Junta de Castilla y León

eclap

JORNADA

APLICANDO LA NUEVA NORMATIVA SOBRE PROTECCIÓN DE DATOS

VALLADOLID, 17 DE OCTUBRE 2018

Mesa redonda: Nuestras obligaciones y responsabilidades como empleados públicos.

- **Las obligaciones de los empleados públicos.**

  Dña. Marta Abad Gutierrez. Coordinadora de Servicios de la Secretaría General. Delegada de Protección de Datos. Consejería de Agricultura y Ganadería. Junta de Castilla y León.

- **Las responsabilidades de los empleados públicos.**

  Dña. Elisa Casas Noriega. Técnico Jurídico de la Dirección General de Salud Pública. Delegada de Protección de Datos. Consejería de Sanidad. Junta de Castilla y León.

- **El Delegado de Protección de Datos.**

  Dña. Sara de la Viuda Linares. Técnico Asesor de la Secretaría General. Delegada de Protección de Datos. Consejería de Educación. Junta de Castilla y León.

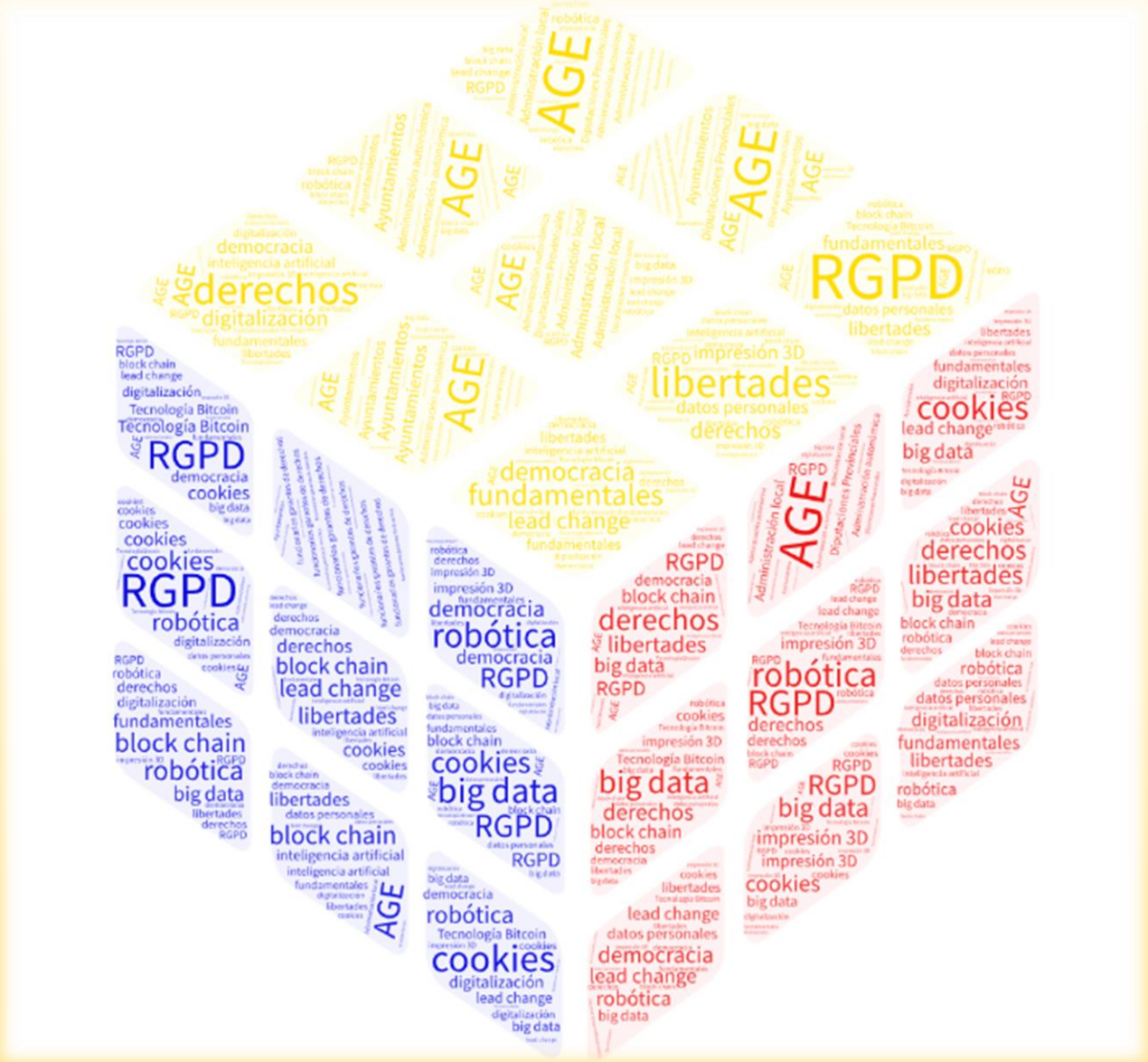
- **Problemática en la aplicación del RGPD.**

  D. Miguel Ángel del Barrio Moreno. Técnico Jurídico de Asuntos Sociales y Deportes. Delegado de Protección de Datos. Diputación de Segovia.

¿ POR QUÉ UN REGLAMENTO EUROPEO?

- Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016 (RGPD)
- De aplicación directa desde el día 25 de mayo de 2018
- Desplaza a la Directiva 95/46/CE
- Desplaza a la LOPD
- Regula un derecho fundamental, europeizado, autónomo del derecho a la intimidad y muy vinculado al desarrollo tecnológico

¿ SE APLICA ÍNTEGRAMENTE EL RGPD A LAS AAPP?




ADMINISTRACIÓN


N-120
RGPD

CONCEPTOS CLAROS

- ¿Qué es un dato de carácter personal?
- Categorías especiales de datos
- ¿Qué es un tratamiento de datos de carácter personal?
- ¿Quién es el responsable del tratamiento?
- ¿Quién es el encargado del tratamiento?
- Consentimiento del interesado

DATO DE CARÁCTER PERSONAL. CATEGORÍAS ESPECIALES DE DATOS

TRATAMIENTO DE DATOS PERSONALES EN LA ADMINISTRACIÓN

RESPONSABLE DEL TRATAMIENTO.
Autoridad pública

ENCARGADO DEL TRATAMIENTO:

- Debe ofrecer las garantías suficientes
- Se exige un contrato por escrito entre responsable y encargado

CONSENTIMIENTO

[ ] Se autoriza al Órgano competente para resolver, de acuerdo a lo establecido en el art…..,a obtener directamente y/o por medios telemáticos la información que estimen precisa para la determinación, conocimiento y comprobación de los datos en cuya virtud deba pronunciarse la resolución.

Se entenderá que no autorizan para la obtención de los datos necesarios si no se cumplimenta correctamente este apartado, dando lugar a la obligación de aportar la documentación necesaria para tramitar el procedimiento.

Vs

"Autoriza que sus datos personales aportados en la solicitud y contenidos en la documentación que en su caso la acompañe serán tratados por el órgano competente para resolver, con la finalidad de .....
(indicar las finalidades principales y accesorias del tratamiento)
Si no consiente en el uso de sus datos con la finalidad de…… marque la siguiente casilla □
Con la finalidad de..... autoriza que sus datos sean cedidos a..... (indicar destinatarios).
En caso de no autorizar la cesión, marque la siguiente casilla □

PRINCIPIOS QUE RIGEN NUESTRAS OBLIGACIONES EN RELACIÓN CON EL TRATAMIENTO DE DATOS

- **Licitud** (legalidad). Artículo 6 RGPD
- **Lealtad** (buena fe)
- **Transparencia**
- **Limitación de la finalidad**. Fines determinados, explícitos, legítimos. No tratados incompatiblemente con otros fines
- **Minimización de datos**
- **Exactitud**
- **Limitación del plazo de conservación**
- **Integridad** y **confidencialidad. Artículo 53 TREBEP**

DEBER DE SECRETO Y CONFIDENCIALIDAD DE LOS EMPLEADOS PÚBLICOS

Artículo 53 TREBEP:

Guardar secreto de las materias clasificadas u otras cuya difusión esté prohibida legalmente, manteniendo la debida discreción sobre aquellos asuntos que conozcan por razón de su cargo, sin que puedan hacer uso de la información obtenida para beneficio propio o de terceros, en perjuicio del interés público.

RESPONSABILIDAD PROACTIVA

- **Protección desde el diseño**

- **Protección por defecto. Estrategias:**
  - Need –to-know
  - Recogida de datos
  - Tratamiento de datos
  - Conservación
  - Accesibilidad

OBLIGACIONES RELATIVAS AL TRATAMIENTO DE DATOS

- Contar con el/la **DPD** de nuestra organización, colaborar con él/ella
- Asegurarnos de que nuestro tratamiento está recogido en el **Registro interno de actividades de tratamiento**, en su caso, incluirlo. Mantenerlo actualizado
- Revisar la **legitimidad** que fundamenta el tratamiento de datos
- **Revisar los contratos con los encargados de los tratamientos**
- Revisar **la información** que se ofrece a los interesados

OBLIGACIONES RELATIVAS A LOS DERECHOS DE LOS INTERESADOS. EL DERECHO DE INFORMACIÓN

De conformidad con lo establecido en los artículos 5 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa que los datos aportados en este formulario serán incorporados al fichero automatizado "……" creado para ……. Asimismo, se informa que los datos identificativos podrán ser comunicados a otros órganos administrativos para el cumplimiento de fines directamente relacionados con sus funciones legítimas. Podrán ejercitar los derechos de acceso, rectificación, cancelación y oposición previstos en la citada Ley, dirigiéndose a ……., mediante escrito, según modelos normalizados por Orden PAT/175/2003, de 20 de febrero.

Vs

Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A.
Finalidad	Gestión de la suscripción
Legitimación	Ejecución de un contrato
Destinatarios	No se cederán datos a terceros, salvo obligación legal
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/protecciondatos

Epígrafe	Información adicional (2ª capa, detallada)
"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 ampliada de los fines del tratamiento
	Plazos o criterios de conservación de los datos
	Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (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)	Destinatarios o categorías de destinatarios
	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	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)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
	Categorías de datos que se traten

OTROS DERECHOS DE LOS INTERESADOS

PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS DE LOS INTERESADOS

- Los responsables deben **facilitar** a los interesados **el ejercicio de estos derechos**
- El ejercicio de estos derechos será **gratuito** para el interesado
- La **solicitud** de ejercicio de los derechos debe **dirigirse al responsable** del tratamiento
- Es una **facultad del interesado acudir al DPD** pero el DPD no resuelve la solicitud
- El interesado debe **identificarse** en el momento de formular la solicitud
- El responsable **contestará** al interesado en el **plazo de un mes**
- Si el responsable decide no atender una solicitud, deberá informar de ello y **motivar la negativa**
- Si se trata gran cantidad de información sobre un interesado se le podrá pedir que **especifique la información**
- El responsable podrá **contar con la colaboración de los encargados**
- Es conveniente **incorporar la supervisión del DPD** cuando se vaya a resolver negativamente
- **Frente a una resolución negativa** de ejercicio de sus derechos **o una falta de respuesta**, el interesado puede presentar una **reclamación ante la AEDP**.

OBLIGACIONES RELATIVAS A LAS MEDIDAS DE SEGURIDAD

ANÁLISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

Antes: El Reglamento LOPD establecía las medidas de seguridad según tres niveles de exigencia: básico, medio y alto.

Ahora: El RGPD: “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 los **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.”

ANÁLISIS DE RIESGOS

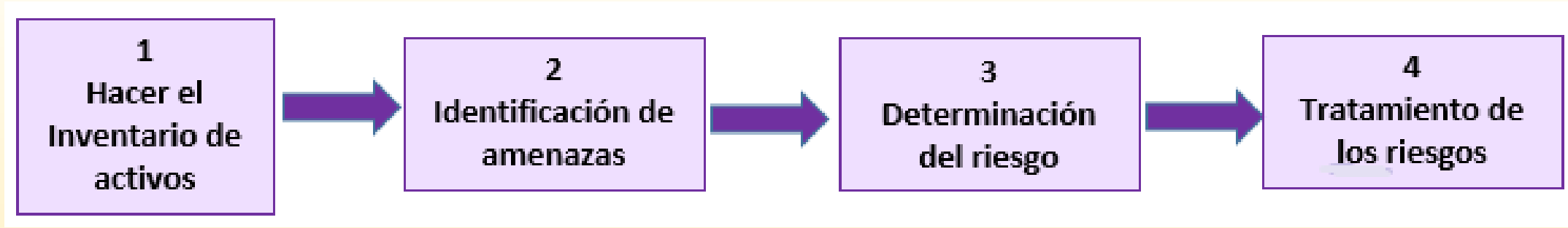
CONCEPTOS:

- **Activo**. Lo que queremos proteger
- **Amenaza**. Aquello de lo que queremos proteger al activo
- **Impacto**. Lo que podemos evitar.
- **Cuantificación del riesgo**:

RIESGO= IMPACTO X PROBABILIDAD

RIESGOS:

- Riesgo **tolerable**
- Riesgo **gestionable**
- Riesgo **inaceptable**



- **Inventario de activos:** instalaciones, equipamientos, sistemas de información, intangibles, datos de carácter personal, …
- **Amenazas:** Desastres naturales, interrupciones de servicios, errores humanos, … (creatividad)
- **Determinación del riesgo:**

ANÁLISIS DE RIESGOS				
ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
Servidor 01 (Contabilidad)	Fuga de información	2	3	6
Servidor 01 (Contabilidad)	Degradación de los soportes de almacenamiento de la información	1	3	3
Router Wifi (Clientes)	Caída del sistema por sobrecarga	1	2	2
Router Wifi (Clientes)	Denegación de servicio	2	1	2
Servidor 02 (Web)	Denegación de servicio	3	2	6
Servidor 02 (Web)	Corte del suministro eléctrico	1	2	2
…				
	(Añadir a la tabla tantas filas como sea necesario)			

Riesgo= probabilidad x impacto

- **Tratamiento de los riesgos.** Determinar las **medidas de seguridad**

EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS

Artículo 35 ***del RGPD***

Establece que ante la probabilidad de que un tratamiento *"entrañe un alto riesgo para los derechos y libertades de las personas físicas"* será necesario llevar a cabo una EIPD antes de la puesta en marcha del tratamiento. Esta obligación está alineada con el principio de privacidad que tiene como objetivo analizar un tratamiento desde su fase de diseño y garantizar una adecuada gestión de los riesgos, además de cumplir con los principios de necesidad y proporcionalidad.

Amenazas:

4.5.2016 ES Diario Oficial de la Unión Europea L 119/15

(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

También:

- Tratamientos dirigidos a la elaboración de perfiles
- Tratamientos a gran escala

OBLIGACIÓN DE CONOCER LAS MEDIDAS DE SEGURIDAD

- En el ámbito de las AAPP: **Esquema Nacional de Seguridad**
- La **metodología** para el análisis de riesgos es **"MAGERIT"** publicada por el Centro Criptológico Nacional
- Otras **normas y metodologías al uso**:
  - Las **normas ISO 31000** y **31010** para el análisis de riesgo en general
  - La **norma ISO 27005** para el análisis de riesgos para la seguridad de la información
  - **Guía práctica de análisis de riesgos** en los tratamientos de datos personales de la **AEPD**.

Identificador	Nombre del documento	Título	Propósito	Versión	Fecha de firma
P-02-AYG	P-02-AYG	P-02-AYG Gestion de accesos de usuario	El presente documento tiene por objeto describir los procedimientos a aplicar para el control de acceso de usuarios, tanto internos como externos, con acceso a los sistemas de información del Organismo Pagador, con el objetivo de garantizar que cada usuario tenga acceso autorizado únicamente a aquellos datos y recursos que precisa para el desarrollo de sus funciones, así como para el control de los registros de seguridad utilizados en el Sistema de Gestión de la Seguridad de la Información del Organismo Pagador de Castilla y León.	4	20/06/17
P-04-AYG	P-04-AYG	P-04-AYG Gestion de Activos	Este documento describe el procedimiento que se sigue en el Organismo Pagador de Castilla y León para elaborar y mantener el inventario de todos los activos relevantes que forman parte del alcance del Sistema de Gestión de la Seguridad de la Información.	1	6/06/16
P-06-AYG	P-06-AYG	P-06-AYG Seguridad física y del entorno	El presente procedimiento tiene por objeto establecer los criterios para garantizar el uso adecuado y eficaz de los controles para prevenir el acceso físico no autorizado a la información del Organismo Pagador y a los recursos de tratamiento de esta información. De tal modo, mediante este procedimiento se pretende dar cumplimiento al apartado A.11 del anexo A de la norma ISO/IEC 27001:2013.	2	18/05/17
P-07-AYG	P-07-AYG	P-07-AYG Gestión del cambio	Controlar los cambios en explotación que se producen en el OP que afectan a la seguridad de la información.	2	21/09/18
P-13-AYG	P-13-AYG	P-13-AYG Gestión de Vulnerabilidades	Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.	2	21/09/18
P-05-AYG	P-05-AYG	P-05-AYG Criptografía	El presente procedimiento tiene por objeto establecer los criterios para garantizar el uso adecuado y eficaz de los controles criptográficos para proteger la confidencialidad, la autenticidad y la integridad de la información.	2	21/09/18
A-02_P-08-AYG	A-02_P-08-AYG	A-01_P-08-AYG Politica uso servicios red corporativa	BOCYL-D-19072016-16 Politica uso servicios red corporativa ORDEN FYM/643/2016, de 12 de julio, por la que se determina la política de uso de los servicios de comunicaciones e informática prestados en la Red Corporativa de la Administración de la Comunidad de Castilla y León	1	17/08/16
PG-06-AYG	PG-06-AYG	PG-06-AYG Documento de Seguridad LOPD	Recoger las medidas de índole técnica y organizativa acorde a la normativa de seguridad vigente (LOPD) que será de obligado cumplimiento para el personal con acceso a los datos de carácter personal de nivel MEDIO.	1	18/05/17
N-01-AYG	N-01-AYG	N-01-AYG Alcance SGSI	Establecer del alcance de este Sistema de gestión con los siguientes objetivos: - Asegurarse de que el personal que actúa dentro del SGSI conoce los límites de dicho sistema una vez determinadas las cuestiones internas y externas de la organización. - Asegurarse de que las actividades que se desarrollan tanto a nivel interno como a nivel externo que son relevantes para el logro de los objetivos establecidos por la Dirección se llevan a cabo conforme a los requisitos de la norma ISO 27001.	3	20/01/17
N-02-AYG	N-02-AYG	N-02 Organización Seguridad	Describir el marco organizativo constituido por el conjunto de requisitos establecidos por la base normativa aplicable al Organismo Pagador en materia de seguridad de los sistemas de información.	3	20/01/17

Orden HAC/858/2014, de 30 de septiembre, por la que se aprueba la política de seguridad de la información de la Administración de la Comunidad de Castilla y León

La Administración de la Comunidad de Castilla y León considera la información un valor esencial para el cumplimiento adecuado de sus funciones. Y por lo tanto, asume la seguridad de la información como un objetivo estratégico, siendo necesario para establecer un sistema de gestión, formalizar un marco de referencia que garantice su disponibilidad, integridad y confidencialidad, evite su modificación o destrucción y nos ayude a reducir el riesgo de pérdida.

La Dirección General de Telecomunicaciones, mantiene dentro de sus objetivos el articular todas las acciones necesarias para que los procesos realizados dentro de la Junta de Castilla y León se desarrollen cumpliendo los requisitos de seguridad definidos por la normativa vigente.

- ¿Qué es la seguridad de la información?
- Política de Seguridad de la Junta de Castilla y León
- Política de uso de los servicios de comunicaciones e informática
- Incidentes de seguridad
- Modelos
- Organización de la seguridad
- Normativa sobre seguridad de la información
- Petición de acceso al portal colaborativo OTS

VIOLACIONES DE SEGURIDAD

- 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.

- El RGPD introduce la necesidad de gestionar las violaciones de seguridad de los datos.

- **El responsable debe comunicar las violaciones de seguridad siempre que exista un riesgo para los derechos y libertades de las personas físicas**

A la AEPD en el plazo máximo de 72 horas:

- Naturaleza de la quiebra de seguridad
- Categorías de afectados
- Nº aproximado de afectados
- Categorías de datos comprometidos
- Nº de registros de datos personales afectados
- Nombre y datos de contacto del DPD
- Posibles consecuencias de la quiebra de seguridad sufrida
- Medidas adoptadas o propuestas para remediar esta quiebra

A las personas físicas cuyos datos se hayan visto afectados cuanto antes.
Excepto:

- Se han adoptado medidas que hacen ininteligibles los datos para cualquier persona sin autorización
- Se han adoptado medidas que garanticen que ya no existe un alto riesgo para los derechos y libertades
- Que la comunicación fuese un esfuerzo desproporcionado, optándose por una comunicación pública o medida semejante.

- **Si el encargado del tratamiento sufre una quiebra de seguridad debe notificarlo sin dilación al responsable**

LEY 39/2015, DE 1 DE OCTUBRE – LEY 40/2015, DE 1 DE OCTUBRE – RGPD

Ley 39/2015, de 1 de octubre:

- **Artículo 28.** Los interesados no estarán obligados a aportar documentos que hayan sido elaborados por cualquier Administración, …. siempre que el interesado haya expresado su consentimiento… Se presumirá que…. es autorizada… salvo que conste oposición expresa.
- **Artículo 53.** Derechos de los interesados. A no presentar documentos originales…
- **Artículo 46.** Indicación de notificaciones y publicaciones. Si el órgano competente apreciase que la notificación … lesiona derechos o intereses legítimos, se limitará a publicar… una somera indicación…

Ley 40/2015, de 1 de octubre:

Artículo 155. 1. Obligación de cada Administración de facilitar al resto de las AAPP los datos relativos a los interesados que obren en su poder, especificando… con las máximas garantías de seguridad, integridad y disponibilidad.

2. La disponibilidad de datos ha de estar limitada estrictamente a aquellos que son requeridos a los interesados por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia, de acuerdo con la normativa reguladora de los mismos

Artículo 6 RGPD. Bases jurídicas para el tratamiento de datos

LEY 37/2007, DE 16 DE NOVIEMBRE– RGPD

RGPD:
Artículo 86. Tratamiento y acceso del público a documentos oficiales
Los datos personales … en posesión de alguna autoridad u organismo público… podrán ser comunicados… con el fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de datos...

Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público

Consagra como límite del derecho a la reutilización el derecho a la protección de datos.

Las AAPP deberán realizar un análisis de riesgos de la actividad de tratamiento que es la reutilización de datos/open data. Resultado:

- Puede llevarse a cabo la reutilización con datos personales. Tener en cuenta:
  - El principio de minimización de datos.
  - Indicar en la licencia de puesta a disposición de los documentos: la finalidad, los límites, la prohibición de revertir el proceso de disociación.
- Alto riesgo para los derechos y libertades de los interesados. La reutilización con datos personales no podrá llevarse a cabo sin adoptar medidas destinadas a la disociación de los datos.

NUESTRAS OBLIGACIONES SE RESUMEN EN TRES:

1ª. Documentar

2ª. Documentar

3ª. Documentar