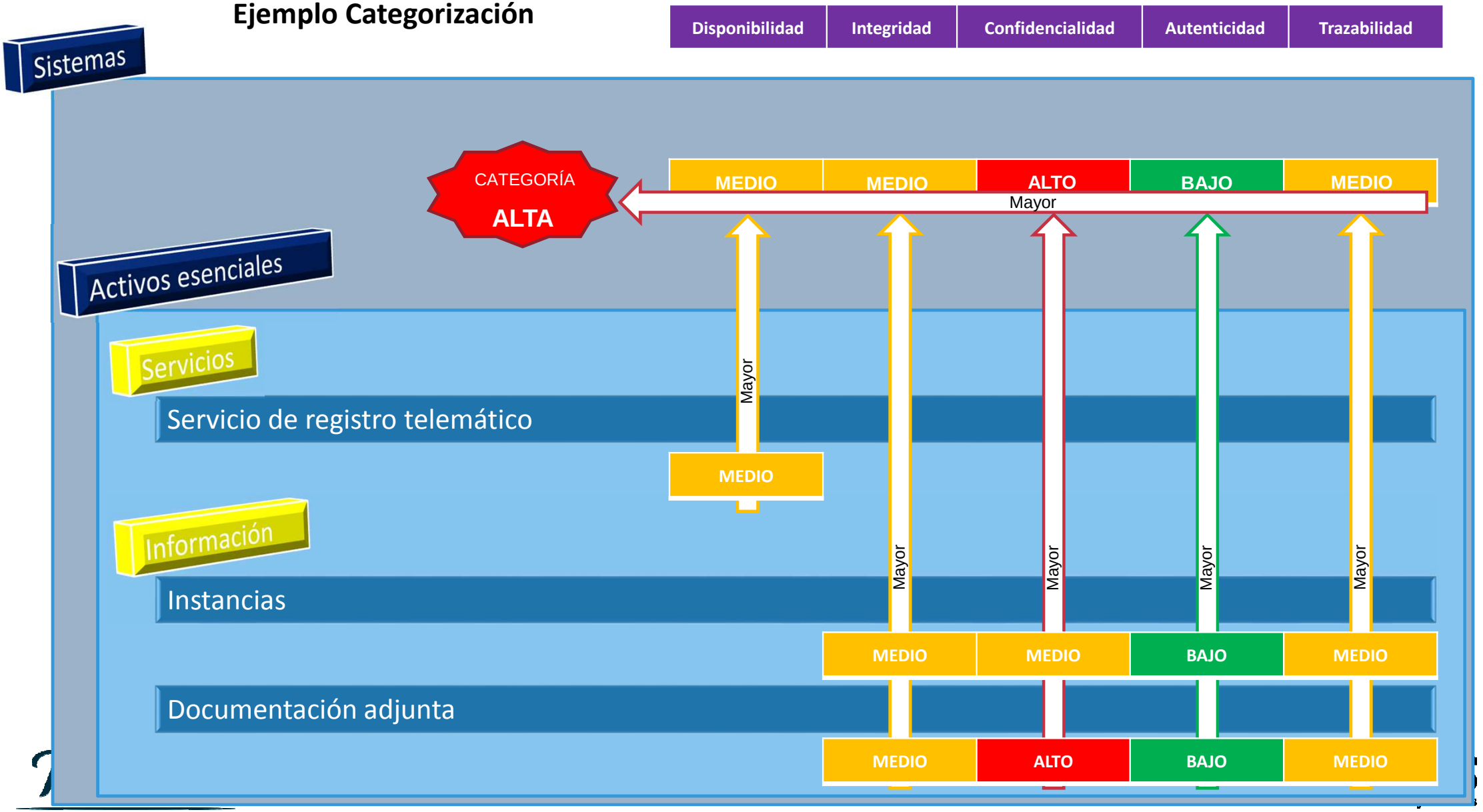
Identificación de activos: Valoración ENS

¿Por qué interesa un activo? Por lo que vale.

De un activo puede interesar valorar diferentes dimensiones:

- Su **disponibilidad**: ¿qué perjuicio causaría no tener el servicio o no poder utilizarlo?
- Su **confidencialidad**: ¿qué daño causaría que la información la conociera quien no debe?
- Su **integridad**: ¿qué perjuicio causaría que la información estuviera dañada o corrupta?
- La **autenticidad**: ¿qué perjuicio causaría no saber quien hace o ha hecho cada cosa?
- La **trazabilidad**: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Ejemplo Categorización



Identificación de activos: RGPD

En materia de RGPD, los activos a proteger no pueden ser otros que los "***Tratamientos",*** entendiendo como tal el conjunto de operaciones.

Como resultado de la identificación de estos activos surgirá el llamado **Registro de Actividades del Tratamiento**, que es el heredero natural de la antigua organización por ficheros.

Esta definición guarda estrecha relación con la realización del AARR:

Parece obvio que si se requiriese un análisis de riesgos conjunto, estos activos también deberían contribuir a marcar los requisitos de seguridad para todos los demás componentes del sistema **transmitiéndoles su valor**, al mismo tiempo que estos activos son susceptibles **al riesgo transmitido por los activos de soporte**.

Telefónica

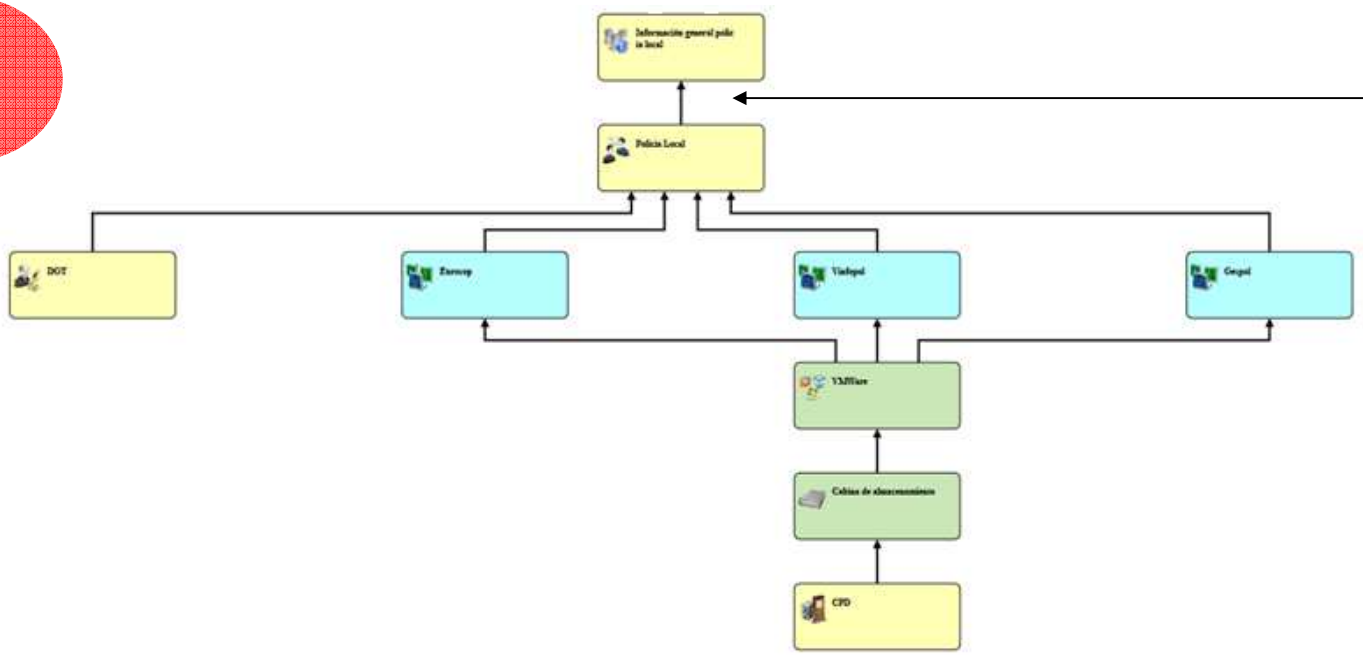
AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Identificación de activos: Cuestiones frecuentes

¿En dónde tienen espacio los tratamientos?

1



Actividades de Tratamiento

Si quisiésemos realizar una evaluación de riesgos conjunta, con la Sexta Dimensión de "Privacidad", teniendo en cuenta la transmisión de valor y riesgo

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

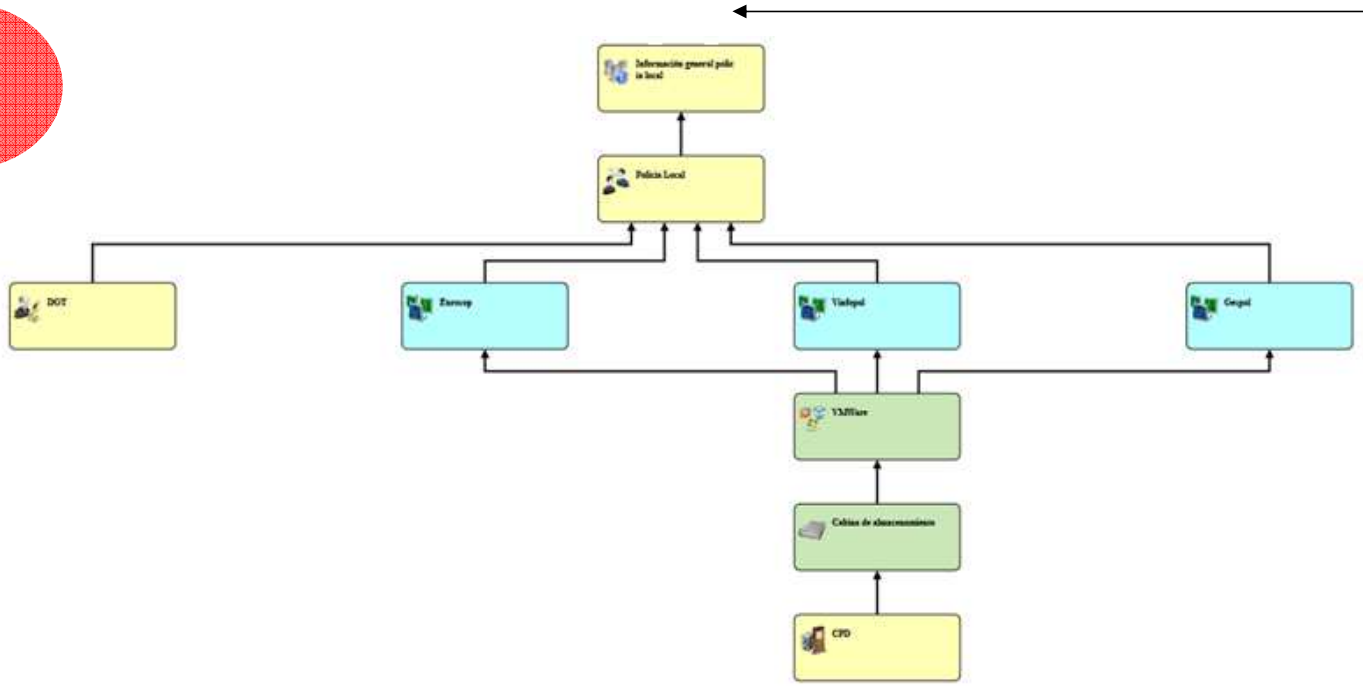
GOVERTIS
Advisory Services

Identificación de activos: Cuestiones frecuentes

¿En dónde tienen espacio los tratamientos?

2

Actividades de Tratamiento



Si realmente se optase por la realización de dos apreciaciones de riesgo, y se entendiese el Tratamiento como un subconjunto de datos del Activo "Información"

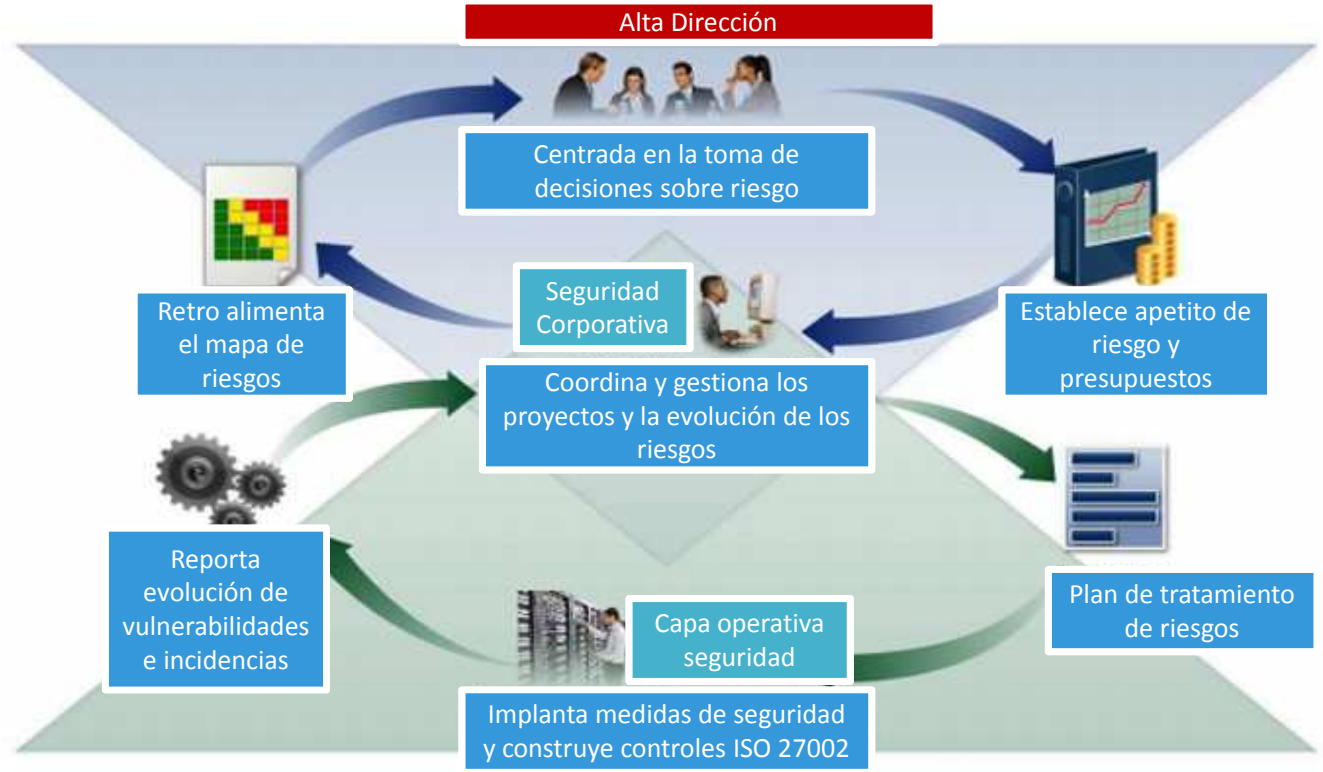
Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Análisis de Riesgos: ENS y RGPD

Tanto el ENS como la nueva aproximación del RGPD exigen gestionar la seguridad orientada al riesgo.



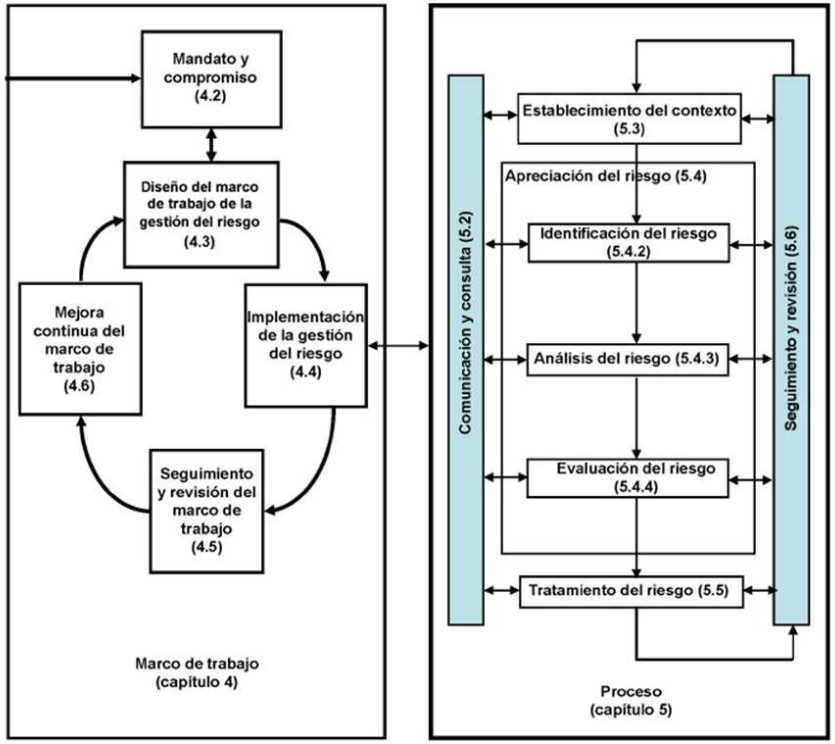
Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Análisis de Riesgos: ENS y RGPD

En la siguiente tabla de la UNE ISO 31000 se puede ver:



Establece que el proceso de apreciación del riesgo se divide en las siguientes **fases:**

1. Apreciación del riesgo
   Identificación del riesgo.
   Análisis del riesgo.
   Evaluación del riesgo.

2. Tratamiento de los riesgos

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Análisis de Riesgos: ENS y RGPD

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Análisis de Riesgos: ENS y RGPD

La fórmula del riesgo es una fórmula sencilla:

Para poder aplicar la fórmula, es necesario disponer de una matriz de riesgo, que se deberá definir y documentar.

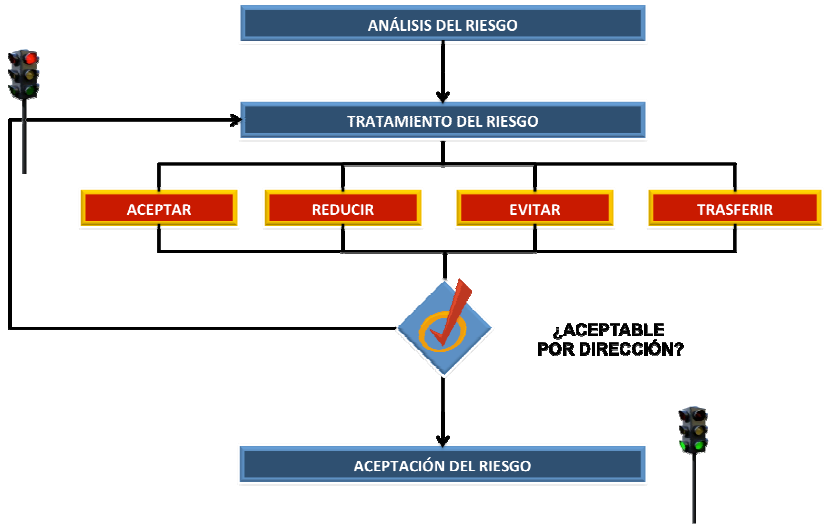
Casi seguro	Medio	Alto	Alto	Muy Alto	Muy Alto
Muy a menudo	Medio	Medio	Alto	Alto	Muy Alto
Probable	Medio	Medio	Medio	Alto	Alto
Poco probable	Bajo	Bajo	Medio	Medio	Alto
Muy raro	Bajo	Bajo	Bajo	Medio	Medio
	Muy bajo	Bajo	Medio	Alto	Muy Alto

Telefónica

GOVERTIS Advisory Services

Análisis de Riesgos: ENS y RGPD

TRATAMIENTO DEL RIESGO: Específicamente, según la ISO 31000, se pueden adoptar 4 posiciones diferentes para tratar el riesgo:



1. Aceptarlo: Esta medida implica que la organización no dispondrá más recursos para el tratamiento de este riesgo, por considerarlo, en la mayoría de ocasiones, como un riesgo que se encuentra por debajo del umbral aceptable.

2. Mitigarlo: Esta posición implica la implementación de medidas que hagan descender el nivel de riesgo (ya sea por reducir la probabilidad de que se suceda, o bien se reduzca el impacto.

Ejemplo: La amenaza de una interrupción en la alimentación de un servidor, que afecta a la Disponibilidad, podría ser mitigada con la adquisición de un SAI, reduciendo, en este caso, la probabilidad.

3. Transferirlo: Compartiéndolo con terceros generalmente, a través de la contratación de seguros o similares.

4. Evitarlo: Dejando de disponer del activo que genera dicho riesgo.

Ejemplo: Tras la implantación de varias medidas de seguridad, el riesgo sigue estando por encima del umbral de riesgo aceptable, se decide dejar de prestar un servicio por no poder prestarlo con suficientes garantías de seguridad.

Telefónica

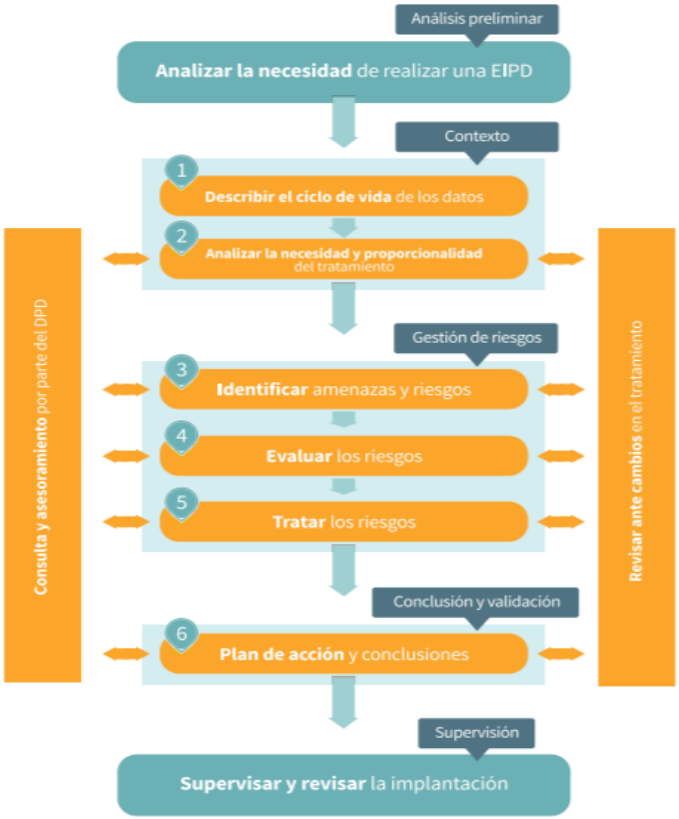
AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

EIPD: RGPD

¿Qué es? La EIPD es una herramienta con **carácter preventivo** que debe realizar el responsable del tratamiento para **poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas**. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

FASES



Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

EIPD: Cuestiones frecuentes

¿Qué diferencia hay entre un AARR y una EIPD?

ANÁLISIS DE RIESGOS

Se realizará para **todos los tratamientos**.
Habrá que **identificar los activos del sistema, las amenazas probables, las salvaguardas desplegadas,** utilizando una **metodología.**
Se valorarán **dimensiones de seguridad** distintas.

EIPD

No se realiza sobre todos los tratamientos, sólo para los que puedan **generar un riesgo alto**.
Se le puede aplicar una **metodología similar** en su ejecución a la utilizada en el análisis de riesgos, aunque, en cuanto a la atribución de amenazas, puede haber más libertad (no responde a una lista como la de Magerit)
Se valora una **dimensión concreta:** La privacidad y su afectación sobre los derechos y libertades de los ciudadanos.

Telefónica AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD GOVERTIS Advisory Services

Declaración de aplicabilidad: ENS

¿Qué es? Es simplemente el documento que se elabora, a nivel organizativo, para establecer la relación de las medidas que son aplicables a cada sistema o sub-sistema de información.

¿Qué implica? Habitualmente se recurrirá a las medidas detalladas en el Anexo II, enriquecidas o matizadas por características determinadas del sistema o exigencias derivadas del tratamiento de datos de carácter personal.

Cuando se recurra a medidas alternativas, se indicará el motivo, así como las medidas que sustituye.

Las medidas se complementarán con aquellas que sean pertinentes a la vista del análisis de riesgos realizado.

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Sistema Nivel Medio
	ORG	MARCO ORGANIZATIVO	
categoría	org.1	Política de seguridad	Aplica – B
categoría	org.2	Normativa de seguridad	Aplica – B
categoría	org.3	Procedimientos de seguridad	Aplica – B
categoría	org.4	Proceso de autorización	Aplica – B
	OP	MARCO OPERACIONAL	
	op.pl	Planificación	
categoría	op.pl.1	Análisis de riesgos	Aplica – M
categoría	op.pl.2	Arquitectura de seguridad	Aplica – M
categoría	op.pl.3	Adquisición de nuevos componentes	Aplica – B
D	op.pl.4	Dimensionamiento /Gestión de capacidades	Aplica – M
categoría	op.pl.5	Componentes certificados	No Aplica
	op.acc	Control de acceso	

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

A tener en cuenta…

Anexo II

Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización

Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
				mp	**Medidas de protección**
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoría	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos

Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Categoría
MEDIO	MEDIO	ALTO	BAJO	MEDIO	ALTO

Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
				op	**Marco operacional**
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	+	++	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento/Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local *(local logon)*
I C A T	aplica	+	=	op.acc.7	Acceso remoto *(remote login)*
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidentes
I	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
categoría	aplica	+	=	op.exp.11	Protección de claves criptográficas

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Informe de Insuficiencias: ENS y RGPD

¿Qué es? Dice la Guía CCN-STIC 806 que pueden detectarse insuficiencias por varias vías:

- Incumplimiento formal de las medidas de seguridad exigidas en el Anexo II del ENS.
- Incumplimiento formal de las medidas de seguridad exigidas por el RD 1720/1997 para los datos de carácter personal tratados por el sistema.
- Existencia de riesgos no asumibles.

Al fin y al cabo, es un ejercicio de transparencia de la entidad en donde se explica el estado actual, para poder elaborar un estado "Objetivo."

¿Qué implica? Implica la realización de entrevistas con los interlocutores autorizados de la entidad en donde se obtenga la información necesaria para la realización de un plan de mejora.

4.2 ACTUACIÓN 1: MARCO ORGANIZATIVO

Medidas de seguridad	Situación actual / Insuficiencia del Sistema	Nivel
Política de seguridad	Se dispone de Política de Seguridad, aprobada por la Dirección, y está publicada en la Intranet.	L2
Normativa de seguridad	Se dispone de normativa de seguridad, no obstante, se ha visto que es necesario una actualización.	L1-L2
Procedimientos de seguridad	Se dispone de procedimientos de seguridad internos en la organización, se ha visto que es necesario una actualización.	L1-L2
Proceso de Autorización	Existen procesos de autorización en la organización verbales, de cualquier forma, es necesario revisarlos y formalizarlos.	L1-L2

Telefónica

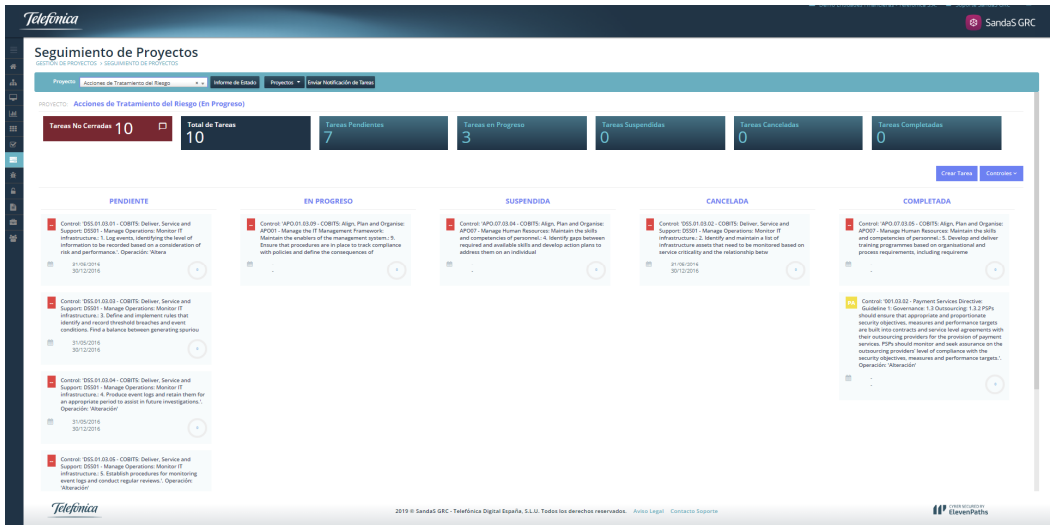
AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS Advisory Services

Plan de mejora: ENS y RGPD

¿Qué es? Dice la Guía CCN-STIC 806 que el Plan de Mejora constará de una serie de acciones destinadas a subsanar las deficiencias detectadas, y que la organización pueda cumplir con el ENS y el RGPD en congruencia con su análisis de riesgos y su declaración de aplicabilidad.

En este sentido, es muy interesante poder contar con **herramientas como Sandas GRC**, las cuales te permiten gestionar el proyecto de forma integral, teniendo, para esta actividad, por ejemplo, la posibilidad de ordenar las acciones de mejora en un **Tablero Kanban**, en donde definir acciones, responsables, tiempos y gráfico de evolución, así como el estado de la acción, consiguiendo un análisis rápido y sencillo.



Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Obligaciones adicionales: RGPD

Cumplir con el Deber de Informar

Guía Deber de Informar

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable Identidad y datos de contacto del representante Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento Plazos o criterios de conservación de los datos Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo. Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones Previsión de Transferencias, o no, a terceros países	Destinatarios o categorías de destinatarios Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento Derecho a retirar el consentimiento prestado Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público Categorías de datos que se traten

Gestionar los Prestadores de Servicios (ET)

Guía Responsables y Encargados

ANEXO I

Ejemplo de cláusulas contractuales para supuestos en que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas

(Estas cláusulas tienen sólo carácter orientativo y deben adaptarse a las circunstancias concretas del tratamiento que se lleve a cabo)

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la entidad ....., encargada del tratamiento, para tratar por cuenta de ...., responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de ..... .

El tratamiento consistirá en: *(descripción detallada del servicio)*

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Obligaciones adicionales: RGPD

Procedimiento Atención Derechos

Art. 15 a 22 RGPD

Procedimiento Brechas Seguridad

Guía Brechas Seguridad

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Normativas y Procedimientos: ENS y RGPD

En esta fase se evidenciarán las sinergias de cumplimiento entre el ENS y el RGPD. De hecho, en concreto, en lo relativo a la implantación de las medidas de seguridad, la recién publicada LOPDGDD, en su disposición adicional primera establece la siguiente premisa.

Disposición adicional primera Medidas de seguridad en el ámbito del sector público

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Normativas y Procedimientos: ENS y RGPD

En el ámbito del ENS…

Ejemplos

Marco normativo:

Tener en cuenta la Guía CCN-STIC 821

Marco procedimental:

- Procedimiento de gestión y aprobación de la documentación
- Procedimiento de clasificación, marcado y etiquetado de información y soportes
- Procedimiento de contratación de personal
- Procedimiento de contratación y seguimiento de servicios externos
- Procedimiento de gestión de la formación y concienciación
- Procedimiento de altas, bajas y modificaciones de usuarios
- Procedimiento de gestión del cambio y configuración segura de los sistemas
- Procedimiento de gestión del mantenimiento hardware y software
- Procedimiento de entrada y salida de equipamiento y soportes
- Procedimiento de copias de seguridad y restauración
- Procedimiento de gestión de incidentes
- Procedimiento de paso a producción
- Informes plan de continuidad
- Procedimiento de control de acceso físico

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

Formación: ENS y RGPD

Quizás sea la acción **más importante** para alcanzar el éxito en la implantación de estas materias, ya que los **principales riesgos** que se pueden derivar de la gestión de la seguridad de la información, en muchas ocasiones, **proviene directamente del factor humano.**

De hecho, en el Anexo II del ENS se configuran como una medida de protección más con la que cumplir.

Actualmente, se valoran mucho las acciones formativas originales:

Cursos interactivos

Vídeos sobre situaciones reales

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

FASE CHECK Y FASE ACT

Telefónica

GOVERTIS Advisory Services

Auditorías: ENS y RGPD

En el ámbito del ENS

Autoevaluaciones o auditorías internas como forma **de preparación**

Auditoría de certificación para Nivel Medio y Alto

En el ámbito del RGPD

Autoevaluaciones o auditorías internas o externas, como característica **de proactividad** y que, a la vez, sirvan como mecanismo de garantía ante terceros

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

No Confomidades y Acciones Correctivas: ENS y RGPD

En el ámbito del ENS y del RGPD

Las auditorías son un proceso periódico que cumple con este objetivo

Se procede a identificar aquellas causas que tienen un efecto significativo sobre el problema

Se procede con la búsqueda de soluciones adecuadas

Se procede con la implantación de las acciones de mejora

Se revalúan y comienza de nuevo el ciclo

Telefónica

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GOVERTIS
Advisory Services

MUCHAS GRACIAS!

GOVERTIS
Advisory Services

DAVID BARRIENTOS ARBOLEYA

https://es.linkedin.com/in/david-barrientos-arboleya-39780b62