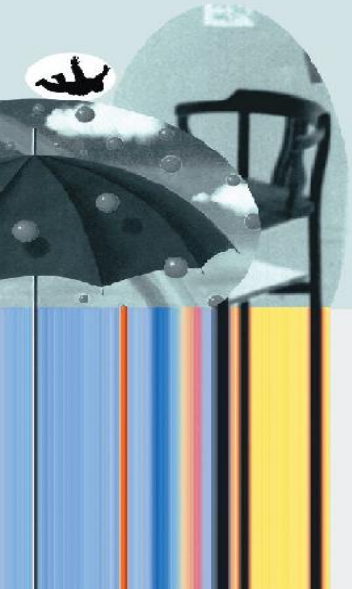
Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

Protección de Datos y Seguridad en el #RGPD para Ingenieros



Pedro Alberto González

Jefe del Servicio de
Registro y Auditoría de Ficheros

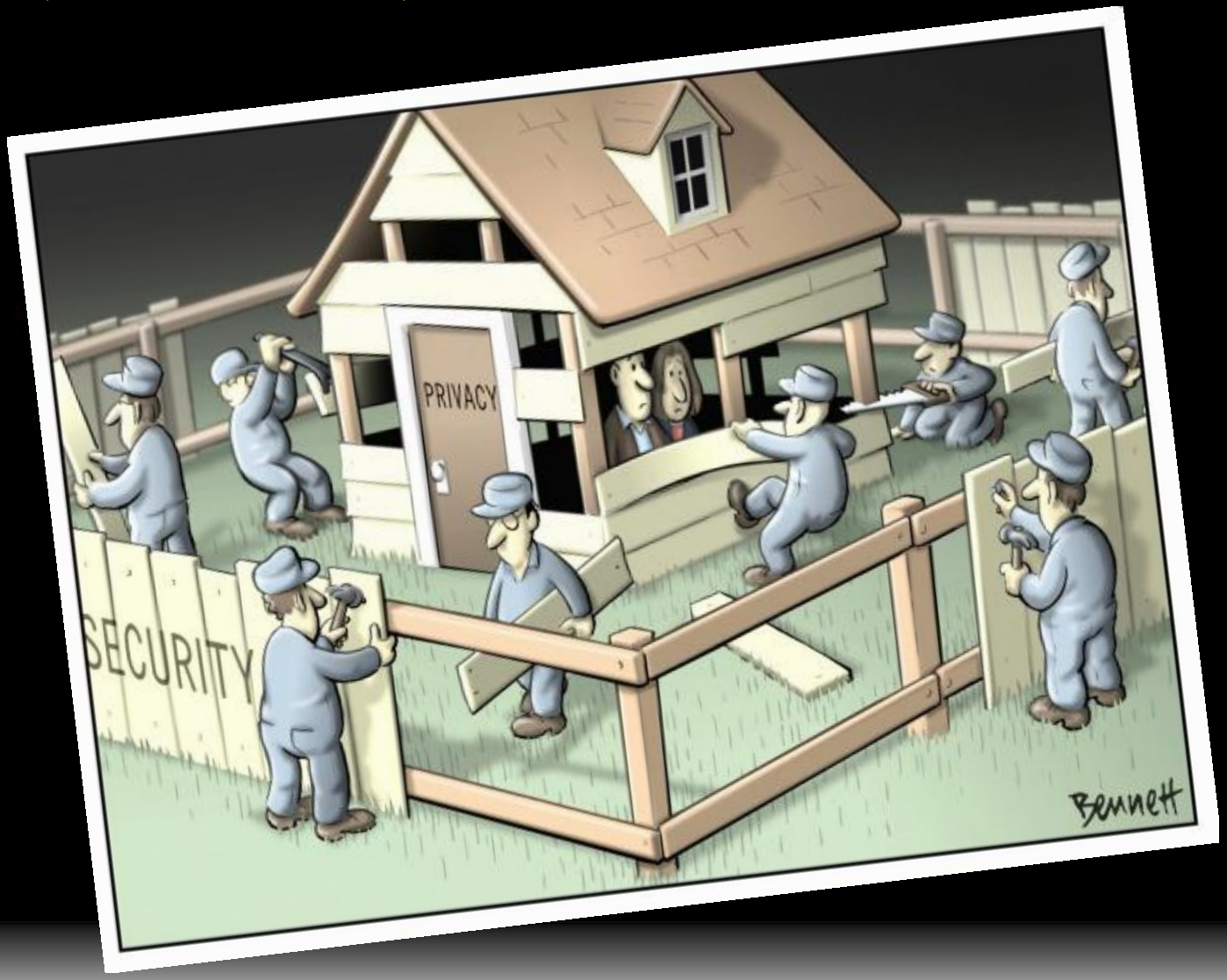
paGonzalez@avpd.es

Guión de la exposición

1. La seguridad, vista desde la privacidad
2. Marco de referencia de la Privacidad
3. Nuevo enfoque del #RGPD
   a. Responsabilidad Proactiva
   b. “Privacy by Design & Default”
   c. Evaluación de Impacto sobre la PD
   d. Códigos de conducta y Certificación
   e. Gestión de la Seguridad
4. Conclusiones e Interacción

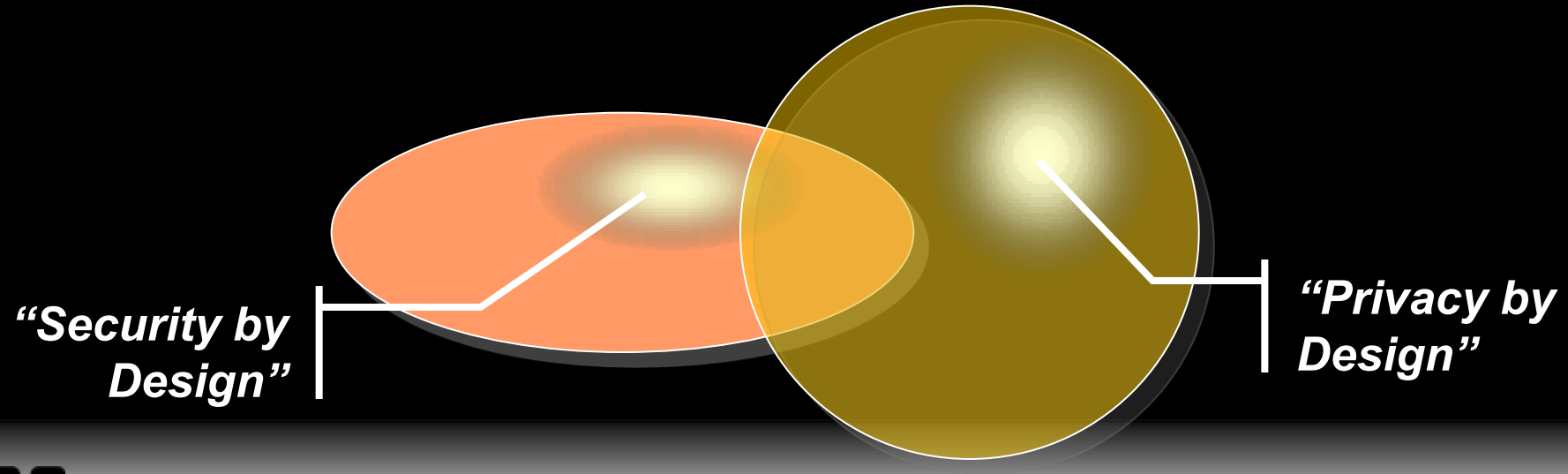
Colisión Seguridad <> Libertad

Colisión Seguridad <> Privacidad



Seguridad ≠ Privacidad

- Adjetivo (un ***medio***)
  - Protección de activos
    - Evitar riesgo
    - Mitigar impacto
- Sustantivo (un ***fin***)
  - Derecho
    - Fundamental
    - Constitucional



Guión de la exposición

1. La seguridad, vista desde la privacidad
2. Marco de referencia de la Privacidad
   - Principios
   - Derechos
3. Nuevo enfoque del #RGPD
   a. Responsabilidad Proactiva
   b. “Privacy by Design & Default”
   c. Evaluación de Impacto sobre la PD
   d. Códigos de conducta y Certificación
   e. Gestión de la Seguridad
4. Conclusiones e Interacción

La intimidad

- "*Derecho a que me dejen en paz*" -1890
- Delimitación de la intimidad:
  - Ámbito espacial:
    - Mis cuatro paredes
  - Ámbito subjetivo
    - Persona / personaje
  - Ámbito objetivo
    - Conducta privada / pública


VOLUME 114 JANUARY 2001 NUMBER 3

HARVARD LAW REVIEW

IN MEMORIAM: ABRAM CHAYES

ARTICLE

COMMENTARY

NOTES

RECENT CASES

RECENT PUBLICATIONS

THE HARVARD LAW REVIEW ASSOCIATION

La Privacidad

- *La **Intimidad**:*
  - *protege la esfera en que se desarrollan las facetas más **singularmente reservadas** de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, …*
- *La **Privacidad**.*
  - *constituye un conjunto, más amplio, más global, de **facetas de su personalidad** que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, **coherentemente enlazadas** entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.”*

Exposición de motivos de la antigua LORTAD

Derechos Humanos de Cuarta Generación

1. Derechos Civiles y Políticos
   - Vida, Libertad, dignidad, …
2. Derechos socioeconómicos y culturales
   - Educación, Salud, Trabajo, prot. Social, …
3. Derechos de solidaridad
   - Medio ambiente, consumo, …
4. ***Ciberderechos***

La Protección de Datos: un Derecho Fundamental *Europeo*

- Carta de los Derechos Fundamentales de la Unión Europea (2000)
  - Artículo 1: Dignidad humana
  - Artículo 2: Derecho a la vida
  - Artículo 3: Derecho a la integridad de la persona
  - Artículo 4: Prohibición de la tortura y de las penas o los tratos inhumanos o degradantes
  - Artículo 5: Prohibición de la esclavitud y del trabajo forzado
  - Artículo 6: Derecho a la libertad y a la seguridad
  - Artículo 7: Respeto de la vida privada y familiar
  - ***Artículo 8: Protección de datos de carácter personal***

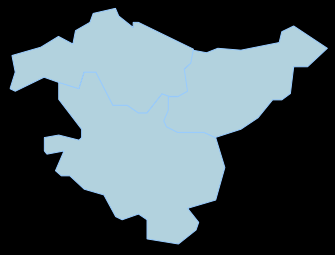
La Protección de Datos: un *Derecho Fundamental*

- Art. 18.4 de la Constitución (1978):
  - *"La Ley limitará **el uso de la informática** para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio en su derecho"*
- Art. 1 de la Ley Orgánica 15/1999:
  - *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los **derechos fundamentales** de las personas físicas, y especialmente de su honor e intimidad personal y familiar"*

Entorno Legal actual de la P.D.

- ***Directiva 95/46/CE*** del Parlamento Europeo y del Consejo, de 24 de Octubre, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- ***Reglamento General de Protección de Datos de la Unión Europea***

- ***Ley Orgánica 15/1999***, de 13 de Diciembre, de protección de datos de carácter personal (LOPD)
  - Traspone la Directiva 95/46/CE
  - Sutituye a la antigua LORTAD de 1992
- ***Real Decreto 1720/2007***, que desarrolla la LOPD (en particular, desarrolla las Medidas de Seguridad previstas en su art. 9)

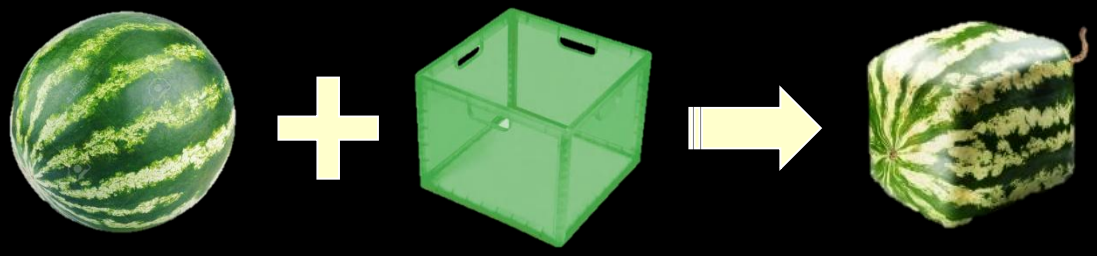


- ***Ley 2/2004*** de Ficheros de datos de Carácter Personal de Titularidad pública y de Creación de la Agencia Vasca de Protección de datos (LAVPD):
  - Objeto y ámbito de aplicación y sistemática de la ley
  - Creación de la AVPD y regulación de la misma
  - Establecimiento del régimen sancionador

El #RGPD: Características generales

- Reglamento vs Directiva
  - Adaptación, no trasposición
- "Libre circulación de datos" en la UE
  - "Tratamientos transfronterizos"
- Aplicación a "no establecidos en la UE"
  - El "Representante"
- "Responsabilidad proactiva"
  - DPO, PIAs, PbD, CdC, Certs, …

Adaptación al #RGPD



- Dos años de “vacatio legis” (2018-05-25)
  - LOPD + RD-1720/2007, en vigor
- Desarrollos legislativos pendientes:
  - Regulación del régimen sancionador
- Adecuación y adaptación a los nuevos elementos
  - Responsabilidad proactiva
  - Seguridad en base a Gestión de Riesgos

Framework de la Privacidad (Principios de la LOPD)

1. Calidad de los datos (minimización)
2. Especial protección de algunos datos
3. Información en la recogida
4. Consentimiento del afectado
5. Limitación de las cesiones de datos
6. Cumplimiento derechos A-R-C-O-
7. Deber de secreto
8. Seguridad de los datos

Calidad de los datos

- Los datos de carácter personal sólo se podrán recoger o tratar, cuando sean ***adecuados, pertinentes, no excesivos y puestos al día*** en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
- Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.
- Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

Datos especialmente protegidos

- Datos sobre o Ideología, religión creencias.
  - Nadie podrá ser obligado a declarar sobre estos datos
  - Cuando se recabe el consentimiento, se advertirá al interesado acerca de su derecho a no prestarlo.
  - El consentimiento en estos casos ha de ser expreso y por escrito (también la afiliación sindical)

Datos especialmente protegidos

- Datos sobre Origen racial, salud y vida sexual
  - Sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
- Están expresamente prohibidos los ficheros creados con la finalidad exclusiva de almacenar los anteriores datos especialmente protegidos.

Otros datos protegidos

- Datos relativos a la comisión de infracciones penales o administrativas
  - Los sólo podrán ser incluidos en ficheros de las Administraciones públicas
    - en los supuestos previstos en las respectivas normas reguladoras.

Derecho de información

- En qué consiste
  - Los ciudadanos y ciudadanas, tenemos derecho, cuando se nos solicita cualquier tipo de dato personal, a que se nos informe adecuadamente acerca del uso que se hará del nuestros datos.
- Nos deben informar de:
  - la existencia de un fichero de tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
  - si es obligatoria o facultativa la respuesta a las preguntas que nos sean planteadas.
  - las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
  - la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
  - la identidad y dirección del responsable del tratamiento o, en su caso, de su representante....

Excepciones al derecho de información

- Cuando expresamente una ley lo prevea,
- Cuando el tratamiento tenga fines históricos, estadísticos o científicos,
- Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados (a criterio de la Autoridad de Control correspondiente)
- Cuando los datos procedan de *fuentes accesibles al público* y se destinen a la actividad de publicidad o prospección comercial
  - en cada comunicación que se dirija al interesado se le informará del origen de los datos,
  - de la identidad del responsable del tratamiento
  - así como de los derechos que le asisten.

Consentimiento del afectado

- El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado
- El consentimiento podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

Excepciones al consentimiento

- Cuando una ley disponga otra cosa.
- Cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias
- Cuando se refieran a las partes de un contrato o de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento
- Cuando el tratamiento tenga por finalidad proteger un interés vital del interesado (prevención, diagnóstico o tratamiento)
- Cuando los datos figuren en fuentes accesibles al público

Habilitación para el tratamiento de datos

Deber de secreto

- El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional.
  - Esta obligación subsistirá aun después de finalizar sus relaciones con el titular del fichero.

Comunicación o cesión de los datos

- Cesión o comunicación de datos es toda revelación de datos realizada a una persona distinta del interesado
- No se considera comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

Condiciones para las cesiones

- Los datos sólo podrán ser comunicados a un tercero:
  - para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario
  - con el previo consentimiento del interesado.
- El consentimiento para la comunicación de datos tiene carácter de revocable.
  - Será nulo el consentimiento, cuando la información facilitada no permita conocer la finalidad o el tipo de actividad a que destinarán los datos cuya comunicación se autoriza.
- Aquel a quien se comuniquen los datos se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.
  - La comunicación constituye la creación de un nuevo fichero

El consentimiento exigido para las cesiones no será preciso:

- Cuando la cesión está autorizada en una ley.
- Cuando la comunicación que deba efectuarse tenga por destinatario:
  - el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas.
  - al Defensor del Pueblo o el Tribunal de Cuentas, o instituciones autonómicas con funciones análogas.
- Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria
  - para solucionar una urgencia que requiera acceder a un fichero
  - para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Las cesiones entre Administraciones Públicas estarán permitidas :

- Cuando tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- Cuando los datos recogidos o elaborados por una Administración Públicas, precisamente con destino a otra Administración Pública
- Únicamente se podrán ceder datos para el ejercicio de competencias que versen sobre las mismas materias.

El consentimiento tampoco será preciso para las cesiones cuando:

- Cuando se trate de datos recogidos de fuentes accesibles al público.
- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

Derechos de las personas en la LOPD

- Derechos "A.R.C.O."
  - Acceso
  - Rectificación
  - Cancelación
  - Oposición

Derechos de las Personas

- Ejercicio personalísimo
- Se ejercen ante el responsable del fichero
  - Su ejercicio ha de ser gratuito
- Puede reclamarse la tutela de las Autoridades de Control APD's

Acceso

- El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos
- Plazos:
  - No podrá llevarse a cabo en intervalos inferiores a 12 meses.
  - El responsable deberá responder en el plazo máximo de un mes.
  - Transcurrido este plazo, se entenderá denegado el acceso.
- La información deberá contener de modo legible e inteligible
  - los datos incluidos en el fichero, y los resultantes de cualquier elaboración, proceso o tratamiento,
  - el origen de los datos y los cesionarios previstos
  - la especificación de los usos concretos y finalidades para los que se almacenaron.

Rectificación

- Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos
- Plazos:
  - El responsable deberá responder en el plazo de diez días.
  - Transcurrido este plazo, se entenderá denegado el acceso.
  - El responsable deberá rectificar en el plazo de diez días.
  - Los datos a rectificar deben de justificarse adecuadamente

Cancelación

- Condiciones para la cancelación:
  - Cuando los datos no se ajusten a la Ley;
  - Hayas sido recabados por medios fraudulentos, desleales o ilícitos;
  - resultan inadecuados o excesivos,
  - hayan dejado de ser pertinentes o necesarios para la finalidad para la que fueron recabados
- Restricciones a la cancelación:
  - Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables
  - en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado
- Forma de cancelación:
  - La cancelación implica el cese inmediato de su tratamiento
  - Se conservarán únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.
  - Cumplido el citado plazo deberá procederse a la supresión física.

Oposición

- El consentimiento podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
  - Cuando no sea necesario el consentimiento del afectado, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal
- Casos concretos de oposición:
  - Impugnación de valoraciones
  - Exclusión de directorios telefónicos
  - Publicidad no deseada

Guión de la exposición

1. La seguridad, vista desde la privacidad
2. Marco de referencia de la Privacidad
3. Nuevo enfoque del #RGPD
   a. Responsabilidad Proactiva
   b. “Privacy by Design & Default”
   c. Evaluación de Impacto sobre la PD
   d. Códigos de conducta y Certificación
   e. Gestión de la Seguridad
4. Conclusiones e Interacción

“Responsabilidad proactiva”

"Responsabilidad proActiva"

"*El responsable del tratamiento (…) será* ***capaz de***

- ***cumplir***
- ***demostrar***

que trata los datos de acuerdo con los principios de:

1. Licitud, lealtad y transparencia
2. Limitación de la finalidad
3. Minimización de datos
4. Exactitud (y vigencia)
5. Limitación del plazo de conservación
6. Integridad y confidencialidad

(art. 5.2 #RGPD)

Cambio de "esquema mental"

"Cumplimiento pasivo"

- Declarar los ficheros en el Registro…
- Incluir una "clausula LOPD"…
- Copiar un "documento de seguridad"…
- ¿Problemas?
  - (…salir del paso…)
  - Reaccionar a posteriori

"Responsabilidad proActiva"

- Llevara un registro interno de tratamientos
- Disponer de un Delegado de Protección de Datos
- Efectuar Evaluaciones de Impacto sobre la privacidad
- Aplicar la Privacidad desde el diseño
- Adoptar Códigos de Conducta, certificaciones y sellos

Aspectos clave

- Actores y roles
  - Responsable del tratamiento (RT)
  - Encargado / subencargado del tratamiento (ET)
  - Delegado de protección de datos (DPO's)
- Nuevos elementos
  - Registro (interno) de tratamientos
  - Evaluación de Impacto sobre la Privacidad (PIA)
  - Privacidad desde el diseño y por defecto (PbD)
  - Seguridad basada en Análisis de Riesgos (ISRM)
  - Códigos de Conducta, certificaciones y sellos (CdC)

RESPONSABLES Y ENCARGADOS DE TRATAMIENTOS

«RESPONSABLE DEL TRATAMIENTO» O «RESPONSABLE»:

- "Persona física o jurídica, autoridad pública, servicio u otro organismo,
- que, solo o junto con otros, determine los fines y medios del tratamiento"
  - Ya no se habla de "Ficheros", sino de "Tratamientos"
  - Establecido en varios estados miembros (con un "Establecimiento Principal")
  - Establecidos fuera de la UE (con designación de Representante)
  - Posibilidad de existencia de "Co-Responsables"

Sujeto principal de la "Responsabilidad activa"

- "Teniendo en cuenta:
  - la naturaleza, el ámbito, el contexto y los fines del tratamiento
- así como los riesgos de diversa
  - probabilidad y gravedad

  para los derechos y libertades de las personas físicas,
- el responsable del tratamiento aplicará
  - medidas técnicas y organizativas apropiadas
- a fin de
  - garantizar y poder demostrar

  que el tratamiento es conforme con el presente Reglamento.
- Dichas medidas se revisarán y actualizarán cuando sea necesario."

(art. 24.1 #RGPD)

Sujetos principales de la "Responsabilidad activa"

- Medidas técnicas y organizativas para Garantizar y Demostrar que el tratamiento es conforme al Reglamento
  - Delegado de Protección de Datos
  - Registro de sus propios tratamientos
  - Protección de datos desde el diseño y por defecto
  - Evaluaciones de Impacto sobre PD
  - Autoregulación por Códigos de Conducta

«ENCARGADO DEL TRATAMIENTO» O «ENCARGADO»

- “La persona física o jurídica, autoridad pública, servicio u otro organismo
- …que trate datos personales por cuenta del responsable del tratamiento”
  - Mayor importancia que hasta ahora
  - La mayor parte de las obligaciones son para ambos, Responsable y Encargado
  - Exigencia de garantías técnicas y organizativas
  - Permitidos los sub-Encargos, con autorización del Responsable

Exigencia de Contrato o "acto jurídico" vinculante

- Constancia por escrito / electrónico
- Tratamiento bajo instrucciones documentadas del Responsable
- Garantía y compromiso de confidencialidad
- Especificación de medidas de seguridad
- Condiciones de subEncargo
- Devolución o Destrucción de datos
- Realización de auditorías e inspecciones

LOS DELEGADOS DE PROTECCIÓN DE DATOS

Los Delegados de Protección de Datos

- Necesario siempre que los Tratamientos:
  - Se lleven a cabo por Autoridades u Organismos Públicos
  - Requieran una observación habitual y sistemática de interesados a gran escala
  - Traten a gran escala de datos personales de categorías especiales o relativos a condenas e infracciones penales
- Puede ser único para:
  - Grupos Empresariales
  - Autoridades u Organismos Públicos
  - Asociaciones u Organismos representativos

Algunos "Conceptos (mas o menos) indeterminados"

- "Gran Escala"
- "Ocasional" / "Habitual" / "Sistemático"
- "Alto Riesgo" / "Riesgo improbable"

Cualificación y Posición

- Conocimientos especializados del derecho y la Práctica de la PD
- Puede ser empleado o servicio externo
- Independiente. Inviolable. No exclusivo
- Reporta al más alto nivel jerárquico
- Datos de contacto publicados y notificados a ACPD

Funciones del DPD

- a) informar y asesorar al responsable o encargado;
- b) supervisar el cumplimiento legal y de las políticas del responsable o del encargado, incluidas:
  - la asignación de responsabilidades,
  - la concienciación y formación del personal
  - las auditorías correspondientes;
- c) ofrecer el asesoramiento acerca de las evaluaciones de impacto y supervisar su aplicación;
- d) cooperar con la autoridad de control;
- e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

El DPD, ¿jurista o tecnólogo?

"Art. 37.5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, …

- *a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos*

y a su capacidad para desempeñar sus funciones."

- Puede ser una evolución de los actuales Responsables de Seguridad…
- …pero necesitarán mayor formación en "*el derecho y la práctica en materia de protección de datos*"
- Oportunidades de mercado laboral

Registro (interno) de Tratamientos

el actual Registro de Ficheros... ¡¡¡ Desaparece !!!

Actualmente, ¿qué son los Registros de Ficheros?

- Órgano previsto en la LOPD para garantizar la publicidad de la existencia de ficheros (art. 39)
- Registro de ficheros de la ***AEPD***:
  - Ficheros de titularidad privada
  - Ficheros de titularidad pública de
    - Órganos Constitucionales
    - AGE (Administración General del Estado)
    - EELL y CCAA sin APD
- Registro de ficheros de la ***AVPD***:
  - Ficheros de titularidad pública de Euskadi

¿Qué pasos hay que dar para crear Ficheros con D.C.P.?

Adoptar una Disposición General
(por el responsable)

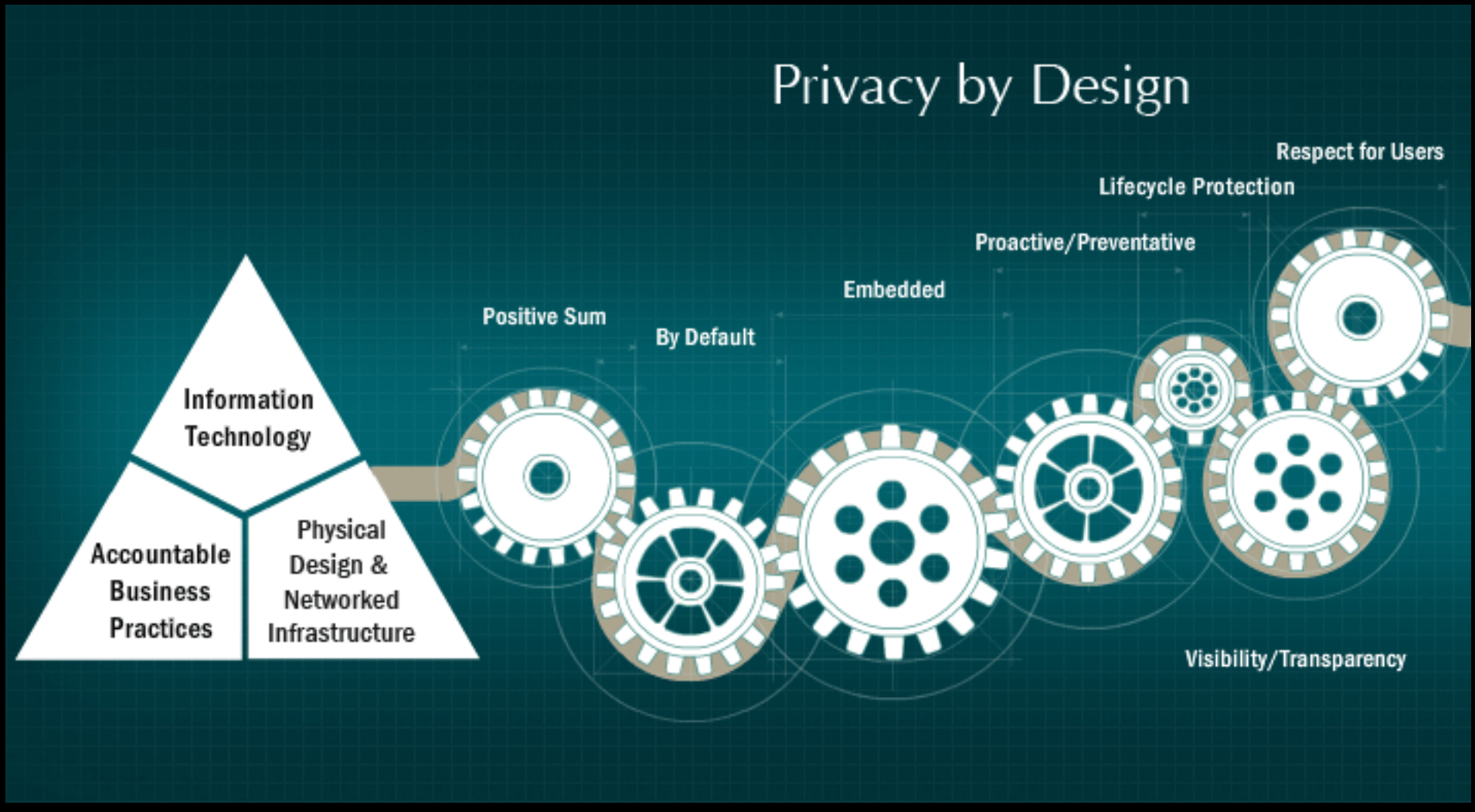
Publicar en el Boletín Oficial

Notificar a la APD

El (nuevo) registro (interno) de tratamientos

- ***El registro, tal como lo conocemos hoy, desaparece.***
- Se mantiene la necesidad de llevanza de un registro (interno) de las actividades de tratamiento
  - Por el Responsable
  - Por el Encargado
- Para las organizaciones:
  - Que empleen más de 250 personas, o bien:
  - Que el tratamiento entrañe riesgos para los interesados,
  - no sea ocasional
  - o incluya categorías especiales o relativos a condenas e infracciones penales.
- Dicho Registro interno estará a disposición de las Autoridades de Control

La privacidad, desde el diseño (y por defecto)


Privacy by Design
Respect for Users
Lifecycle Protection
Proactive/Preventative
Embedded
Positive Sum
By Default
Information Technology
Accountable Business Practices
Physical Design & Networked Infrastructure
Visibility/Transparency

7 Principios fundamentales de la Privacidad desde el Diseño

1. Diseño Proactivo, no Reactivo;
   - Preventivo, no Correctivo
2. Privacidad como configuración por defecto
3. Privacidad incrustada en el diseño
4. Funcionalidad total:
   - "Suma-Positiva", no "Suma-Zero"
5. Seguridad en todo el ciclo de vida ("end-to-end")
6. Visibilidad y transparencia – "Keep it Open"
7. Respeto a la privacidad personal ("User-centric")

Protección de datos desde el diseño y por defecto en #RGPD

Art. 25.1.- Teniendo en cuenta

- el estado de la técnica, el coste de la aplicación
- y la naturaleza, ámbito, contexto y fines del tratamiento,
- así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas,

el responsable del tratamiento aplicará,

- tanto en el momento de determinar los medios de tratamiento
- como en el momento del propio tratamiento,

medidas técnicas y organizativas apropiadas,

- como la seudonimización,

concebidas para aplicar de forma efectiva los principios de protección de datos,

- como la minimización de datos,

e integrar las garantías necesarias en el tratamiento.

Art. 25.- Protección de datos desde el diseño y por defecto

(…)

Art. 25.2.- El responsable del tratamiento implementará mecanismos con miras a garantizar que,

- por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico del tratamiento
- y, especialmente, que no se recojan ni conserven más allá del mínimo necesario para esos fines, tanto por lo que respecta a la cantidad de los datos como a la duración de su conservación.
- En concreto, estos mecanismos garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas.

EVALUACIONES DE IMPACTO SOBRE LA PROTECCIÓN DE DATOS

Las evaluaciones de impacto

- Necesarias cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, en particular en caso de:
  - evaluación sistemática y exhaustiva de aspectos personales, que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos;
  - tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales, o
  - observación sistemática a gran escala de una zona de acceso público.
- Tipos de operaciones establecidos por Autoridades de Control

Contenido de la evaluación de impacto

- a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento;
- b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- c) una evaluación de los riesgos para los derechos y libertades de los interesados, y
- d) las medidas previstas para afrontar los riesgos.

¿Cómo hacer Evaluaciones de impacto sobre la Privacidad?

CÓDIGOS DE CONDUCTA , CERTIFICACIONES Y SELLOS

Códigos de Conducta

- Definición en el #RGPD:
  - No hay definición en el #RGPD
- Definición de la OIE (Organización Internacional de Empleadores, 1999)
  - *"Declaración expresa de la política, los valores o los principios en que se inspira el comportamiento de una empresa en lo que atañe a:*
    - *el desarrollo de sus recursos humanos,*
    - *su gestión medioambiental*
    - *su interacción con los consumidores, los clientes, los gobiernos y las comunidades en las que desarrolla su actividad*

Códigos de Conducta

- Definición de Wikipedia:
  - *"Documento redactado voluntariamente por una empresa en el que se exponen una serie de principios que se compromete unilateralmente a seguir."*
  - *"En algunas oportunidades los códigos de conducta alcanzan a las empresas proveedoras, subcontratistas y terceristas"*

Códigos de Conducta

- Definición en las Directivas 2005/29/CE y 2008/122/CE
  - *«**código de conducta**»:*
    - *un acuerdo o conjunto de normas no impuestas por disposiciones legales, reglamentarias o administrativas de un Estado miembro,*
    - *en el que se define el comportamiento de aquellos comerciantes que se comprometen a cumplir el código*
    - *en relación con una o más prácticas comerciales o sectores económicos concretos;*
  - *«**responsable del código**»:*
    - *cualquier entidad, incluido un comerciante o un grupo de comerciantes, que sea responsable de la elaboración y revisión de un código de conducta o de supervisar su cumplimiento por quienes se hayan comprometido a respetarlo.*

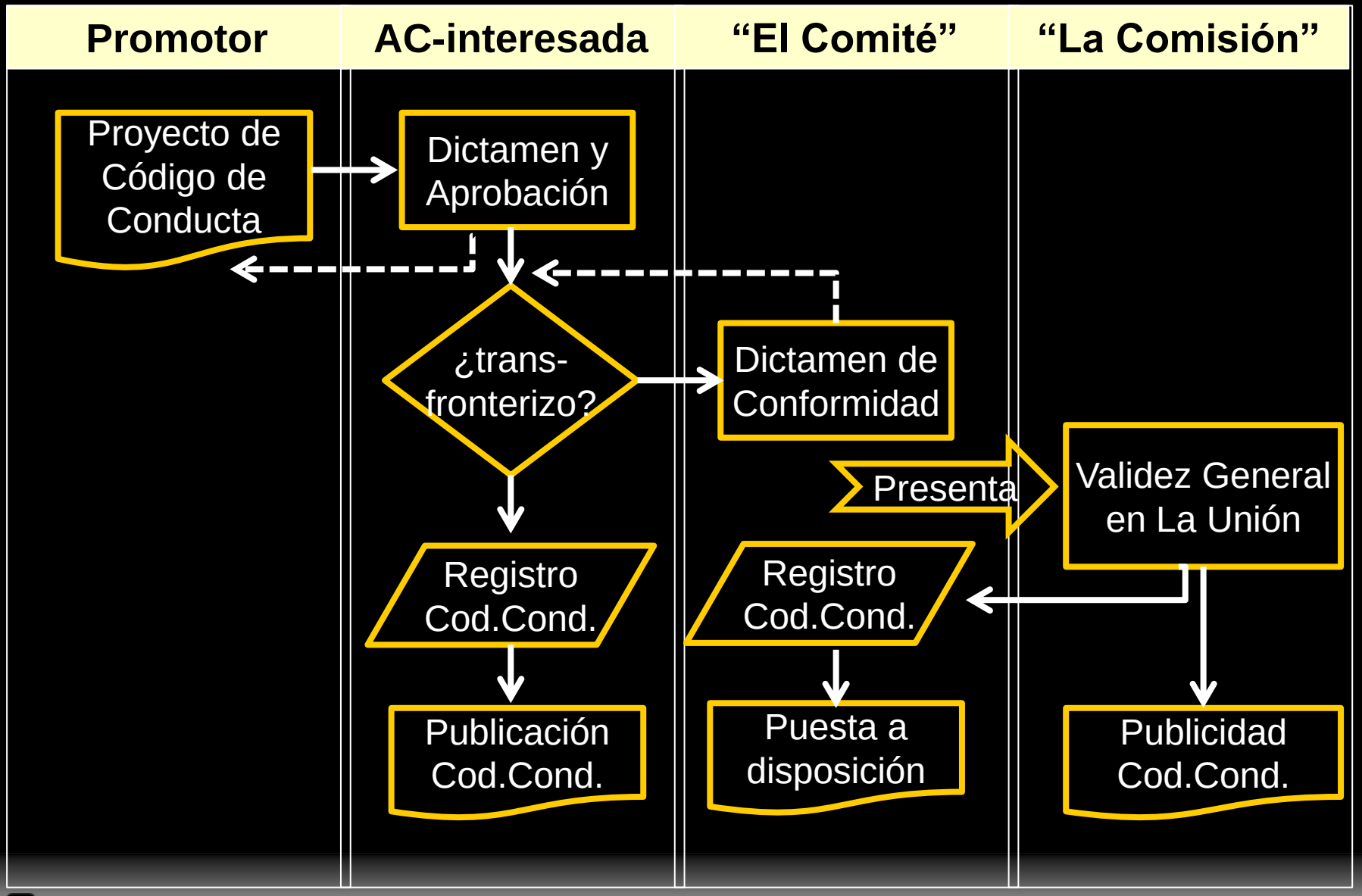
Los Códigos de Conducta y Certificación

- Mecanismos para la ***acreditación del cumplimiento*** de obligaciones
  - (art.24.3, 28.5, 32.3, 46.2.e)
- Promocionados por:
  - Estados miembros, Autoridades de control,
  - “el Comité”, “la Comisión “
- Supervisados por
  - Organismos acreditados
  - Autoridades de Control (sin perjuicio de…)
- Cuando afectan a más de un estado miembro, aplica el “***mecanismo de coherencia***”

Códigos de Conducta

- Finalidad:
  - "***contribuir a la correcta aplicación del Reglamento***", teniendo en cuenta:
    - las características de los sectores de tratamiento
    - las necesidades de las (…) pequeñas (…) empresas

Códigos de Conducta



GESTIÓN DE LA SEGURIDAD

Marco LOPD
Seguridad de los Datos

Art. 9 LOPD:

- "Se adoptarán las ***medidas técnicas y organizativas*** necesarias para garantizar la seguridad de los datos,
  - evitando su alteración o pérdida
  - y su tratamiento o acceso no autorizado
- "Teniendo en cuenta:
  - el estado de la tecnología
  - la naturaleza de los datos almacenados
  - los riesgos a que estén expuestos
- "Afecta tanto al Responsable del Fichero como al Encargado del Tratamiento

Desarrollo LOPD: RD-1720/2007

BOE

LEGISLACIÓN CONSOLIDADA

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Ministerio de Justicia
«BOE» núm. 17, de 19 de enero de 2008
Referencia: BOE-A-2008-979

TEXTO CONSOL
Última modificación: 8 d

TÍTULO VIII. De las medidas de seguridad en el tratamiento de datos de carácter personal
CAPÍTULO I. Disposiciones generales
- Artículo 79. Alcance.
- Artículo 80. Niveles de seguridad.
- Artículo 81. Aplicación de los niveles de seguridad.
- Artículo 82. Encargado del tratamiento.
- Artículo 83. Prestaciones de servicios sin acceso a datos personales.
- Artículo 84. Delegación de autorizaciones.
- Artículo 85. Acceso a datos a través de redes de comunicaciones.
- Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
- Artículo 87. Ficheros temporales o copias de trabajo de documentos.

CAPÍTULO II. Del documento de seguridad
- Artículo 88. El documento de seguridad.

CAPÍTULO III. Medidas de seguridad aplicables a ficheros y tratamientos automatizados
Sección 1.ª Medidas de seguridad de nivel básico
- Artículo 89. Funciones y obligaciones del personal.
- Artículo 90. Registro de incidencias.
- Artículo 91. Control de acceso.
- Artículo 92. Gestión de soportes y documentos.
- Artículo 93. Identificación y autenticación.
- Artículo 94. Copias de respaldo y recuperación.

Sección 2.ª Medidas de seguridad de nivel medio
- Artículo 95. Responsable de seguridad.
- Artículo 96. Auditoría.
- Artículo 97. Gestión de soportes y documentos.
- Artículo 98. Identificación y autenticación.
- Artículo 99. Control de acceso físico.
- Artículo 100. Registro de incidencias.

Sección 3.ª Medidas de seguridad de nivel alto
- Artículo 101. Gestión y distribución de soportes.
- Artículo 102. Copias de respaldo y recuperación.
- Artículo 103. Registro de accesos.
- Artículo 104. Telecomunicaciones.

CAPÍTULO IV. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados
Sección 1.ª Medidas de seguridad de nivel básico
- Artículo 105. Obligaciones comunes.
- Artículo 106. Criterios de archivo.
- Artículo 107. Dispositivos de almacenamiento.
- Artículo 108. Custodia de los soportes.

Sección 2.ª Medidas de seguridad de nivel medio
- Artículo 109. Responsable de seguridad.
- Artículo 110. Auditoría.

Sección 3.ª Medidas de seguridad de nivel alto
- Artículo 111. Almacenamiento de la información.
- Artículo 112. Copia o reproducción.
- Artículo 113. Acceso a la documentación.
- Artículo 114. Traslado de documentación.

Estructura del RD 1720/2007

- Clasificación de la Información
  - Criterios de exigencia de los niveles de seguridad
- Requisitos de documentación
  - Estructura y contenido del "Documento de Seguridad"
- Relación de "Puntos de control"
  - Medidas de seguridad, diferenciadas para cada uno de los niveles exigibles

Niveles de seguridad

10 puntos de control en medidas de seguridad

1. Organización de la Seguridad
2. Documentación de Seguridad
3. Funciones y obligaciones del personal
4. Identificación y autenticación de usuarios
5. Controles y registros de accesos
6. Accesos a través de redes / Internet
7. Soportes y documentos con información
8. Copias de respaldo y recuperación
9. Gestionar Incidencias de seguridad
10. Efectuar Auditorías y Controles

1.- Responsable de Seguridad

Nivel Básico	Nivel Medio	Nivel Alto
	✓ Debe existir uno o varios, designados por el responsable del fichero. ✓ Es el encargado de ***coordinar y controlar*** las medidas de seguridad. ✓ En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero ✓ También ha de gestionar la seguridad de los ***ficheros no automatizados*** (archivística)	
	Aplicable a ficheros automatizados y manuales	

2.- Documento de Seguridad - Requisitos

Nivel Básico	Nivel Medio	N. Alto
Establece y recopila, como mínimo: ✓ El Ámbito de aplicación. ✓ Las medidas, normas, procedimientos y estándares de seguridad. ✓ Las funciones y obligaciones del personal. ✓ La estructura de los ficheros y la descripción de los sistemas de información. ✓ Los procedimientos de gestión y respuesta ante incidencias. ✓ Los procedimientos de realización de las copias de respaldo y recuperación de datos. ✓ Las Medidas para el transporte, destrucción y reutilización de soportes.	Además debe contener: ✓ La Identificación del ***responsable de seguridad***. ✓ Los Controles periódicos del cumplimiento del documento.	
Aplicable a ficheros automatizados y manuales		

3.- Funciones y obligaciones del Personal

Nivel Básico	Nivel Medio	Nivel Alto
✓ Las funciones y obligaciones relacionadas con el acceso a datos personales habrán de estar claramente definidas y documentadas. ✓ Deben definirse las funciones de control y autorizaciones delegadas ✓ El personal debe conocer las normas que les afecten ✓ El personal debe conocer las consecuencias de su incumplimiento.		
Aplicable a ficheros automatizados y manuales		

9.- Procedimiento de Gestión de Incidencias

Nivel Básico	Nivel Medio	Nivel Alto
✓ Debe existir un Registro de Incidencias con: ✓ tipo de incidencia, ✓ cuándo se ha producido, ✓ persona que la notificia, ✓ persona a quien se comunica ✓ efectos derivados.	✓ Además, debe contener: ✓ Procedimientos efectuados para recuperación de los datos, ✓ persona que lo ejecuta, ✓ datos restaurados ✓ datos grabados manualmente. ✓ Es necesaria la autorización por escrito del responsable del fichero para su recuperación.	
Aplicable a ficheros automatizados y manuales	***Aplicable solo a ficheros automatizados***	

10.- Controles del Documento de Seguridad y Auditorías

Nivel Básico	Nivel Medio	Nivel Alto
✓ Realizar controles periódicos ✓ Mantener actualizado el Documento de Seguridad		

	✓ Al menos una auditoría cada dos años.
	✓ Cuando se realicen modificaciones sustanciales
	✓ Puede ser interna o externa.
	✓ Debe dictaminar sobre:
	  ✓ Adecuación de medidas y controles.
	  ✓ Deficiencias identificadas
	  ✓ Medidas correctoras necesarias.
	✓ El responsable de seguridad debe:
	  ✓ Analizar el informe de Auditoría
	  ✓ Elevar sus conclusiones al responsable del fichero
	✓ A disposición de la APD	

Aplicable a ficheros automatizados y manuales		

Marco #RGPD
Seguridad del Tratamiento:

Diario Oficial de la Unión Europea

L 119

Edición en lengua española

Legislación

59º año

4 de mayo de 2016

Sumario

I *Actos legislativos*

REGLAMENTOS

* Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (1) 1

Enfoque completamente distinto del RD-1720/2007

Marco #RGPD
Seguridad del Tratamiento

Artículo 32 - 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 riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, ***el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo***, que en su caso incluya, entre otros:

a)la seudonimización y el cifrado de datos personales;

b)la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c)la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Seguridad del Tratamiento (cont.)

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

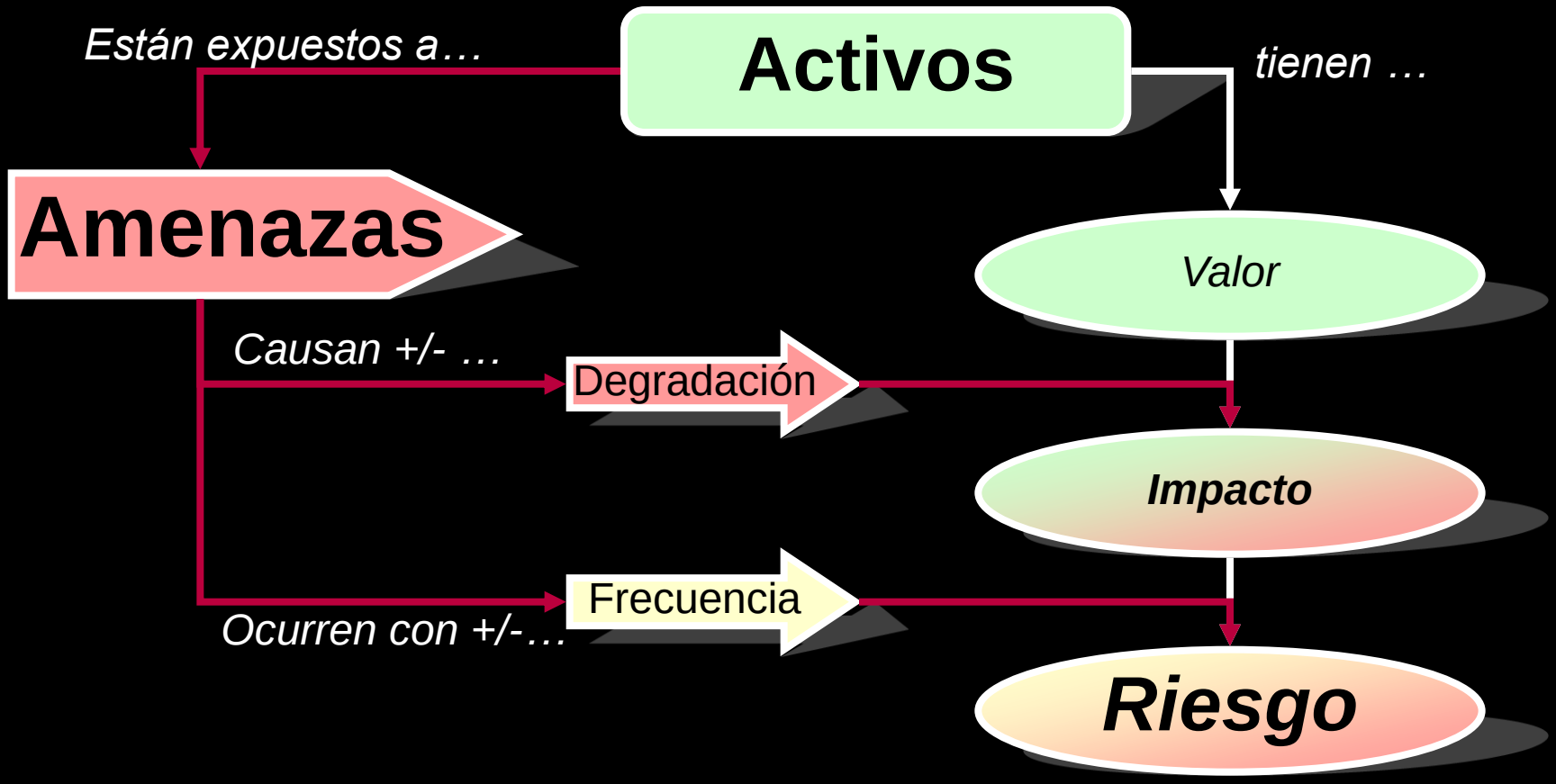
Marco #RGPD
Seguridad del Tratamiento

- Art. 32 #RGPD:
  "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,

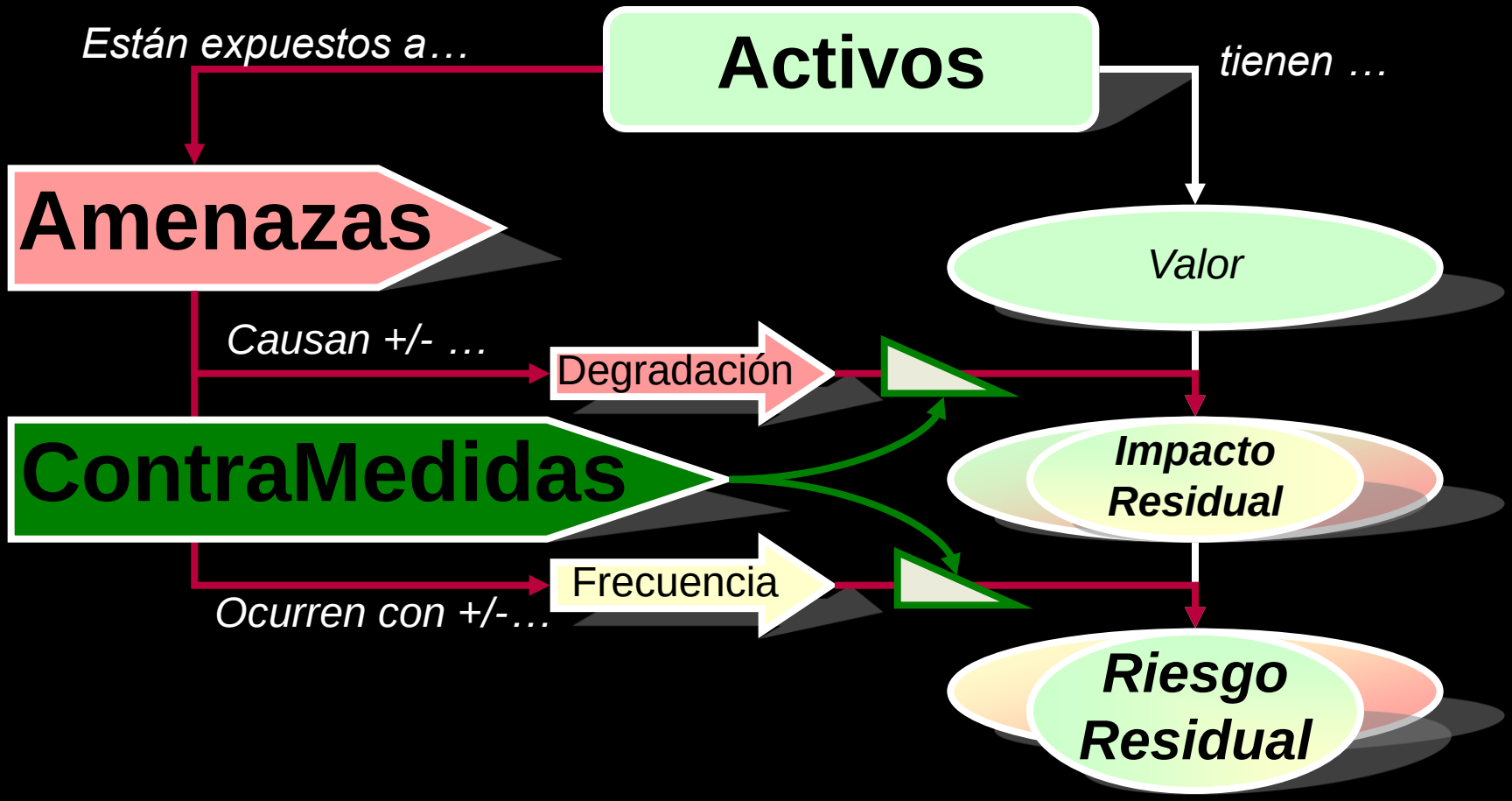
  así como
  - riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas,

  "el responsable y el encargado del tratamiento aplicarán:
  - medidas técnicas y organizativas apropiadas
  - para garantizar un nivel de seguridad
  - adecuado al riesgo"
- Orientación hacia "evaluación y gestión de riesgos"

Modelo de Análisis de Riesgos



Modelo de Gestión de Riesgos



Activos más comunes

- Instalaciones
  - Edificios, locales, canalizaciones, redes de comunicaciones,…
- Equipamientos
  - Mobiliario, maquinaria, ordenadores personales, …
- Sistemas de Información
  - Servidores, sistemas de almacenamiento,…
  - Aplicaciones y programas de ordenador
  - Información, datos de negocio, datos personales

Activos más comunes

- Intangibles
  - Licencias, derechos,..
  - Reputación, imagen, …
  - Personas de la Organización
- Servicios prestados
  - Continuidad del negocio

Activos en Protección de Datos

- Datos de Carácter Personal
- y, como consecuencia,
  - Instalaciones donde se ubican,
  - Equipos donde se tratan
  - Redes por donde “viajan”
  - Programas que los tratan
  - Soportes que los contienen
  - Personas que los gestionan

Amenazas más comunes

- Desastres naturales
  - Fuego, agua, … terremotos, …
- Desastres industriales
  - Explosiones, derrumbes, fallo de equipos,
- Interrupciones de servicios
  - Luz, agua, teléfono, internet, …
- Errores humanos no intencionados
  - De usuarios, de administradores, de operadores,
- Ataques intencionados
  - Contra personas, equipos, programas,
  - Posibles empleados desleales

Dimensiones de la seguridad de la Información

- Confidencialidad
  - Acceso o revelación indebidos
- Integridad
  - Modificación de los datos
- Disponibilidad
  - Sabotaje
- (Autenticidad)
  - Suplantación de Identidad

Medidas previstas en el #RGPD:

- a) la seudonimización y el cifrado de datos personales;
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Nuevos conceptos

- Resiliencia
  - "capacidad de soportar y recuperarse ante desastres"
- Seudonimización:
  - el tratamiento de datos personales de manera tal que:
    - ya no puedan atribuirse a un interesado sin utilizar información adicional,
    - siempre que dicha información adicional figure por separado
    - y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

Notificación de violaciones de seguridad

- Notificación a la Autoridad de Control
  - Salvo que haya un riesgo improbable
- Comunicación a los interesados
  - Siempre que haya un alto riesgo
  - salvo que se hayan aplicado medidas que minimicen el riesgo
  - O suponga un esfuerzo desproporcionado

CONCLUSIONES

Cómo gestionar la seguridad desde mayo de 2018?

- El RD-1720/2007 ya no sirve
- Ámbito de tratamientos privados:
  - Códigos de conducta y esquemas de certificación existentes y comúnmente aceptados: ISO-27000, ISO-29000, ISO-31000
  - Nuevos CC&Cert que puedan adoptarse
- Tratamientos de AAPP en España:
  - Normativas de autorregulación, como por ejemplo, ENS (Esquema Nacional de seguridad)

Puntos de Control ISO-27001

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

Octubre-2013

Puntos de Control en el ENS

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
				op	Marco operaciona
				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
AT	aplica	=	=	op.acc.1	Identificación
ICAT	aplica	=	=	op.acc.2	Requisitos de acceso
ICAT	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
ICAT	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
ICAT	aplica	+	++	op.acc.5	Mecanismo de autenticación
ICAT	aplica	+	++	op.acc.6	Acceso local (local logon)
ICAT	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoría	aplica	=	=	op.exp.4	Mantenimiento
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 incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	+	=	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas

				mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				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

Dimensiones				MEDIDAS DE SEGURIDAD	
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección de las comunicaciones
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad
IA	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
IC	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desarrollo
categoría	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoría	aplica	=	=	mp.info.1	Datos de carácter personal
C	aplica	+	=	mp.info.2	Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3	Cifrado
IA	aplica	+	++	mp.info.4	Firma electrónica
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos
D	n.a.	aplica	=	mp.info.9	Copias de seguridad (backup)
				mp.s	Protección de los servicios
categoría	aplica	=	=	mp.s.1	Protección del correo electrónico
categoría	aplica	=	=	mp.s.2	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

Gracias por la atención

http://www.flickr.com/photos/rosino/3658259716/