Jornada sobre

PROTECCIÓN DE DATOS

Museo Arqueológico Provincial de Alicante (MARQ)
Salón de Actos
Plaza Dr. Gómez Ulla, s/n
03013 - Alicante

Martes, 12 de noviembre de 2019

Organizada por:

DIPUTACIÓN DE ALICANTE

Fundación Democracia y Gobierno Local

En colaboración con:

aepd agencia española protección datos

Proyecto co-financiado por el programa Derechos, Igualdad y Ciudadanía de la Unión Europea

T4DATA

PROTECCIÓN DE DATOS PERSONALES Y MEDIDAS DE SEGURIDAD EN LA ADMINISTRACIÓN LOCAL

Eva Rivera Fernández

datalawyers

MF
MARCA FRANCA

Medidas de seguridad

Regulación : RGPD + LOPDGDD + Normativa específica

¿quién es responsable? ¿quién las aplica?¿sobre qué? ¿cuándo? ¿dónde se plasman? ¿qué medidas se aplican?

Medidas concretas: Esquema Nacional de Seguridad

Gestión de las Violaciones de seguridad

Infracciones

Las obligaciones de seguridad se exigen al **responsable del tratamiento** que:

- Aplicará **medidas técnicas y organizativas apropiadas**
- a fin de **garantizar y poder demostrar** que el tratamiento es **conforme al RGPD y la LOPDGDD**

También a los encargados de tratamiento, corresponsables y a quienes intervengan en el tratamiento de datos.

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.

Ámbito de aplicación (I)

Servicios a las Personas

- Gestión de los servicios sociales y de las políticas de inclusión social.
- Promoción del deporte y de actividades deportivas y gestión de equipamientos deportivos de uso público y titularidad municipal
- Cultura y de actividades culturales y gestión de equipamientos culturales de uso público
- Políticas de integración social
- Políticas de juventud

Actividad y Promoción Económica

- Turismo local
- Desarrollo local económico y social y políticas de fomento o planes locales de empleo
- Políticas en materia de cooperación para el desarrollo

Área Institucional, organizativa y de seguridad

- Policía local, ordenación del tráfico, seguridad vial, estacionamiento de vehículos
- Actividades organizadas en espacios públicos y en los lugares y establecimientos de pública concurrencia
- Materia de animales de compañía y potencialmente peligrosos
- Estructuras de participación ciudadana, transparencia, buen gobierno y acceso a las nuevas tecnologías, administración electrónica, racionalización y simplificación de procedimientos

Área de Territorio e Infraestructuras

- Conservación del patrimonio histórico municipal y elaboración y aprobación de planes especiales de protección
- Gestión, ejecución y disciplina en materia urbanística
- Gestión del uso de servicios, equipamientos, infraestructuras e instalaciones públicas de titularidad municipal

Ámbito de aplicación (II)

Identificación de tratamientos:

- Datos personales
- Colectivos de interesados
- Categorías de datos
- Fines de tratamientos
- Sistemas de tratamiento

Operaciones de tratamiento

- Obtención, acceso, modificación, organización, consulta, cotejo estructuración, transmisión, conservación, almacenamiento, supresión

Tratamientos efectuados / Diseño del tratamiento

Dirección/ubicación:

Servicio/ concejalía:

Organigrama:

Actividad	**Prestación directa**	**Prestación por terceros** (identificar a la empresa)	**Finalidad**	**Origen y procedencia de los datos**	**Colectivos afectados**	**Datos recabados**	**Datos de categorías especiales**	**Sistema de tratamiento** (papel y en automatizado, en cuyo caso indicar software principal)	**Destinatarios de los datos** (a quién se le comunican)	**Personas del Ayuntamiento que acceden y tratan los datos**	**Archivo de la documentación** (indicar lugar , medidas de seguridad y personas autorizadas para acceder)

Ejemplo

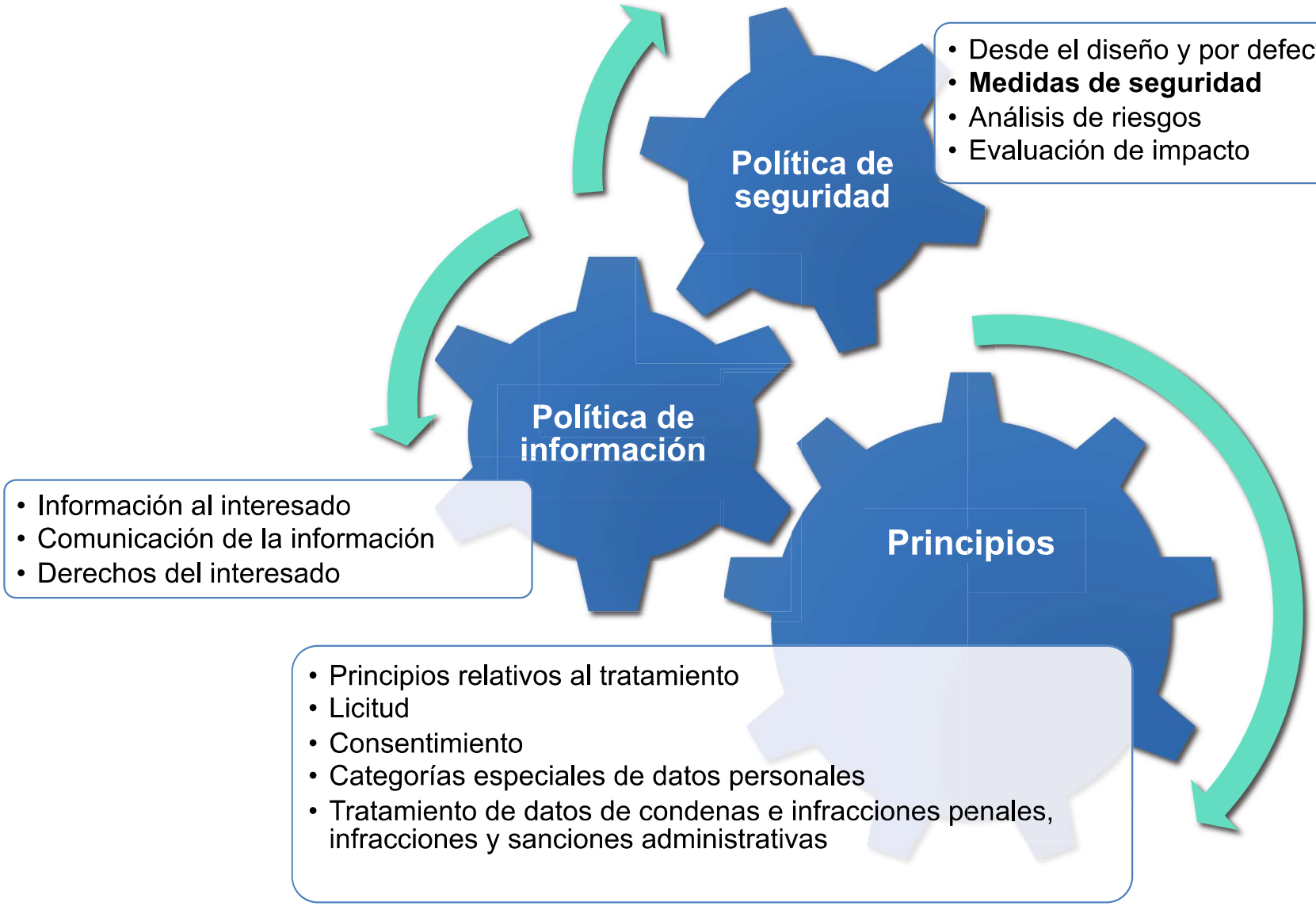
En el momento del tratamiento

En el momento en el que se determinan los medios del tratamiento

El RT y ET deberán garantizar desde el diseño y por defecto:

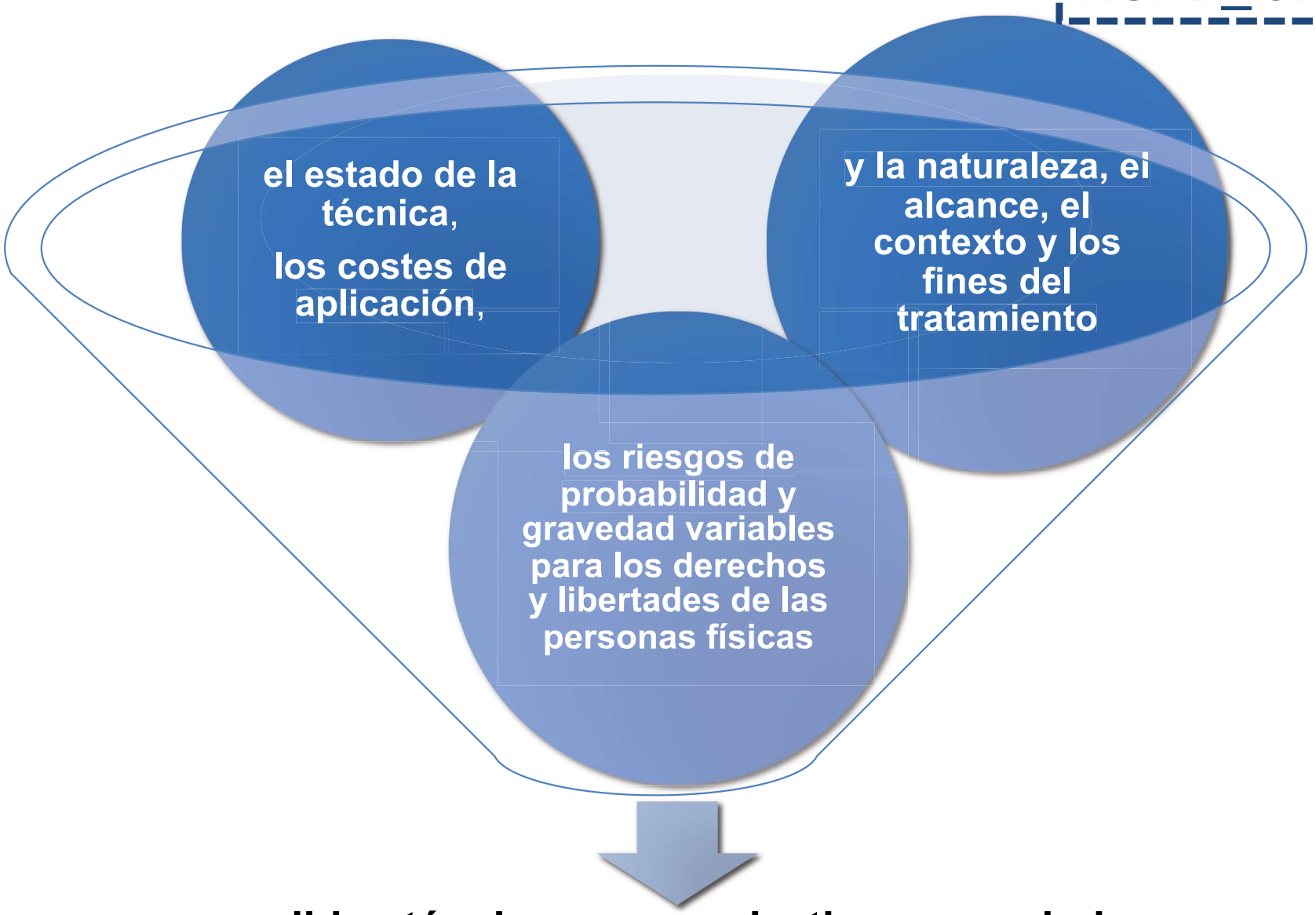
- Que el tratamiento se realice para fines específicos.
- Que sólo sean objeto de tratamiento los datos que sean necesarios para cada uno de los fines del tratamiento.
- La exactitud, confidencialidad, integridad, seguridad física y supresión de los datos.
- La protección de los derechos del interesado.
- Que los datos no sean accesibles a un número indeterminado de personas.
- La aplicación de los resultados de la evaluación de impacto, en su caso

Conformidad legal



Medidas de seguridad

RGPD_ artículo 32



medidas técnicas y organizativas apropiadas

garantizar un nivel de seguridad adecuado al riesgo

RGPD_ artículo 32

medidas técnicas y organizativas apropiadas garantizar un nivel de seguridad adecuado al riesgo

Análisis de riesgos

Tipos de medidas tales como:

- Seudonimización
- cifrado de datos personales
- garantizar la **confidencialidad**,
- garantizar la **integridad**
- garantizar la **disponibilidad**
- garantizar **la resiliencia permanente de los sistemas y servicios de tratamiento;**
- **restaurar la disponibilidad y el acceso a los datos personales de forma rápida**

proceso de verificación evaluación y valoración de la eficacia:

*destrucción,

* pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma,

*la comunicación o acceso no autorizados a los datos

Análisis de riesgos

Consiste en examinar de forma **continua** todas las operaciones de tratamiento llevadas a cabo con los datos con el fin de **identificar las amenazas**, **diagnosticar si existen riesgos** y **tratarlos para minimizar la probabilidad y el impacto** de que se materialicen con el fin de conseguir un nivel de se considere razonable.

- En el ENS se establecen los criterios para la realización de un análisis de riesgos y las pautas para establecer medidas de seguridad adecuadas.

Centro Criptológnico Nacional se propone una herramienta de análisis de riesgos **PILAR**, que facilita la gestión **normativa tanto del Reglamento Europeo de Protección de Datos (RGPD) como del ENS** (versión 7.1.7)

Análisis de riesgos

El responsable o el encargado:

- **deben evaluar los riesgos inherentes al tratamiento** determinar los riesgos concretos
- **aplicar medidas para mitigarlos**

✓ Determinar las actividades del tratamiento
✓ Identificar las situaciones de riesgos
✓ Analizar los riesgos
✓ Evaluar
✓ Tratarlos: minimizar la probabilidad y la gravedad
✓ Verificar/ revisar

Evaluación de Impacto

¿qué es?

- ***"es una herramienta con carácter preventivo*** *que debe realizar el responsable del tratamiento para 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"* _ Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD (AEPD)

¿quién debe de realizar?_

- El RT

¿cuándo? _

- antes de realizar el tratamiento

¿en qué casos?_

- **Cuando sea probable que un tipo de tratamiento que entrañe un alto riesgo para los derechos y libertades de las personas físicas**.
  - a)Evaluación sistemática y exhaustiva de aspectos personales de personas físicas, que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar
  - b)Tratamiento a gran escala de las categorías especiales de datos y datos relativas a condenas e infracciones penales
  - c) Observación sistemática a gran escala de una zona de acceso público

¿una por cada tipo de tratamiento?

- el RGPD específicamente establece que podrá abordar una serie de operaciones de tratamiento similares que entrañan altos riesgos similares.

Evaluación de Impacto

La AEPD ha publicado una lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)

- **https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf**

Algunos tratamientos que requieren EIPD_

- Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia
- Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.
- (…)

Otras referencias a las medidas de seguridad en la normativa de aplicación

Considerando (78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento**. A fin de poder demostrar la conformidad con el presente Reglamento**, el responsable del tratamiento debe **adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto**. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, **dar transparencia a las funciones y el tratamiento de datos personales**, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al **desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento** de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que **tengan en cuenta el derecho a la protección de datos** cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. **Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos**.

Otras referencias normativas a las medidas de seguridad

En relación al **Registro de Actividades** (artículo 30 g) “cuando sea posible, una **descripción general de las medidas técnicas y organizativas de seguridad** a las que se refiere el artículo 32.1

RGPD Artículo 5. **Principios** relativos al tratamiento. 1. Los datos personales serán: f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales**, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas** («integridad y confidencialidad»).

Considerando 39 (final) Los datos **personales deben tratarse de un** modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

Medidas de seguridad en el ámbito del sector público

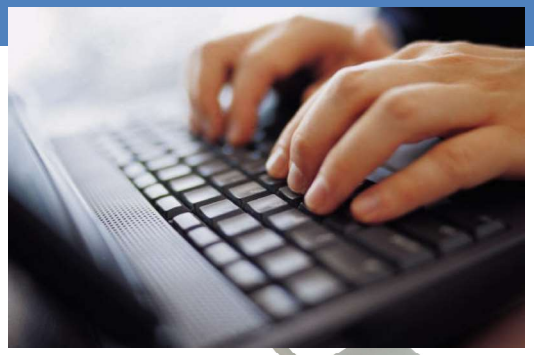
LOPDGDD_ Disposición adicional 1ª

- El **Esquema Nacional de Seguridad (ENS)** incluirá las medidas que deban implantarse en caso de tratamiento de datos personales, adaptando los criterios de determinación del riesgo a lo establecido en el **artículo 32 del RGPD**.

- Los siguientes RT (artículo 77.1) deberán aplicar a los tratamientos de datos personales las **medidas de seguridad previstas en el ENS e impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a ellos**:
  - Los órganos constitucionales o con relevancia constitucional.
  - Los órganos jurisdiccionales.
  - **La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.** (….)

Cuando un tercero preste servicios a una Administración pública en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad **se corresponderán con las de dicha administración y se ajustarán al ENS**


Esquema Nacional
de Seguridad
Protección
de datos
personales
Anexo I_ Categoría de los sistemas básica, media , alta en función de la valoración del impacto que tendrá el incidente para la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad
Anexo II_ Medidas de seguridad




CONFIDENTIAL


DATA

ENS_ marco organizativo

4

- Política de seguridad
- Normativa de seguridad
- Procedimientos de seguridad
- Proceso de autorización

ENS_ marco organizativo

Política de seguridad:

- Objetivos
- Marco legal
- Roles y funciones de seguridad; descripción de designaciones, renovaciones, responsabilidades y deberes
- Estructura del comité para la gestión y coordinación de la seguridad, estableciendo deberes y responsabilidades
- Directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Normativa de seguridad, formada por documentos que describan:

- Uso correcto de equipos, servicios e instalaciones
- Qué se entiende por uso indebido
- Responsabilidad del personal en relación al cumplimiento de estas normas.

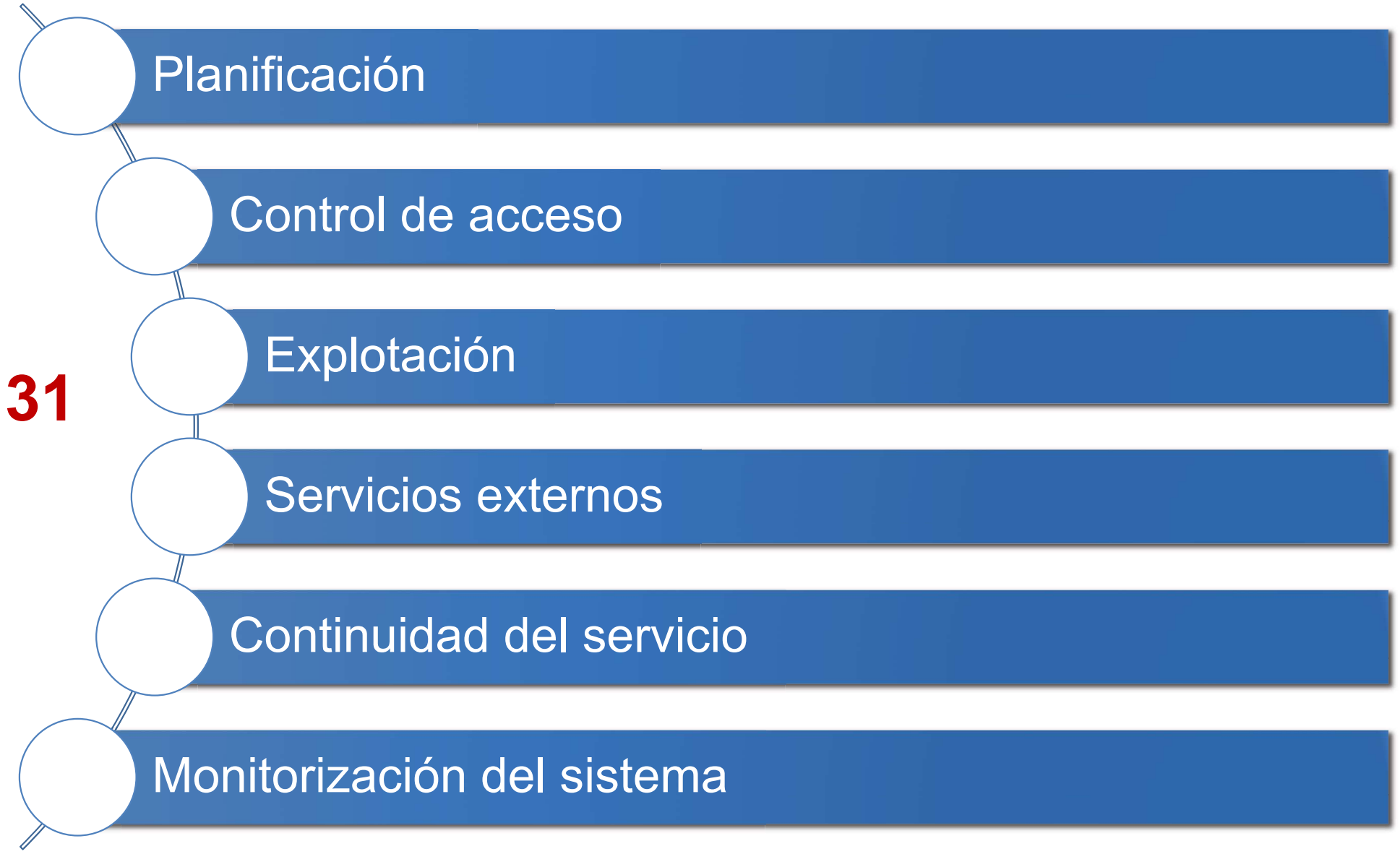
Procedimientos de seguridad que detallen de forma clara y precisa:

- Cómo y quién debe de llevar a cabo cada tarea
- Cómo identificar y notificar comportamientos anómalos

Proceso de autorización formal en relación al sistema de información:

- Utilización de instalaciones, habituales y alternativas
- Entrada de equipos
- Entrada a aplicaciones
- Establecimiento de enlaces de comunicaciones con otros sistemas
- Utilización de medios de comunicación
- Utilización de soportes
- Utilización de equipos móviles (ordenadores portátiles, smartphones…)

ENS_ marco operacional



ENS_ marco operacional

Planificación

- Instalaciones
- Información del sistema: equipo, redes internas, punto de acceso al sistema, puestos de trabajo
- Sistemas de identificación y autenticación de usuarios
- Medidas de seguridad técnicas (cortafuegos…etc)

Control de acceso:

- Identificadores únicos, políticas de inhabilitación de cuentas,etc
- Privilegios y autorizaciones
- Autenticación: contraseñas, datos biométricos, certificados electrónicos
- Intentos permitidos y registro de accesos
- Accesos remotos

Explotación:

- Inventario de activos y configuración
- Sistemas de prevención y reacción frente a malware, virus, troyanos, etc.
- Gestión de incidentes, **violaciones de la seguridad**

Servicios externos:

- Contratación y acuerdo de nivel de servicio, estableciendo las responsabilidades de las partes

Continuidad del servicio:

- Evaluación de impacto
- Plan de continuidad
- Pruebas periódicas

Monitorización del sistema

ENS_ medidas de protección

40

- Protección de las instalaciones e infraestructuras
- Gestión del personal
- Protección de los equipos y de los soportes
- Protección de las comunicaciones
- Protección de las aplicaciones informáticas
- Protección de la información
- Protección de los servicios

ENS_ medidas de protección (I)

Protección de las instalaciones

- Identificación de las personas que acceden a los locales, registros de entrada y salida
- Acondicionamiento de los locales (temperatura, humedad, …)
- Protección frente a incendios/ inundaciones
- Registro de entrada y salida de equipamiento incluyendo identificación de las personas

Gestión del personal

- Definición de responsabilidad, deberes y obligaciones, medidas disciplinarias, etc.
- Concienciación sobre normativa, bien uso, incidentes de seguridad
- Formación para gestionar la información, almacenamiento, copias, distribución, etc.
- Personal alternativo para sustituir al personal habitual

Protección de los equipos

- Puestos de trabajo despejados y cerrados si no se está utilizando
- Bloqueo de equipo y necesidad de contraseña para reanudar la actividad
- Protección de portátiles y otros hardware con alto riesgo de pérdida o robo

Protección de las comunicaciones

- Perímetro seguro mediante sistemas de cortafuegos
- Protección de la confidencialidad empleando VPN, certificados, etc.
- Protección de la autenticidad y de la integridad
- Segregación de redes

ENS_ medidas de protección (II)

Protección de los soportes de información

- Etiquetado sin revelar contenidos
- Criptografía que garantice la integridad y confidencialidad
- Custodia, transporte, borrado y destrucción

Protección de las aplicaciones informáticas

- Verificación de criterios de seguridad y pruebas con datos no reales, coherencia en la integración

Protección de la información

- Calificación de la información según establece la Política de Seguridad, determinación de responsables, nivel de seguridad, procedimientos para etiquetar y tratar la información
- Firma electrónica como medio de comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio
- Sellos de tiempo
- Limpieza de documentos: incumplimiento de esta medida puede perjudicar el mantenimiento de la confidencialidad de información
- Copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada y en relación a las aplicaciones en explotación, incluyendo los sistemas operativos, datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga, las claves utilizadas para preservar la confidencialidad de la información.

Protección de los servicios

- Protección del correo electrónico (cuerpo y adjuntos), protección frente a spam y programas dañinos, limitaciones en relación a comunicaciones privadas, etc… lo que supone concienciación y formación sobre el uso del email
- Protección de aplicaciones web

Documentación y garantías

El responsable del tratamiento será responsable del cumplimiento y capaz de demostrarlo («responsabilidad proactiva»).

- el cumplimiento de principios
- la información a los interesados
- consentimientos explícitos
- cláusulas web
- firma de contratos
- iconos informativos
- registro de actividades de tratamiento
- protocolo para la atención de los derechos del interesado.
- registro de acuerdos de confidencialidad con el personal autorizado.
- registro de contratos de protección de datos con empresas externas.
- **registro de los incidentes de seguridad (documentación, resolución y notificación).**
- **medidas de seguridad**
- **análisis de riesgos**
- **evaluación de impacto**
- participación de los intervinientes en formaciones
- auditoría de cumplimiento del RGPD
- medidas correctivas a implementar
- **Acreditar formación a los intervinientes**

Medidas de seguridad - intervinientes

- Personal debe de ser:
  - Formado, porque es el que gestiona
  - Escuchado, porque conoce de primera mano las particularidades de la prestación del servicio.

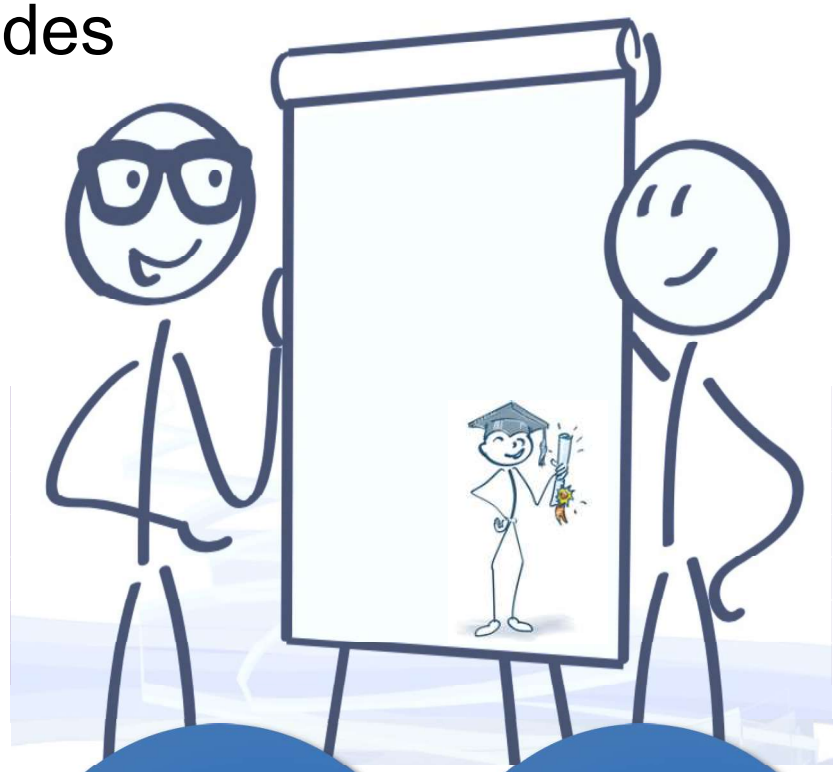
(Medidas de seguridad – intervinientes)

Diseñar las medidas de seguridad en función de las necesidades, para que realmente sean efectivas y, su diseño y cumplimiento, garantice el **derecho a la protección de datos**

Planes de formación

Plan formativo, según las necesidades del puesto de trabajo:

- itinerario formativo _ evaluación
- la periodicidad de la formación



Para favorecer:

- cumplimiento y la puesta en practica de las políticas y los protocolos de seguridad
- ejecución de los protocolos para el ejercicio de derechos
- aplicación de medidas de seguridad
- cumplimiento del deber de confidencialidad en relación a la información del RT
- activación de los **protocolos establecidos en relación con las quiebras de seguridad**

Incidentes de seguridad

"Guía para la gestión y notificación de brechas de seguridad" publicada en la web aepd.es

¿qué es un incidente de seguridad?

ENS define “ incidente de seguridad”: como aquel suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información

RGPD: “violaciones de seguridad de los datos personales como aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida, o alteración accidental o o ilícita de datos personales transmitidos, conservados o tratados de otra forma o la comunicación o acceso no autorizados a dichos datos

ENS asigna al Centro Criptológico Nacional (CCN) la coordinación en materia de respuesta a incidentes de seguridad para articular mecanismos de respuesta a los incidentes de seguridad mediante la estructura del CCN-CERT, obligando a la notificación de incidentes de seguridad a las AAPP

Obligación de gestionar las brechas de seguridad

(propone la herramienta LUCIA)

Documentarlas: garantía de responsabilidad proactiva

Considerando 87) **Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado**. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento

PROTOCOLO DE ACTUACIÓN PARA GESTIONAR LAS BRECHAS DE SEGURIDAD

Protocolo de actuación

- Si el incidente se considera brecha de seguridad, en la que se han comprometido datos personales, se inicia el proceso de análisis, respuesta y notificación a la autoridad de control competente y a los afectados, si procede, resolución y cierre.

- Asesorarse con expertos
- Delegar en el encargado del tratamiento
- Apoyarse en el DPO, en caso de que haya sido designado)

El RT deberá **documentar** **cualquier violación de la seguridad** de los datos personales producida bajo su responsabilidad y **notificarla** **a la AC**, sin dilación indebida, a ser posible en un **máximo de 72 horas** desde que se haya tenido constancia de ella.

- En el caso de notificarla a la Autoridad de control pasadas 72 horas desde que se haya tenido conocimiento, deberá acompañarse una justificación motivada

Cuando la violación se haya producido bajo la **responsabilidad del ET**, éste lo notificará al RT sin dilación indebida

No será necesario notificar una violación de datos a la Autoridad de control cuando sea **improbable que la vulneración de los datos personales constituya un riesgo para los derechos y las libertades de los interesados _ (pueda demostrarlo)**

Contenido a documentar

La naturaleza y contexto de la violación

Los posibles efectos y consecuencias de la violación

Las medidas correctivas adoptadas o propuestas por el Responsable del tratamiento para remediar y mitigar los efectos ocasionados

Cuando sea posible las categorías y número de interesados y registros afectados.

Si es el caso, la identidad y los datos de contacto del DPO u otros contactos para obtener más información.

*Si no es posible facilitar toda la información en una comunicación, se notificará por etapas sin dilación indebida

Protocolo de actuación en relación a las violaciones de la seguridad

Fecha: **Centro de trabajo/ubicación**

Afecta a:

☐ Confidencialidad ☐ Integridad ☐ Disponibilidad

Registro y valoración

Categoría o nivel de criticidad *(respecto a la seguridad de los sistemas afectados)*

- ☐ Crítico
- ☐ Muy Alto
- ☐ Alto
- ☐ Medio
- ☐ Bajo

Severidad de las consecuencias *(para los individuos afectados)*

- ☐ Baja
- ☐ Media
- ☐ Alta
- ☐ Muy Alta

Naturaleza, sensibilidad y categorías de los datos personales afectados:

- ☐ Datos de escaso riesgo *(datos de contacto e identificativos)*
- ☐ Datos de comportamiento *(localización, hábitos y preferencias)*
- ☐ Datos financieros *(transacciones, posiciones, ingresos, cuentas, factura, etc.)*
- ☐ Datos sensibles *(de salud, biométricos, datos relativos a la vida sexual, etc.)*
- ☐ Datos legibles/ilegibles *(Datos protegidos mediante algún sistema de seudonimización, por ejemplo, cifrado o hash)*
- ☐ Otros:

Ejemplo

Protocolo de actuación en relación a las violaciones de la seguridad

individuos a partir de los datos involucrados en la brecha)

Características especiales de los individuos *(Si afectan a individuos con características especiales o con necesidades especiales)*

Ejemplo

Número de individuos afectados	**El número y tipología de los sistemas afectados**

Perfil de los usuarios afectados *(posición en la estructura organizativa y privilegios de acceso a la información)*

El impacto que la brecha puede tener en la organización *(imagen, protección de la información, conformidad legal, etc.)*	**Notificación a la Autoridad de Control**
☐ Baja ☐ Media ☐ Alta	☐ Si ☐ No

Valoración/ comentario del responsable

Quiebras de seguridad - Interesados

El RT comunicará una violación de datos al interesado, sin dilación indebida, cuando :

- Sea probable que presente un alto riesgo para los derechos y libertades del interesado.
- Le sea exigido por la Autoridad de control

No será necesaria la comunicación de una violación de datos al interesado cuando el RT pueda demostrar:

- Que se han adoptado medidas técnicas y organizativas apropiadas de protección para hacer ininteligibles los datos a personas no autorizadas y que estas se han aplicado a los datos afectados.
- Que se han tomado medidas posteriores que garantizan que ya no sea probable un alto riesgo para los derechos y libertades del interesado.
- Que supusiera un esfuerzo desproporcionado. En este caso, se podrá optar por una comunicación pública que sea igualmente efectiva para informar al interesado

Contenido de la comunicación:

- Una descripción de la naturaleza de la violación.
- Las posibles consecuencias de la violación.
- Las medidas correctivas adoptadas o propuestas por el RT para remediar y mitigar los efectos ocasionados.
- Si es el caso, la identidad y los datos de contacto del DPO u otros contactos para obtener más información

Tratamientos de datos derivados de las notificaciones de incidentes de seguridad **LOPDGDD. Disposición adicional novena**

Cuando deban notificarse incidentes de seguridad, las entidades encargadas de dicha notificación podrán **tratar los datos exclusivamente durante el tiempo y alcance necesarios** para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

- Dichas entidades son:
  - las autoridades públicas competentes
  - equipos de respuesta a emergencias informáticas (CERT)
  - equipos de respuesta a incidentes de seguridad informática (CSIRT)
  - proveedores de redes y servicios de comunicaciones electrónicas
  - proveedores de tecnologías y servicios de seguridad

Infracciones

Sanciones

LOPDGDD. Artículo 74. Infracciones consideradas leves.

Se consideran **leves** y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los **apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679** y, en particular, las siguientes: (…)

- m) La **notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679**.
- n) El **incumplimiento de la obligación de documentar cualquier violación de seguridad**, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.
- ñ) El **incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento** (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.

LOPDGDD Artículo 73. *Infracciones consideradas graves*. En función de lo que establece el **artículo 83.4 del Reglamento (UE) 2016/679** se consideran **graves** y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquél, y en particular las siguientes: (…)

- f) **La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.**
- q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.
- r) **El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.**
- s) **El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad** de protección de datos para llevar a cabo dicha notificación.

Muchas gracias

datalawyers

MF

MARCA FRANCA