

# Informe del Análisis de Riesgos sobre Protección de Datos Personales (RGPD y LOPDyGdd)

14/01/2021

AYUNTAMIENTO DE LAUJAR DE ANDARAX





### 00 - Indice de Contenidos.

- 01.- Informe Ejecutivo.
- 02.- Definiciones.
- 03.- Alcance del Análisis y Metodología Empleada.
- 04.- Definir como gestionar las Medidas de Seguridad.
- 05.- Categorización de Activos. Categoría ENS de las Actividades de Tratamiento.
- 06.- Análisis de la Necesidad de realizar una EIPD.
- 07.- Identificación y Categorización de Amenazas - Riesgo Potencial.
- 08.- Evaluación del Riesgo - Riesgo Potencial.
- 09.- Tratamiento del Riesgo - Nivel de Madurez de las Medidas de Seguridad.
- 10.- Estimación del Estado del Riesgo.
- 11.-Revisión del Documento.
- 12.- Aprobación del Documento.
- 13.- Anexos



## 01- Resumen Ejecutivo.

El presente documento recoge los resultados del análisis de riesgos realizado por la AYUNTAMIENTO DE LAUJAR DE ANDARAX, en adelante la Entidad, en el marco del Reglamento (UE) 2016/679 del Parlamento Europeo (Reglamento General de Protección de Datos), en adelante RGPD, así como en la Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales (LOPDgdd), y en el que se recogen los principales riesgos identificados, y las medidas de seguridad para mitigar el nivel de riesgo,

Los principales riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, se pueden diferenciar en 2 dimensiones:

- Riesgos asociados a la protección de la información con foco en la integridad, disponibilidad y confidencialidad de los datos. Por ejemplo, acceso ilegítimo a los datos o pérdida de datos.
- Riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados. Por ejemplo, uso ilegítimo de datos personales o la posibilidad de que el responsable no pueda atender el ejercicio de los derechos que el RGPD reconoce al titular de los datos porque la organización no tiene correctamente implementados y operativos los procedimientos correspondientes.

El Análisis de Riesgos se ha realizado teniendo como referencia:

- - Las Amenazas y Medidas de seguridad:
  - Para el cumplimiento normativo el Anexo V de la "Guía práctica para la Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD" publicada por la AEPD (ver al guía).
  - Para la Confidencialidad, Disponibilidad e Integridad de los datos personales lo dispuesto en el Esquema Nacional de Seguridad contenido en el Anexo II del Real Decreto 3/2010 de 8 de enero y modificado por el Real Decreto 951/2015 de 23 de octubre.
- - La valoración de riesgos:
  - Para el cumplimiento normativo la "Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD" publicada por la AEPD (ver guía).
  - Para la Confidencialidad, Disponibilidad e Integridad de los datos personales el análisis de riesgos que se obtenga en la Adecuación al ENS con la herramienta PILAR, del Centro Criptológico Nacional.

Considerando los requisitos de seguridad definidos, el grado de madurez de las salvaguardas actuales y las posibles amenazas que podrían materializarse, el nivel de riesgo estimado, considerando el Registro de Actividades de Tratamiento de Datos Personales como los activos esenciales, tenemos un Riesgos con los siguientes valores:

- **RIESGO POTENCIAL: 3 (MEDIO)**
- **RIESGO ACTUAL: 2,7 (MEDIO)**

Aplicando en una escala de 0 a 16 los siguientes criterios: 0-2 (BAJO), 2-6 (MEDIO), 6-9 (ALTA), 9-16 (MUY ALTO), se considera un riesgo potencial inherente de un **3** que es considerado como **MEDIO** y un riesgo actual en función de las salvaguardas implantadas actualmente y del estado actual de la seguridad de **2,7** que es considerado como **MEDIO**.

En general, el nivel de cumplimiento observado en relación a la protección de datos personales esta mejorando, con el proyecto de adecuación a RGPD que se esta llevando a cabo para AYUNTAMIENTO DE LAUJAR DE ANDARAX por una empresa externa, y gracias a las acciones formativas realizadas en los Planes de Formación de la Diputación de Almería, existe conocimiento sobre Seguridad de la Información y la Protección de Datos Personales, pero es necesario seguir trabajando en la concienciación y en la formación, para mejorar el nivel de cultura en estos temas.



Desde la Diputación de Almería, se ha llevado a cabo la dinamización del Comité de Seguridad, que actúa como Delegado de Protección de Datos de Diputación y de las EELL de la provincia que lo soliciten y cumplan con los requisitos establecidos. Además, y se está realizando la implantación de una herramienta para la gestión de la protección de datos personales y del registro de actividades de tratamiento, y la gestión de los riesgos para los tratamientos identificados (proDatos), para ello se está contando con la colaboración de las empresas externas que está llevando un proyecto de Adecuación al RGPD para Diputación y para otros 54 Ayuntamientos. Se han identificado varios aspectos que requieren atención preferente respecto al cumplimiento de los artículos del RGPD:

- - Se debe instalar, configurar y poner en marcha una herramienta específica para la gestión de incidencias relativas a seguridad de la información. El aplicativo debe poder identificar las incidencias que afectan a datos personales, y se deben generar los avisos pertinentes al Delegado de Protección de Datos para que pueda evaluar la incidencia, así como la necesidad (o no) de comunicación de la misma a la AEPD y/o a los usuarios afectados.
- - Se deben definir y aprobar procedimientos que incluyan los mecanismos, protocolos, periodicidad, y roles implicados en los procesos de actualización del RAT, ante la identificación de nuevos tratamientos de datos personales, o modificaciones de los existentes.
- - Se debe dar continuidad a las acciones formativas y de concienciación en materia de seguridad de la información y protección de datos personales.
- - Se debe elaborar un registro de encargados del tratamiento que la Entidad realiza a terceros (Otras Administraciones, etc..).
- - Previamente, se debe incluir en el RAT (no público) información sobre los encargados de tratamiento asociados a cada uno de los tratamientos de datos personales. Se deberá revisar e incluir si es necesario los encargados del tratamiento, y deberán suministrar la información necesaria para poder elaborar el inventario de dichos encargados, incluyendo información sobre el inicio y fin del contrato o convenio, la persona o personas interlocutoras de la empresa tercera, el DPD de la empresa tercera si es el caso, y los tratamientos de datos personales asociados a cada encargo del tratamiento. Se deberá indicar en el citado inventario si se han incluido las cláusulas de encargo de tratamiento en cada caso.
- - Se deben analizar los riesgos específicos de cada tratamiento de datos personales a través de la herramienta de gestión RGPD de la Diputación, y se deben acometer las evaluaciones de impacto en protección de datos, si fueran necesarias..
- - Se debe elaborar un manual jurídico que sirva de hilo conductor para todos los aspectos a cumplir respecto al RGPD y LOPDgdd, y que contenga los procedimientos necesarios.
- - Se debe elaborar un procedimiento para el proceso de ejercicio de derechos por parte de los interesados.

### 01.01.- Activos y amenazas.

El riesgo se deriva, fundamentalmente, a partir del valor de los activos relevantes para el Negocio, de las amenazas a la que están expuestos dichos activos y de las medidas de seguridad que haya desplegadas, considerando no sólo que estén desplegadas como tal, sino su grado de madurez.

Respecto de los activos relevantes, se han identificado las Actividades de Tratamiento de Datos personales que se han inventariado en el Registro de Actividades de Tratamiento de datos personales (RAT) de la Entidad, se han identificado los tipos de datos personales de cada Actividad de Tratamiento, y se ha llevado a cabo la valoración cualitativa de los mismos.

Respecto de las amenazas para Cumplimiento Normativo sobre las Actividades de Tratamientos (Activos esenciales) (ver RAT), se ha partido de un catálogo general de amenazas que aporta el Anexo V de la "Guía práctica para la Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD" publicada por la AEPD (ver al guía), y para la Confidencialidad, Disponibilidad e Integridad de los datos personales se utilizara la metodología de análisis de riesgos seguida, Magerit v3 que se



utilizara en la Adecuacion al Esquema Nacional de Seguridad de la Entidad.

Respecto de la madurez de las medidas de seguridad actualmente desplegadas para RGPD, que son las que contrarrestan el efecto de las amenazas y permiten contener el riesgo, se han llevado a cabo entrevistas con los responsables pertinentes, que han permitido determinar la situación actual de dichas medidas de seguridad.

## 01.02.- Estimación del estado del riesgo.

La Estimación del estado de riesgo teniendo en cuenta la medidas de seguridad que actualmente se están aplicando es la siguiente:

- RIESGO POTENCIAL: 3 (MEDIO)
- RIESGO ACTUAL: 2,7 (MEDIO)

Aplicando en una escala de 0 a 16 los siguientes criterios: 0-2 (BAJO), 2-6 (MEDIO), 6-12 (ALTA), 12-16 (MUY ALTO), se considera el riesgo potencial inherente como 3 (MEDIO) y el riesgo actual de 2,7 (MEDIO).

Se determina que el riesgo planificado o residual será de 0,6 (BAJO), y como maximo aceptable por la Entidad el riesgo planificado sera el inferior a 2 (BAJO)..

## 01.03.- Plan del tratamiento del riesgos (Plan de Mejora de la Seguridad).

El plan de tratamiento de riesgos, llamado Plan de Acción o Plan de Mejora de la Seguridad en el contexto de las medidas de seguridad, consiste en las acciones de mejora identificadas. Se elaborara dicho plan con Proyectos Estratégicos (Elaboración de Documentación, Procesos Organizativos y Operativos, Actuaciones Técnicas, y Medidas Jurídicas RGPD), un conjunto de ámbitos de actuación y una colección de acciones, cuyo detalle se puede ver en el documento del plan (ver documento plan de Mejora de la Seguridad).

## 02 - Definiciones.

- - Activo: Elemento material o inmaterial que tiene un valor para el negocio de la organización, o la parte de ella sujeta a un análisis de riesgos.
- - Activo esencial: activo sobre el que recae el fin último del negocio de la parte de la organización sujeta a un análisis de riesgos. Suele tratarse del servicio final ofrecido a los usuarios, o información que constituye la esencia de lo que la parte de la organización ofrece a sus usuarios.
- - Amenaza: evento que puede desencadenar un detrimento en la seguridad de la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- - Valor de un activo: es una estimación del impacto que tendría en la organización la materialización de una amenaza sobre el activo. Un activo de valor ALTO supone que, si una amenaza se materializara sobre el activo, habría un impacto alto en la organización.
- - Valor acumulado: Los activos dependen de otros activos para poder realizar su función. El valor acumulado de un activo es el mayor entre el suyo propio y el de los activos que dependen de él.
- - Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.



- - Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo. Equivale a una medida de seguridad.
- - Control de seguridad, o simplemente, control: Medida de seguridad.
- - Riesgo potencial o inherente: El riesgo que habría si no existiera ninguna salvaguarda desplegada.
- - Riesgo actual o presente: El riesgo existente teniendo en cuenta las salvaguardas desplegadas en el momento de realizar el análisis de riesgos
- - Riesgo planificado: El riesgo que se alcanzará una vez que se lleve a cabo el Plan de Tratamiento de Riesgos que se ha elaborado para disminuir el riesgo actual. Este riesgo planificado también se conoce como riesgo residual.
- - Riesgo acumulado (o propio): se calcula teniendo en consideración el valor propio o acumulado de cada activo (el mayor de ellos) y el efecto directo de las amenazas sobre dicho activo. Puesto que hay dependencias entre activos, los activos inferiores acumulan el valor de los activos superiores (obtienen el mayor de entre su valor propio y el heredado de los activos dependientes).
- - Riesgo repercutido: es el calculado sobre los activos esenciales, tomando en consideración el riesgo que provocan las amenazas sobre los activos inferiores de los que depende un activo esencial, y considerando el valor propio del activo. Puesto que hay dependencias entre activos, las amenazas sobre los activos inferiores tienen una consecuencia negativa en los activos superiores: si un activo inferior resulta dañado provocará que el activo superior se vea afectado de alguna forma, que es función del tipo de dependencia.

## 03- Alcance del Análisis y Metodología Empleada.

Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, en adelante, RGPD. obliga al cumplimiento de los requerimientos y obligaciones para el responsable y el encargado de tratamiento que este incluye, entre las que destaca, la necesidad de llevar a cabo un análisis de riesgos con el fin de establecer medidas de seguridad y control para garantizar los derechos y libertades de las personas.

A continuación, se incluye una breve descripción del ámbito considerado para la realización del análisis junto con la metodología empleada en su desarrollo.

### 03.01 - Alcance:

El análisis realizado se circunscribe a las actividades de tratamiento de datos personales de AYUNTAMIENTO DE LAUJAR DE ANDARAX, en lo referente a las amenazas del incumplimiento normativo, y se aplicara lo dispuesto en el Esquema Nacional de Seguridad en lo referente a la Integridad, Disponibilidad y Confidencialidad de los datos personales.

### 03.02 - Metodología:

Para el desarrollo del Análisis de Riesgos se ha seguido la siguiente Metodología de Análisis y Gestión de Riesgos, para Cumplimiento Normativo sobre las Actividades de Tratamientos (Activos esenciales) (ver RAT), se ha seguido la "Guía práctica para la Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD" publicada por la AEPD (ver al guía) utilizando las opciones que proporciona el sistema de gestión proDatos de la Diputación, y para la Confidencialidad,



Disponibilidad e Integridad de los datos personales se utilizara la metodología de análisis de riesgos, Magerit v3 que se utilizara en la Adecuacion al Esquema Nacional de Seguridad de la Entidad, en la herramienta PILAR.

Respecto de las amenazas para Cumplimiento Normativo sobre las Actividades de Tratamientos (Activos esenciales) (ver RAT), se ha partido de un catálogo general de amenazas que aporta el Anexo V de la "Guía práctica para la Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD" (ver al guía) y la "Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD" ambas publicadas por la AEPD (ver guía), y para la Confidencialidad, Disponibilidad e Integridad de los datos personales se utilizara la metodología de análisis de riesgos seguida, Magerit v3 que se utilizara en la Adecuacion al Esquema Nacional de Seguridad de la Entidad.

Este documento ofrece una visión global del proceso seguido, desde la identificación de activos y amenazas hasta la evaluación de las salvaguardas y la estimación de los riesgos residuales existentes.

A continuación, se describen las principales fases de la metodología empleada:

- 1.- La primera fase a realizar, es decidir el tipo de gestión para determinar la Categorización de las Medidas de Seguridad o Salvaguardas, si se va a realizar por Dependencias (que sera el caso de Entidades de tamaño grande como la Diputación), o por Entidad (que sera el caso de Entidades de tamaño pequeño como las EELL de la Provincia).
- 2.- Identificación y caracterización de los activos: Identificación y valoración de los activos que forman parte del Análisis de Riesgos.
  - Para la Identificación se ha confeccionado el Registro de (Actividades de tratamiento de datos Personales (- ver RAT- ).
  - La valoración se realiza para la Dimension del cumplimiento normativo de la Protección de Datos Personales, dejando las dimensiones de seguridad Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, para su valoración según las directrices del Anexo I del ENS.
- 3.- Para nuevas Actividades de Tratamiento se debe realizar una fase de Analisis de la necesidad de realizar una Evaluacion de Impacto sobre la protección de datos personales: Una EIPD no se requiere siempre, en cada actividad de tratamiento, se debe valorar la necesidad de llevar a cabo la misma. Es fundamental realizar un análisis previo para determinar de forma preliminar el nivel de riesgo al que puede estar expuesto el tratamiento y tomar la decisión adecuada en base a ello.
- 4.- Fase de Analisis y Gestion de Riesgos, en la que distinguiremos las etapas de Identificación de las Amenazas, Evaluacion de Riesgo y Tratar los Riesgos :
  - a). Identificación de las amenazas: Identificación de las amenazas que afectan a las Actividades de Tratamiento de Datos Personales como activos esenciales.
  - b).Evaluacion de los riesgos: Determinar la vulnerabilidad ante esas amenazas en términos de probabilidad y degradación. De este modo es posible estimar el impacto y riesgo potencial o intrínseco sobre cada uno de los activos.
  - c). Tratamiento del Riesgo: Determinar los controles de seguridad a implantar y la estimación del nivel de madurez, empleando como referencia el marco de controles definido en el Anexo II del ENS, y el RGPD.
- 5. Estimación del estado del riesgo. Analiza los resultados obtenidos con el objetivo de disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

### 03.03 - Analisis de la necesidad de realizar una Evaluacion de Impacto en la Protección de Datos Personales:

La Evaluación de Impacto en la Protección de Datos Personales (en adelante, la EIPD) es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a



cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

El RGPD prevé que las Evaluaciones de Impacto se lleven a cabo “antes del tratamiento” en los casos en que sea probable que exista un alto riesgo para los derechos y libertades de los afectados. Ello implica que el mandato del Reglamento no se extiende a las operaciones de tratamiento que ya estén en curso en el momento en que comience a ser de aplicación.

Una EIPD no se requiere siempre, en cada actividad de tratamiento, se debe valorar la necesidad de llevar a cabo la misma. Es fundamental realizar un análisis previo para determinar de forma preliminar el nivel de riesgo al que puede estar expuesto el tratamiento y tomar la decisión adecuada en base a ello.

Del resultado del análisis sobre la necesidad de realizar una EIPD se puede concluir que:

- Sí es necesario realizar una EIPD: Se realizará y documentará una EIPD con todas sus fases (Ver Guía de Evaluación de Impacto en la Protección de Datos).
- No es necesario realizar una EIPD: Se entiende que las actividades de tratamiento no están expuestas a riesgos relevantes que motiven la necesidad de realizar una EIPD en profundidad. Si como resultado del análisis previo se considera que no es necesario llevar a cabo una EIPD, se debe documentar adecuadamente los motivos por los cuales se ha llegado a esa conclusión. En cualquier caso, se debe mantener evidencia de que se ha llevado a cabo este análisis (responsabilidad proactiva).

### 03.04 - Criterios para categorizar los Activos (Actividades de tratamiento de datos personales):

El valor o categoría de los activos se ha obtenido aplicando a cada Actividad de Tratamiento de Datos Personales (ver RAT), como activos esenciales, los siguientes criterios:

- - Categoría: BAJA: Numero de Interesados bajp (< 10000) y no se tratan categorías especiales de datos personales.
- - Categoría: MEDIA. Numero de interesados medio (> 10000 y < 1000000) o se tratan categorías especiales de datos personales.
- - Categoría ALTA: Numero de interesados alto y se tratan categoría especieles de datos personales.

Tras obtener el valor o categoría de los activos, Actividades de Tratamiento de datos Personales, se establece la madurez planificada que deben alcanzar la medidas de seguridad que se van aplicar, para ello se establecen los siguientes criterios:

- - Categoría: BAJA: Nivel de Madurez L2 (un cumplimiento de las medidas de seguridad del 50%)
- - Categoría: MEDIA: Nivel de Madurez L3 (un cumplimiento de las medidas de seguridad del 80%)
- - Categoría ALTA: Nivel de Madurez L4 (un cumplimiento de las medidas de seguridad del 90%)

### 03.05 - Criterios para la evaluacion de los riesgos:

La evaluación de riesgos consiste en valorar y estimar la probabilidad y el impacto de que el riesgo se materialice. Como punto de partida, es necesario haber definido el criterio que se seguirá a la hora de valorar los riesgos. Los criterios para cuantificar los riesgos, estimar el nivel de impacto y su probabilidad, se pueden basar en estándares o se pueden definir a criterio de la organización.



Escala de posibles valores para el cálculo de la probabilidad, sera de 1 a 4 con los siguientes criterios::

- (1) Probabilidad despreciable: La posibilidad de ocurrencia es muy baja (por ejemplo, un evento que puede pasar de forma fortuita).
- (2) Probabilidad limitada: La posibilidad de ocurrencia es baja (por ejemplo, un evento que puede pasar de forma ocasional).
- (3) Probabilidad significativa: La posibilidad de ocurrencia es alta (por ejemplo, un evento que puede pasar con bastante frecuencia).
- (4) Probabilidad máxima: La posibilidad de ocurrencia es muy elevada (por ejemplo, un evento cuya ocurrencia se produce con mucha frecuencia).

El impacto se determina en base a los posibles daños que se pueden producir si la amenaza se materializa. De igual modo, el impacto también se evaluará con la misma escala de cuatro valores posibles:

- (1) Impacto despreciable: El impacto es muy bajo (por ejemplo, un evento cuyas consecuencias son prácticamente despreciables sin impacto sobre el interesado).
- (2) Impacto limitado: El impacto es bajo (por ejemplo, un evento cuyas consecuencias implican un daño menor sin impacto relevante sobre el interesado).
- (3) Impacto significativo: El impacto es alto (por ejemplo, un evento cuyas consecuencias implican un daño elevado con impacto sobre el interesado).
- (4) Impacto máximo: El impacto es muy alto (por ejemplo, un evento cuyas consecuencias implican un daño muy elevado un impacto crítico sobre el interesado).

El valor del riesgo es Probabilidad x Impacto, estableciendo los siguientes criterios de los resultados de dicho producto:

- Bajo: Si el valor resultante se sitúa entre los valores 1 y 2.
- Medio: Si el valor resultante es mayor que 2 y menor o igual que 6.
- Alto: Si el valor resultante es mayor que 6 y menor o igual que 9.
- Muy Alto: Si el valor resultante es mayor que 9.

### 03.06 - Criterios para establecer la Madurez de las Medidas de Seguridad:

Una vez determinada la aplicabilidad de medidas de seguridad, se han realizado entrevistas a los Responsables de la Entidad, obteniéndose a partir de ellas el grado de madurez de cada medida de seguridad y, a partir de ese dato, el riesgo existente, que es una cuantificación de en qué medida la madurez de las salvaguardas existentes permite afrontar las amenazas identificadas. Indicado a cada medida de seguridad la madurez actual, siguiendo los siguientes valores y criterios:

- - Nivel L0 (0%) - Inexistente. Esta medida no está siendo aplicada en este momento.
- - Nivel L1 (10%) - Inicial / ad hoc. Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas. Pese a una naturaleza caótica, es más que no tener nada; pero es difícil prever la reacción ante una situación de emergencia.
  - - Nivel L2 (50%) - Repetible, pero intuitivo. Cuando existe un mínimo de planificación que, acompañada de la buena voluntad de las personas proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas.
  - - Nivel L3 (80%) - Proceso definido. Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.
  - - Nivel L4 (90%) - Gestionado y medible. Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de



establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.

- - Nivel L5 (100%)- Optimizado. En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

### 03.07 - Elaborar Plan de Medidas de Seguridad:

Para disminuir el riesgo a un valor aceptable, se ha elaborado un Plan de Mejora de la Seguridad, que básicamente ha consistido en identificar las acciones necesarias para elevar el grado de madurez de cada medida de seguridad al valor planificado de madurez (ver documentos plan de Mejora de la Seguridad).

## 04- Definir como gestionar las Medidas de Seguridad.

El continuo avance de la tecnología y la evolución de los tratamientos propician la aparición continua de nuevos riesgos que deben ser gestionados. En este contexto, el RGPD exige que los responsables del tratamiento implementen medidas de control adecuadas para demostrar que se garantizan los derechos y libertades de las personas y la seguridad de los datos, teniendo en cuenta entre otros, los "riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas" (artículo 24.1) y aplicando las medidas oportunas.

AYUNTAMIENTO DE LAUJAR DE ANDARAX como reponsable del Tratamiento de Datos Personales implementara la Medidas de Control necesarias, y para ello realizara una gestion de dichas medidas por Entidad, donde el responsable de gestion de los Datos Personales de la Entidad determinara el nivel de madurez de las Medidas que se adopten, y los maximos reponsables de la Entidad velaran por su cumplimiento..

## 05- Categorización de Activos. Categoría ENS de las Actividades de Tratamiento.

Cada Actividad de Tratamiento de Datos Personales, como activo esencial se ha valorado en base a los criterios de valoración que se establecen en el Anexo I del ENS. Esta valoración se ha realizado solo para la dimensión de Datos Personales (DP). Siendo los criterios para la Categoría y en funcion de las características de los datos personales tratados, los siguientes:

- - Categoría: BAJA: Numero de Interesados bajo (< 10000) y no se tratan categorías especiales de datos personales.
- - Categoría: MEDIA. Numero de interesados medio (> 10000 y < 1000000) o se tratan categorías especiales de datos personales.
- - Categoría ALTA: Numero de interesados alto y se tratan categoría especieles de datos personales.

La relación de las Actividades de Tratamiento de Datos Personales como activos esenciales, junto con la valoración dada a cada uno de ellas se recoge en la siguiente lista:

- ATENCIÓN DERECHOS DE TRANSPARENCIA Y PROTECCIÓN DE DATOS (BAJA)
- ACTIVIDADES CULTURALES (BAJA)
- ACTIVIDADES DEPORTIVAS (BAJA)
- ANIMALES PELIGROSOS (BAJA)
- ARCHIVO GENERAL DEL AYUNTAMIENTO (BAJA)
- ATENCIÓN AL CONSUMIDOR (BAJA)



- CEMENTERIO MUNICIPAL (BAJA)
- CONTRATACIÓN DE OBRAS BIENES Y SERVICIOS (BAJA)
- DIRECTORIO DE SERVICIOS Y ACTIVIDADES DE EMPRESAS O PROFESIONALES (BAJA)
- GESTIÓN ACTIVIDADES DE JUVENTUD Y CENTRO DE INFORMACIÓN JUVENIL (BAJA)
- GESTION AVISOS DE INCIDENCIAS EN EL MUNICIPIO (BAJA)
- GESTIÓN CENTROS GUADALINFO (BAJA)
- GESTIÓN DE DISCIPLINA URBANÍSTICA (BAJA)
- GESTION DE LICENCIAS DE ACTIVIDADES (BAJA)
- GESTIÓN DE NOMINAS Y PERSONAL (BAJA)
- GESTIÓN DE RESERVAS DE RECURSOS POR WEB (BAJA)
- GESTIÓN DE SERVICIOS SOCIALES (BAJA)
- GESTIÓN DE SUMINISTRO DE AGUA DOMICILIARIA (BAJA)
- GESTIÓN DEL PLANEAMIENTO (BAJA)
- GESTIÓN ECONÓMICO Y CONTABLE (BAJA)
- GESTIÓN RADIO MUNICIPAL (BAJA)
- GESTION TRIBUTARIA Y RECAUDACION (BAJA)
- GESTIÓN Y CONTROL DE LA BIBLIOTECA MUNICIPAL (BAJA)
- GRABACIÓN Y RETRANSMISIÓN DE SESIONES DE ÓRGANOS COLEGIADOS (BAJA)
- INSCRIPCIONES EN ACTIVIDADES Y EVENTOS POR LA WEB DIPUTACIÓN (BAJA)
- MIEMBROS DE LA CORPORACIÓN (BAJA)
- PADRON MUNICIPAL DE HABITANTES (BAJA)
- POLICÍA LOCAL (BAJA)
- PREVENCIÓN Y SALUD LABORAL (BAJA)
- PROTECCIÓN CIVIL (BAJA)
- REGISTRO DE ENTRADA Y SALIDA DOCUMENTOS Y GESTIÓN DE EXPEDIENTES (BAJA)
- REGISTRO DE UNIONES DE HECHO (BAJA)
- REGISTRO MUNICIPAL DE ENTIDADES CIUDADANAS (BAJA)
- SELECCIÓN DE PERSONAL (BOLSAS DE TRABAJO) (BAJA)
- SOLICITUD DE INFORMACIÓN Y CONSULTAS (BAJA)
- SUBVENCIONES (BAJA)
- SUGERENCIAS Y RECLAMACIONES (BAJA)
- TERCEROS (BAJA)

Puesto que existen Actividades de Tratamiento de Datos Personales que han obtenido una valoración de valor **BAJA**, la Categoría Global para las Actividades de tratamiento de datos personales es de:

**Categoría global = BAJA**

La categoría de la Integridad, Disponibilidad y Confidencialidad se realizara conforme a lo dispuesto en el ENS, y se realizara en el Plan de Adecuación al ENS de la Entidad, donde tambien se realizara el Análisis de Riesgos correspondiente.

## 06- Análisis de la Necesidad de realizar una EIPD.

Para la valoración si es necesario o no la realización de una EIPD se han realizado para AYUNTAMIENTO DE LAUJAR DE ANDARAX, una Análisis de la Necesidad de Realizar una EIPD en las siguientes Actividades de Tratamiento de Datos Personales, que se han seleccionado por su relevancia y como muestra:

- ATENCIÓN DERECHOS DE TRANSPARENCIA Y PROTECCIÓN DE DATOS (BAJA) (No se ha realizado el Análisis de Necesidad de EIPD)
- ACTIVIDADES CULTURALES (BAJA) (No se ha realizado el Análisis de Necesidad de EIPD)
- ACTIVIDADES DEPORTIVAS (BAJA) (No se ha realizado el Análisis de Necesidad de EIPD)
- ANIMALES PELIGROSOS (BAJA) (No se ha realizado el Análisis de Necesidad de EIPD)
- ARCHIVO GENERAL DEL AYUNTAMIENTO (BAJA) (No se ha realizado el Análisis de Necesidad de EIPD)
- ATENCIÓN AL CONSUMIDOR (BAJA) (No se ha realizado el Análisis de Necesidad de EIPD)



- CEMENTERIO MUNICIPAL (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- CONTRATACIÓN DE OBRAS BIENES Y SERVICIOS (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- DIRECTORIO DE SERVICIOS Y ACTIVIDADES DE EMPRESAS O PROFESIONALES (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN ACTIVIDADES DE JUVENTUD Y CENTRO DE INFORMACIÓN JUVENIL (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTION AVISOS DE INCIDENCIAS EN EL MUNICIPIO (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN CENTROS GUADALINFO (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN DE DISCIPLINA URBANÍSTICA (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTION DE LICENCIAS DE ACTIVIDADES (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN DE NOMINAS Y PERSONAL (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN DE RESERVAS DE RECURSOS POR WEB (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN DE SERVICIOS SOCIALES (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN DE SUMINISTRO DE AGUA DOMICILIARIA (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN DEL PLANEAMIENTO (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN ECONÓMICO Y CONTABLE (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN RADIO MUNICIPAL (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTION TRIBUTARIA Y RECAUDACION (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GESTIÓN Y CONTROL DE LA BIBLIOTECA MUNICIPAL (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- GRABACIÓN Y RETRANSMISIÓN DE SESIONES DE ÓRGANOS COLEGIADOS (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- INSCRIPCIONES EN ACTIVIDADES Y EVENTOS POR LA WEB DIPUTACIÓN (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- MIEMBROS DE LA CORPORACIÓN (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- PADRON MUNICIPAL DE HABITANTES (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- POLICÍA LOCAL (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- PREVENCIÓN Y SALUD LABORAL (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- PROTECCIÓN CIVIL (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- REGISTRO DE ENTRADA Y SALIDA DOCUMENTOS Y GESTIÓN DE EXPEDIENTES (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- REGISTRO DE UNIONES DE HECHO (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- REGISTRO MUNICIPAL DE ENTIDADES CIUDADANAS (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- SELECCIÓN DE PERSONAL (BOLSAS DE TRABAJO) (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- SOLICITUD DE INFORMACIÓN Y CONSULTAS (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- SUBVENCIONES (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- SUGERENCIAS Y RECLAMACIONES (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)
- TERCEROS (BAJA) (No se ha realizado el Analisis de Necesidad de EIPD)

-Numero de Actividades de Tratamiento de Datos Personales con Análisis de Necesidad de realizar una EIPD = 0 de un total de 38

## 07- Identificación y Categorización de Amenazas - Riesgo Potencial.

El catálogo de amenazas, para el cumplimiento normativo, que se ha utilizado para realizar la gestión de riesgos para AYUNTAMIENTO DE LAUJAR DE ANDARAX ha sido el catálogo de la herramienta de gestión de datos personales de Diputación proDatos "AYTO - Catálogo de Amenazas para aplicar a los Ayuntamientos más reducido que el de la AEPD".

Para el cumplimiento de la Integridad, Disponibilidad y Confidencialidad de los datos personales se valora el riesgo sobre la adecuación de la Entidad al ENS, dejando la gestión de riesgos de las amenazas por estas dimensiones de la seguridad al proyecto de Adecuación al ENS que se realice y que utilice el catálogo estándar contemplado en la metodología MAGERIT y que se implementa en la herramienta Pilar del CCN-CERT.

Para cada amenaza para el cumplimiento normativo, se ha establecido su probabilidad de ocurrencia y el impacto que tendría para la dimensión de la protección de datos personales para cada uno de los activos.

El catálogo de amenazas que se aplicará será el siguiente, con unos valores por defecto de (probabilidad x impacto):

### - AYTO-01-Generales

- AYTO-Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales y derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas (1 x 1=1)



- AYT0-Incorporación tardía del delegado de protección de datos o DPO, al proyecto o definición deficiente de sus funciones y competencias. (2 x 1=2)
- AYT0-Poco conocimiento y concienciación del personal de la Entidad en la Protección de Datos Personales (3 x 1=3)
- **AYTO-02-Ligitimacion y cesion**
- AYT0-Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales (2 x 1=2)
- AYT0-Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias (2 x 1=2)
- AYT0-Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada (3 x 1=3)
- **AYTO-03-Transferencias Internacionales**
- AYT0-Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia (0 x 0=0)
- **AYTO-04-Notificación y Registro de las Actividades**
- AYT0-Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe registrarse la creación, modificación o cancelación de actividades de tratamiento. (2 x 1=2)
- **AYTO-05-Transparencia de los tratamientos**
- AYT0-Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.). (3 x 1=3)
- AYT0-Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales. (2 x 1=2)
- **AYTO-06-Calidad de los datos**
- AYT0-Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas (2 x 1=2)
- AYT0-Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas: ( Datos transaccionales, de navegación o de geolocalización), (Toma de decisiones económicas, sociales, laborales, etc., relevantes sobre las personas ), (Toma de decisiones automatizadas), ( Utilización de los metadatos para finalidades no declaradas) (2 x 1=2)
- AYT0-Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron (2 x 1=2)
- **AYTO-08-Deber de secreto**
- AYT0-Accesos no autorizados a datos personales. (3 x 1=3)
- AYT0-Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización (2 x 1=2)
- **AYTO-09-Tratamientos por Encargo**
- AYT0-Falta de diligencia (o dificultad para demostrarla) en la elección de encargado de tratamiento (3 x 1=3)
- AYT0-Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato (3 x 1=3)
- **AYTO-10-Derechos de los Interesados**
- AYT0-Dificultar o imposibilitar el ejercicio de los derechos de los interesados. (2 x 1=2)
- AYT0-Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales. (2 x 1=2)
- **AYTO-15-Seguridad - Medidas para tratamiento y gestión en Papel**
- AYT0-Recogida de datos personales en formularios en Papel sin adoptar las medidas adecuadas (2 x 1=2)
- AYT0-Archivo y almacenamiento de datos personales en Papel sin adoptar las medidas adecuadas (2 x 1=2)
- AYT0-Destrucción de papel con datos personales sin adoptar las medidas adecuadas (2 x 1=2)
- **AYTO-01-Generales**
- AYT0-Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados. (2 x 1=2)
- **AYTO-02-Ligitimacion y cesion**
- AYT0-Tratar datos personales cuando no es necesario para la finalidad perseguida (1 x 1=1)
- AYT0-Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión. (2 x 1=2)
- AYT0-Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la re-identificación de información disociada. (2 x 1=2)
- **AYTO-06-Calidad de los datos**
- AYT0-Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos (2 x 1=2)
- **AYTO-07-Categorías Especiales de Datos**
- AYT0-Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando éste sea la causa que legitima su tratamiento o cesión (3 x 1=3)
- **AYTO-09-Tratamientos por Encargo**
- AYT0-Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas. (3 x 1=3)
- AYT0-No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos de los interesados realizados ante los encargados de tratamiento (3 x 1=3)
- **AYTO-10-Derechos de los Interesados**
- AYT0-Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados. (2 x 1=2)
- **AYTO-12-Seguridad. Medidas del ENS**
- AYT0-Problemas de Confidencialidad, Integridad y Disponibilidad de Datos Personales que se tratan ya que existen carencias en la adecuación e implantación de medidas según el ENS: (3 x 1=3)



- AYTO-15-Seguridad - Medidas para tratamiento y gestión en Papel
- AYTO-Transporte de datos personales en Papel sin adoptar las medidas adecuadas (2 x 1=2)
- AYTO-02-Ligitimacion y cesion
- AYTO-Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros (2 x 1=2)
- AYTO-03-Transferencias Internacionales
- AYTO-Acceso secreto a los datos personales por parte de autoridades de terceros países (0 x 0=0)
- AYTO-05-Transparencia de los tratamientos
- AYTO-En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que hagan muy difícil su acceso conjunto y detallado (2 x 1=2)
- AYTO-06-Calidad de los datos
- AYTO-Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio (2 x 1=2)
- AYTO-09-Tratamientos por Encargo
- AYTO-Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad. (3 x 1=3)
- AYTO-11-Registro y notificación de incidentes y violaciones de seguridad
- AYTO-Carecer de los mecanismos y procedimientos necesarios para registrar incidentes y violaciones de seguridad y en su caso notificar a Organo de Control correspondiente (2 x 1=2)

Los valores de (probabilidad x impacto) que el catalogo propone por defecto, deben ser modificados por valores que se obtendran de las entrivistas que se realicen con los responsables de los tratamiento de los datos personales.

## 08- Evaluación del Riesgo - Riesgo Potencial.

La evaluación de riesgos consiste en valorar y estimar la probabilidad y el impacto de que el amenaza se materialice. Como punto de partida, es necesario haber definido el criterio que se seguirá a la hora de valorar los riesgos. Los criterios para cuantificar los riesgos, estimar el nivel de impacto y su probabilidad, los criterios a seguir para la evaluacion de los riesgos seran los descritos en los apartados anteriores.

La Evaluacion de los riesgos se realizara para una muestra significativa de las Actividades de Tratamiento de Datos Personales de la Entidad, y para el caso de AYUNTAMIENTO DE LAUJAR DE ANDARAX las actividades de tratamiento de la muestran son:

- PADRON MUNICIPAL DE HABITANTES (Riesgo Potencial=3)

Los datos para la Entidad son los siguientes:

- - Actividades de Tratamiento de Datos Personales valorados: 1
- - Numero de Amenazas valoradas: 37
- - Riesgo Potencial: 3

Puede ver mas informacion sobre el Analisis de riesgos de AYUNTAMIENTO DE LAUJAR DE ANDARAX en el siguiente enlace (Ver informacion Analisis de Riesgos):

## 09- Tratamiento del Riesgo - Nivel de Madurez de las Medidas de Seguridad.



Para poder valorar el grado de madurez de cada una de las medidas que hay que aplicar, se valora por los responsables de los tratamientos para cada Actividad de Tratamiento el valor estimado de madurez de las Medidas de Seguridad, siendo estos valores para las Actividades de Tratamiento de datos personales seleccionadas para realizar el Analisis de Riesgos los siguientes:

### - PADRON MUNICIPAL DE HABITANTES (L1)

En la lista siguiente se muestran las valoraciones de madurez (en qué medida los controles de seguridad se encuentran documentados, difundidos, conocidos, aplicados y gestionados) para las medidas de seguridad que se han obtenido en base a los datos recabados del personal responsable. La madurez se indica (Lx/Ly) donde Lx es el nivel de madurez actual y Ly es el valor de madurez planificado.

El color de los valores de la madurez de las medidas sigue el criterio de colores establecido en la guía CCN-STIC-815 Métricas e Indicadores en el ENS, e indica lo más o menos aceptable que resulta el grado de madurez actual, y que está relacionado con la Categoría ENS de la Actividad de Tratamiento, ya que, en función de eso, un mismo valor de madurez puede estar más o menos cerca del mínimo aceptable, en base a los mínimos establecidos en la guía CCN-STIC 804. Esquema Nacional de Seguridad. Guía de Implantación. Los valores son;

- - Color verde indica que la madurez de la medida de seguridad correspondiente se encuentra en un valor aceptable y no es necesaria, en una primera instancia, ninguna acción.
- - Color amarillo indican que algún requisito de la medida de seguridad se encuentra por debajo de lo recomendable y es preciso realizar alguna acción correctiva.
- - Color rojo indican que los requisitos de la medida se cumplen de forma claramente insuficiente y su remediación debe ser motivo de estudio inmediato.

### - AMENAZAS - CUMPLIMIENTO NORMATIVO

#### - AYT0-01-Generales

- DIP\_AYT-Formación apropiada del personal sobre protección de datos , seguridad y uso adecuado de las TIC. (L1/L2)
- DIP\_AYT-Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización así como de las sanciones aparejadas al incumplimiento de las mismas. (L1/L2)
- DIP\_AYT-Nombrar a una persona o departamento como responsable de la interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella. (L1/L2)
- DIP\_AYT-Nombrar un Delegado de Protección de Datos o Data Protection Officer (que dependiendo del tamaño de la organización será una persona o un departamento interno o externo) para ocuparse de todas las cuestiones relativas a la privacidad dentro de la organización y contar con asesoramiento cualificado. Si se procede a este nombramiento, el Delegado de Protección de Datos puede hacerse cargo también de la interlocución con los afectados. (L1/L2)
- DIP\_AYT-Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del DPD en las fases iniciales de los mismos. (L1/L2)
- DIP\_AYT-Establecer desde la dirección las funciones, competencias y atribuciones del DPD en el desarrollo y gestión de los proyectos, y exigir cumplimiento de dichas funciones y competencias. (L1/L2)
- DIP\_AYT-Formación apropiada del personal sobre protección de datos , seguridad y uso adecuado de las TIC. (L1/L2)

#### - AYT0-02-Ligitimacion y cesion

- DIP\_AYT-Usar datos disociados o pseudónimos siempre que sea posible y no implique un esfuerzo desproporcionado (L1/L2)
- DIP\_AYT-Evitar el uso de datos biométricos salvo que resulte imprescindible o esté absolutamente justificada (L1/L2)
- DIP\_AYT-Asegurarse de que no existen otras causas de legitimación más adecuadas (L1/L2)
- DIP\_AYT-Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrecer siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato (L1/L2)
- DIP\_AYT-Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas (L1/L2)
- DIP\_AYT-Establecer procedimientos claros para manifestar la revocación del consentimiento o la solicitud de oposición a un determinado tratamiento. Si la organización realiza acciones publicitarias, tener en cuenta las reglas especiales existentes para las comunicaciones comerciales y, en particular, cuando estas se llevan a cabo a través de comunicaciones electrónicas. (L1/L2)
- DIP\_AYT-Exigir garantías de que los datos personales provenientes de terceros se han obtenido y cedido lealmente. (L1/L2)
- DIP\_AYT-Si se ceden datos personales, establecer por escrito acuerdos que contemplen las condiciones bajo las que se produce la cesión y, en su caso, las relativas a cesiones ulteriores así como las posibilidades de supervisión y control del cumplimiento del acuerdo. (L1/L2)
- DIP\_AYT-Verificar que el tratamiento de datos especialmente protegidos es absolutamente imprescindible para la finalidad o finalidades perseguidas y se realiza según la normativa de protección de datos (L1/L2)
- DIP\_AYT-Verificar la legitimidad de la interconexión de datos prevista y Definir claramente los datos personales resultantes del tratamiento y verificar tras el proceso que son los únicos que se han generado (L1/L2)
- DIP\_AYT-Evitar el uso de cookies u otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos



cortos de caducidad de las cookies, etc.). (L1/L2)

- DIP\_AYT- Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas. (L1/L2)

### - AYTO-04-Notificación y Registro de las Actividades

- DIP\_AYT- Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo. (L1/L2)

### - AYTO-05-Transparencia de los tratamientos

- DIP\_AYT- Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas. (L1/L2)

- DIP\_AYT- Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada y Estructurada, y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión. (L1/L2)

- DIP\_AYT- Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión. (L1/L2)

- DIP\_AYT- Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización. (L1/L2)

### - AYTO-06-Calidad de los datos

- DIP\_AYT- Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso. (L1/L2)

- DIP\_AYT- Establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización que estén autorizados a utilizarlo. (L1/L2)

- DIP\_AYT- Siempre que sea posible, utilizar datos anónimos, disociados o pseudónimos. Y garantizar que se apliquen las medidas de seguridad adecuadas. (L1/L2)

- DIP\_AYT- Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas. (L1/L2)

- DIP\_AYT- Suministra información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en particular, a través de una política de privacidad visible y accesible. (L1/L2)

- DIP\_AYT- Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer. (L1/L2)

- DIP\_AYT- Definir claramente los plazos de cancelación de todos los datos personales de los sistemas de información, y establecer los controles adecuados. (L1/L2)

### - AYTO-07-Categorías Especiales de Datos

- DIP\_AYT- Evitar el uso de datos especialmente protegidos salvo que resulte absolutamente necesario y si es necesario. Y establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él. (L1/L2)

### - AYTO-08-Deber de secreto

- DIP\_AYT- Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales. (L1/L2)

- DIP\_AYT- Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores que acceden a datos personales de la obligación de guardar secreto sobre aquellos datos personales que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento. (L1/L2)

- DIP\_AYT- Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales. (L1/L2)

- DIP\_AYT- Formación adecuada de los empleados sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información. (L1/L2)

- DIP\_AYT- Establecimiento de sanciones disuasorias para los empleados que violen la confidencialidad de los datos personales y comunicación clara y completa de las mismas. (L1/L2)

### - AYTO-09-Tratamientos por Encargo

- DIP\_AYT- Establecer procedimientos que garanticen que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos. (L1/L2)

- DIP\_AYT- Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad. Establecer contractualmente mecanismos de supervisión, verificación y auditoría de los tratamientos encargados a terceros estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación homologados y de acreditada solvencia. (L1/L2)

- DIP\_AYT- Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado de tratamiento. (L1/L2)

- DIP\_AYT- Definir acuerdos de nivel de servicio que garanticen el correcto cumplimiento de las instrucciones del responsable y la adopción de las medidas de seguridad adecuadas. (L1/L2)

- DIP\_AYT- Incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados. Y Definir los procedimientos operativos para que esta comunicación se lleve a cabo de forma ágil y eficiente. (L1/L2)

- DIP\_AYT- Incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio. Y Establecer medidas técnicas y organizativas que garanticen la portabilidad. (L1/L2)

### - AYTO-10-Derechos de los Interesados

- DIP\_AYT- Implantar sistemas transparentes que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos. (L1/L2)

- DIP\_AYT- Formar a todo personal para que conozca qué ha de hacer si recibe una petición de derecho de los interesados o ha de informar a los afectados sobre cómo ejercerla. (L1/L2)

- DIP\_AYT- Definir qué personas o departamentos se ocuparán de gestionar los derechos de los interesados y atenderlos



adecuadamente (L1/L2)

- DIP\_AYT-Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados (L1/L2)
- DIP\_AYT-Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate. (L1/L2)
- **AYTO-11-Registro y notificación de incidentes y violaciones de seguridad**
- DIP\_AYT- Establecer procedimiento y medidas necesarias para registro de incidencias y violaciones de seguridad y en su caso notificación a órgano de control correspondiente. (L1/L2)
- **AMENAZAS - USO SISTEMA DE INFORMACION**
- **AYTO-12-Seguridad. Medidas del ENS**
- DIP\_AYT-Implantar las Medidas de seguridad del Esquema Nacional de Seguridad (ENS) (L1/L2)
- **AMENAZAS - TRATAMIENTO DATOS EN PAPEL**
- **AYTO-15-Seguridad - Medidas para tratamiento y gestión en Papel**
- DIP\_AYT-Definir los procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.) (L1/L2)
- DIP\_AYT-Utilizar archivadores o salas de archivo con llaves o sistemas de cerrado, así como de registro del personal que accede a los documentos en papel. (L1/L2)
- DIP\_AYT-Política de mesas Limpias, y cajones en las mesas con llaves (L1/L2)
- DIP\_AYT-Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias. (L1/L2)
- DIP\_AYT-Definir los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales. (L1/L2)

## 9.1.- Insuficiencias de las Medidas de Seguridad.

La relación de controles de seguridad que no llegan a un nivel suficiente de madurez se obtienen de la información detallada de madurez mostrada en el apartado anterior, y eligiendo las medidas de seguridad donde el valor de la madurez es de color amarillo o rojo.

Estos controles de madurez insuficiente son los que sirven de base para el Plan de Seguridad ya que, para cada uno de ellos se plantean acciones para elevar su madurez al nivel requerido.

Puede ver mas informacion sobre los Niveles de madurez de las Medidas de Seguridad de AYUNTAMIENTO DE LAUJAR DE ANDARAX en el siguiente enlace (Ver informacion sobre Medidas de Seguridad):

## 10- Estimación del Estado del Riesgo.

Se puede definir el impacto como la medida del daño sobre los activos resultante de la materialización de las amenazas.

Por otro lado, el riesgo es la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El estado del riesgo del presente análisis se calcula realizando una estimación donde, además de los activos y las amenazas, se consideran las salvaguardas implantadas actualmente con su grado de madurez.

Para representar el nivel de riesgo al que se encuentran expuestos las Actividades de Tratamiento de Datos Personales se ha utilizado la escala cualitativa adoptada por la herramienta proDatos. Dicha escala consta de los siguiente niveles:

- Despreciable. Valor 0.
- BAJO. Valor Mayor que 0 y menor o igual a 2.
- MEDIO. Valor Mayor que 2 y menor o igual a 6.
- ALTO. Valor Mayor que 6 y menor o igual a 9
- MUY ALTO. Valor Mayor que 9.



El análisis realizado contempla el riesgo sobre los activos en la dimensión de Datos Personales.

El riesgo potencial máximo al que se enfrentarían las Actividades de Tratamiento de Datos Personales si no hubiese medidas de seguridad desplegadas, es de **3** que se considera **MEDIO**, lo que se traduce en que las amenazas a las que se enfrentan los activos podrían suponer un daño **MEDIO**, para la organización.

Con las medidas de seguridad existentes en la actualidad e implantadas a fecha actual ese riesgo potencial se reduce hasta convertirse en un riesgo actual máximo de **2,7** que se considera **MEDIO**.

Tras el proceso de tratamiento de los riesgos propuesto que se llevaría a cabo, y cuyos resultados se recogen en el documento Plan de Mejora de la Seguridad, se ha llegado a un riesgo residual (riesgo planificado) de **0,6**, que se considera **BAJO** y asumible, por debajo del riesgo máximo aceptable, que es 2.

A continuación, se exponen las principales conclusiones obtenidas tras la realización del proceso de análisis y gestión de riesgos:

- - Riesgo potencial máximo (si no se aplicaran salvaguardas): **3** (escala 0-16)
- - Riesgo presente máximo (con las salvaguardas aplicadas actualmente): **2,7** (escala 0-16)
- - Riesgo planificado máximo (si se lleva a cabo el Plan de Mejora de la Seguridad propuesto): **0,6** (escala 0-16)
- - Numero de Actividades de Tratamientos de Datos Personales Valorados: **1**
- - Numero de Amenazas valoradas: **37**
- - Numero de Medidas de Seguridad propuestas: **54**
- - Porcentaje de nivel de implantación de las Medidas de Seguridad: **10**

Ver más información sobre el Análisis de riesgos de AYUNTAMIENTO DE LAUJAR DE ANDARAX en el siguiente enlace (Ver información Análisis de Riesgos):

Ver más información sobre los Niveles de madurez de las Medidas de Seguridad de AYUNTAMIENTO DE LAUJAR DE ANDARAX en el siguiente enlace (Ver información sobre Medidas de Seguridad):

Ver la información sobre las Medidas de Seguridad del ENS (Ver medidas seguridad ENS)

## 11- Revisión del documento.

Este informe debe ser revisado ante cambios en la organización, en la tecnología, en la arquitectura de sistemas, en la incorporación o eliminación de Actividades de Tratamiento de Datos Personales, en las salvaguardas desplegadas, etc., es decir todos aquellos cambios que afecten al mapa de riesgos. Y, rutinariamente, se recomienda una revisión anual.

## 12- Aprobación del documento.

El Delegado de Protección de Datos, como cargo con atribuciones para proponer y validar riesgos y planes de tratamiento alrededor del cumplimiento del RGPD y LOPDyGDD, conoce, y propone para su aprobación el Análisis de Riesgos contenido en el presente documento.



13 - ANEXOS.

• ANEXO 01.- Medidas de Seguridad para Cumplimiento Normativo.

• ANEXO 02 .- Medidas de Seguridad para cumplimiento ENS. (descargar desde el siguiente enlace)

<https://app.dipalme.org/proDatos/descargarDocAlfresco?id=workspace://SpacesStore/a316d599-79c1-480d-9771-f5e70b9bd26f;1.0>

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

### AMENAZAS - CUMPLIMIENTO NORMATIVO

#### AYTO-01-Generales

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
199	<p>DIP_AYT-Formación apropiada del personal sobre protección de datos , seguridad y uso adecuado de las TIC.</p> <p>Descripcion Medida de seguridad</p> <p>Los Responsables de la Entidad, junto con los Responsables de las Dependencias, propondrán y diseñaran acciones formativas para el Personal a su cargo, velando por que todo el personal a su cargo se forme en las materias de Protección de datos y Seguridad de las TIC. Todo el Personal acceder a las acciones formativas que se propongan, para concienciarse y formarse en estas materias.</p> <p>Normativa a la que afecta</p> <p>Capitulo II RGPD - Principios. Capitulo III RGPD - Derechos del Interesado. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Diseñara acciones formativas para que todo el personal. DPD: - Supervisara y propondrá los contenidos de las acciones formativas. Dependencia Gestora de la PD: - Proponer y diseñar los contenidos de las Acciones formativas Responsable Funcional del Tratamiento: - Velaran por que todo el personal a su cargo reciba los cursos de formación que se propongan. Encargado Tratamiento: - Formara a los usuarios que participen en los encargos de tratamiento de datos personales. Usuarios: - Solicitaran y realizaran los cursos de formación que se propongan., - Solicitaran en su caso las necesidades de formación sobre protección de datos personales.</p>	L1/L2
200	<p>DIP_AYT-Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización así como de las sanciones aparejadas al incumplimiento de las mismas.</p> <p>Descripcion Medida de seguridad</p> <p>Los Responsables de la Entidad y de las distintas Dependencias, deberán velar por comunicar al personal a su cargo las Normas, Procedimientos, Medidas de Seguridad, y de mas documentación, para el correcto cumplimiento de la Normativa de Protección de Datos y así como las Medidas de Seguridad sobre el tratamiento de los Datos Personales, y las sanciones que se pudiesen derivar del incumplimiento.</p> <p>Normativa a la que afecta</p> <p>Capitulo II RGPD - Principios. Capitulo III RGPD - Derechos del Interesado. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Aprobar las Políticas, Normas, Procedimientos, Medidas de Seguridad y demás Documentos y comunicarlos a los Responsables y al personal afectado. DPD: - Proponer las Políticas, Normas, Procedimientos, Medidas, etc. y comprobar la difusión de las mismas a todo el Personal. Responsable Funcional del Tratamiento: - Comunicar al personal a su cargos las distintas Políticas, normativas, procedimientos, etc., que se aprueben y responsabilizarse de que se cumplan. Dependencia Gestora de la PD: - Realizara las actuaciones necesarias para que se comunique a todas las dependencias las Aprobación de Políticas, Normas, Procedimientos, etc. sobre protección de datos personales Encargado Tratamiento: - Comunicar al personal a su cargo que trate datos personales del Responsables de las Políticas, Normas, Procedimientos, Medidas, etc. que el Responsable apruebe, y velar por su cumplimiento Usuarios: - Cumplir con las Políticas, Normas, Procedimientos, Medidas, etc. que apruebe el Responsable. - Comunicar a sus Responsables cualquier duda o problema sobre cumplimiento de las Normas.</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
201	<p>DIP_AYT-Nombrar a una persona o departamento como responsable de la interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella.</p> <p><b>Descripción Medida de seguridad</b></p> <p>Se nombrara un Delegado de Protección de Datos que será el interlocutor ante los afectados y los órganos de control, y se publicara y difundirá en distintos medios como contactar con el. En el caso que el DPD sea un Órgano multipersonal, se deberá designar una persona o departamento como interlocutor y que se comunicara al DPD .</p> <p><b>Normativa a la que afecta</b></p> <p>En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Nombrar Delegado de Protección de Datos., y en caso de que el DPD sea un Órgano multipersonal, designara la Persona o Dependencia que actuara como interlocutor,</li> <li>- Comunicar el nombramiento a todos los interesados.</li> <li>- Establecer procedimientos para contactar con el DPD.</li> </ul> <p><b>DPD:</b></p> <ul style="list-style-type: none"> <li>- Asumir las funciones que le sean asignadas.</li> </ul> <p><b>Responsable Funcional del Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Comunicar al personal a su cargo el nombramiento del DPD.</li> <li>- Contactar con el DPD para Temas de Protección de Datos .</li> </ul> <p><b>Dependencia Gestora de la PD:</b></p> <ul style="list-style-type: none"> <li>-Realizar las tareas de difusión del nombramiento del DPD.</li> </ul> <p><b>Encargado Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Contactar con el DPD para cualquier tema sobre Protección de Datos.</li> </ul> <p><b>Usuarios:</b></p> <ul style="list-style-type: none"> <li>- Contactar con el DPD para cualquier tema sobre Protección de Datos, utilizando los procedimientos correspondientes.</li> <li>- Comunicar a su Responsable cualquier duda sobre el DPD.</li> </ul>	L1/L2
202	<p>DIP_AYT-Nombrar un Delegado de Protección de Datos o Data ProtectionOfficer (que dependiendo del tamaño de la organización será una persona o un departamento interno o externo) para ocuparse de todas las cuestiones relativas a la privacidad dentro de la organización y contar con asesoramiento cualificado. Si se procede a este nombramiento, el Delegado de Protección de Datos puede hacerse cargo también de la interlocución con los afectados.</p> <p><b>Descripción Medida de seguridad</b></p> <p>Se tiene que nombrar un Delegado de Protección de Datos, que puede ser de la Propia Entidad o externo. La Diputación de Almería ofrece los Servicios de DPD, por lo que puede solicitar dichos servicios si no dispone de medios internos para su nombramiento. Esta nombramiento no puede demorarse en caso que aun no se hay realizado el nombramiento, así como su inscripción en el Órgano de Control correspondiente que para las EE.LL. de Andalucía es el Consejo de Transparencia y Protección de Datos de Andalucía.</p> <p><b>Normativa a la que afecta</b></p> <p>En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Nombrar al Delegado de Protección de Datos, y en caso de ser un Órgano Multipersonal asignar a la Persona o Dependencia que hará de interlocutor.</li> </ul> <p><b>DPD:</b></p> <ul style="list-style-type: none"> <li>- Asumir las funciones que se le atribuyan.</li> </ul> <p><b>Dependencia Gestora de la PD:</b></p> <ul style="list-style-type: none"> <li>- Comunicar el nombramiento del DPD a toda la Organización.</li> </ul> <p><b>Responsable Funcional del Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Comunicar al personal a su cargo el nombramiento del DPD.</li> <li>- Contactar con el DPD para Temas de Protección de Datos .</li> </ul> <p><b>Usuarios:</b></p> <ul style="list-style-type: none"> <li>- Conocer los datos del DPD que se le comuniquen y los medios y procedimientos para realizar consultas sobre protección de datos personales.</li> </ul>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
203	<p>DIP_AYT-Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del DPD en las fases iniciales de los mismos.</p> <p><b>Descripción Medida de seguridad</b></p> <p>El DPD tiene que participar en el diseño, desarrollo de nuevos productos y servicios, sobre todo en las fases iniciales, por lo que se confeccionaran o modificaran los procedimientos para que el DPD participe activamente en las fases iniciales.</p> <p><b>Normativa a la que afecta</b></p> <p>En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>Responsable Tratamiento: - Aprobar los procedimientos para diseño y desarrollo de nuevos productos y servicios, y establecer la participación del DPD en las operaciones de tratamiento de datos personales.</p> <p>DPD: - Participar en los nuevos diseños y desarrollo en lo referente al tratamiento de datos Personales. Y vigilar que se realicen conforme a las normas de PD.</p> <p>Dependencia de Nuevas Tecnologías: - Consultar con el DPD el tratamiento de datos personales de los nuevos diseños y desarrollos.</p> <p>Dependencia Gestora de la PD: - Coordinar la participación del DPD en los nuevos diseños y desarrollos.</p> <p>Encargado Tratamiento: Usuarios: - Informar de las deficiencias en el Tratamiento de Datos personales en las nuevas implantaciones de productos o servicios.</p>	L1/L2
204	<p>DIP_AYT-Establecer desde la dirección las funciones, competencias y atribuciones del DPD en el desarrollo y gestión de los proyectos, y exigir cumplimiento de dichas funciones y competencias.</p> <p><b>Descripción Medida de seguridad</b></p> <p>El Responsable de la Entidad en el nombramiento del DPD establecerá sus Funciones, competencias y atribuciones , y se le proporcionara los recursos necesarios para que pueda realizarlas con las máximas garantías, y velara por que el DPD cumpla con las mismas.</p> <p><b>Normativa a la que afecta</b></p> <p>En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>Responsable Tratamiento: - Asignar las Funciones al DPD - Proporcionar los recursos necesarios.</p> <p>DPD: - Asumir y cumplir las funciones asignadas. - Solicitar los recursos necesarios.</p> <p>Responsable Funcional del Tratamiento: - Conocer cuales son las funciones del DPD - Comunicar al personal a su cargo las funciones del DPD</p> <p>Dependencia Gestora de la PD: - Coordinar la comunicación de las funciones del DPD a toda la Organización</p> <p>Encargado Tratamiento: - Conocer las Funciones del DPD</p> <p>Usuarios: - Conocer las funciones del DPD</p>	L1/L2
199	<p>DIP_AYT-Formación apropiada del personal sobre protección de datos , seguridad y uso adecuado de las TIC.</p> <p><b>Descripción Medida de seguridad</b></p> <p>Los Responsables de la Entidad, junto con los Responsables de las Dependencias, propondrán y diseñaran acciones formativas para el Personal a su cargo, velando por que todo el personal a su cargo se forme en las materias de Protección de datos y Seguridad de las TIC. Todo el Personal acceder a las acciones formativas que se propongan, para concienciarse y formarse en estas materias.</p> <p><b>Normativa a la que afecta</b></p> <p>Capitulo II RGPD - Principios. Capitulo III RGPD - Derechos del Interesado. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>Responsable Tratamiento: - Diseñara acciones formativas para que todo el personal.</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
199	DIP_AYT-Formación apropiada del personal sobre protección de datos , seguridad y uso adecuado de las TIC.	L1/L2
<b>Descripción Medida de seguridad</b>		
Los Responsables de la Entidad, junto con los Responsables de las Dependencias, propondrán y diseñarán acciones formativas para el Personal a su cargo, velando por que todo el personal a su cargo se forme en las materias de Protección de datos y Seguridad de las TIC. Todo el Personal acceder a las acciones formativas que se propongan, para concienciarse y formarse en estas materias.		
<b>Normativa a la que afecta</b>		
Capitulo II RGPD - Principios. Capitulo III RGPD - Derechos del Interesado. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
<b>Actuaciones de cada Rol</b>		
DPD: - Supervisara y propondrá los contenidos de las acciones formativas. Dependencia Gestora de la PD: - Proponer y diseñar los contenidos de las Acciones formativas Responsable Funcional del Tratamiento: - Velaran por que todo el personal a su cargo reciba los cursos de formación que se propongan. Encargado Tratamiento: - Formara a los usuarios que participen en los encargos de tratamiento de datos personales. Usuarios: - Solicitaran y realizaran los cursos de formación que se propongan., - Solicitaran en su caso las necesidades de formación sobre protección de datos personales.		

### AYTO-02-Ligitimacion y cesion

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
206	DIP_AYT-Usar datos disociados o pseudonimos siempre que sea posible y no implique un esfuerzo desproporcionado	L1/L2
<b>Descripción Medida de seguridad</b>		
En los procesos de trabajo se incorporara medidas para la disociación y pseudonimizacion de los datos personales, empleando los mínimos recursos para ello. Entre otros se pueden emplear en los siguientes procesos: - Archivado de documentos en Papel ordenar por Códigos o referencias, y no utilizar el Nombre de los Interesados para dicho archivo ni otro datos personal. - En la publicación de documentos en Internet, o por medios electrónicos, no publicar datos personales utilizar Códigos o Referencia, siempre que no exista norma que obligue a publicar datos personales, ejemplo publicar ref expediente y no datos personales. Los procesos y sistemas de disociación y seudonimizacion debe ser aprobado por el Responsable del tratamiento. Un ejemplo de seudonimización sería separar los datos como nombre y apellidos de la persona de su número de identificación fiscal, sustituyendo el NIF por un código de manera que no fuese posible atribuir este código a ninguna persona. Entre las tecnicas de seudonimizacion tenemos: - cifrado con clave secreta o con clave de borrado de claves; - función hash; - función con clave almacenada; - descomposición en tokens; - etc.		
<b>Normativa a la que afecta</b>		
Capitulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
<b>Actuaciones de cada Rol</b>		
Responsable Tratamiento: - Aprobar los procesos y sistemas de disociación y seudonimizacion. DPD: - Colaborar en el diseño de los procesos de disociación y seudonimizacion Responsable Funcional del Tratamiento: - Velar por el cumplimiento de los procesos aprobados de disociación y seudonimizacion Dependencia Gestora de la PD: - Comunicar a la organización la Aprobación de los procesos de disociación y seudonimizacion Encargado Tratamiento: - Cumplir con los procedimientos de disociación y seudonimizacion aprobados por el Responsable. Usuarios: - Cumplir y aplicar los proceso de disociación y seudonimizacion		

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
207	<p>DIP_AYT-Evitar el uso de datos biométricos salvo que resulte imprescindible o esté absolutamente justificada</p> <p><b>Descripción Medida de seguridad</b></p> <p>No se utilizarán datos biométricos, a no ser que este bien justificado su uso, y además en el caso que se traten datos biométricos se realizarán las correspondientes justificaciones, y su tratamiento deberá ser aprobada por el órgano competente (Resolución de Alcalde-Presidente)</p> <p><b>Normativa a la que afecta</b></p> <p>Capítulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Aprobar el uso de datos biométricos cuando sea necesario y previa estudio correspondiente.</li> </ul> <p><b>DPD:</b></p> <ul style="list-style-type: none"> <li>- Informar y asesorar sobre el uso de datos biométricos.</li> </ul> <p><b>Responsable Funcional del Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Informar al personal a su cargo sobre el tratamiento de datos biométricos.</li> </ul> <p><b>Dependencia Gestora de la PD:</b></p> <ul style="list-style-type: none"> <li>- Coordinar las comunicaciones del tratamiento de datos biométricos.</li> <li>- Colaborar en los estudios sobre la viabilidad de uso de datos biométricos.</li> </ul> <p><b>Encargado Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Tratar los datos biométricos según las directrices del Responsable.</li> </ul> <p><b>Usuarios:</b></p> <ul style="list-style-type: none"> <li>- Tratar los datos biométricos según las directrices del responsable.</li> </ul>	L1/L2
210	<p>DIP_AYT-Asegurarse de que no existen otras causas de legitimación más adecuadas</p> <p><b>Descripción Medida de seguridad</b></p> <p>Los tratamientos de datos personales se deben realizar con la correspondiente legitimación, así que se tiene que comprobar que la legitimación que justifica el tratamiento es la más adecuada. Hay que tener presente que la legitimación de las Administraciones Públicas es casi siempre la Obligación Legal (en este caso debe haber una norma con rango de ley que justifique el tratamiento), Interés Público y Poder Público (en estos casos existe una competencia que justifica su tratamiento), siendo el Consentimiento una legitimación menos empelada, así con Contratos y el Interés Legítimo.</p> <p>Hay que documentar bien la Base Legítima del Tratamiento, y que no quede ninguna Duda, para ello los Responsables de las Dependencias donde se realiza el tratamiento de los datos personales deben colaborar con el DPD en establecer las Bases de Legitimación del tratamiento de los datos personales.</p> <p><b>Normativa a la que afecta</b></p> <p>Capítulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Establecer procesos para revisión de la legitimación de las actividades de tratamiento</li> </ul> <p><b>DPD:</b></p> <ul style="list-style-type: none"> <li>- Comprobar y aprobar la legitimación de las actividades de tratamiento.</li> </ul> <p><b>Responsable Funcional del Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Comprobar y aprobar la legitimación de las actividades de tratamiento.</li> </ul> <p><b>Dependencia Gestora de la PD:</b></p> <ul style="list-style-type: none"> <li>- Coordinar la comprobación de la legitimación de las Actividades de Tratamiento.</li> </ul> <p><b>Encargado Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Realizar el tratamiento de datos personales conforme a la legitimación asociada a dicho tratamiento.</li> </ul> <p><b>Usuarios:</b></p> <ul style="list-style-type: none"> <li>- Realizar el tratamiento de datos personales conforme a la legitimación asociada a dicho tratamiento.</li> </ul>	L1/L2
211	<p>DIP_AYT-Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrecer siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato</p> <p><b>Descripción Medida de seguridad</b></p> <p>Si la base legítima del tratamiento es un Contrato o Convenio, dejar muy claro si es necesario el Consentimiento para realizar tratamiento de datos que no estén bien legitimados en el contrato.</p> <p>Ejemplo en los contratos de empleados (Laborales o funcionariales), si se piden datos personales que no estén bien contemplados en el contrato, se utilizará el consentimiento, ejemplo solicitar datos de contactos de familiares, datos biométricos, etc.</p> <p><b>Normativa a la que afecta</b></p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
211	<p>DIP_AYT-Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrecer siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato</p> <p><b>Descripción Medida de seguridad</b></p> <p>Si la base legítima del tratamiento es un Contrato o Convenio, dejar muy claro si es necesario el Consentimiento para realizar tratamiento de datos que no estén bien legitimados en el contrato.</p> <p>Ejemplo en los contratos de empleados (Laborales o funcionariales), si se piden datos personales que no estén bien contemplados en el contrato, se utilizará el consentimiento, ejemplo solicitar datos de contactos de familiares, datos biométricos, etc.</p> <p><b>Normativa a la que afecta</b></p> <p>Capítulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Establecer los procedimientos para determinar las recogidas de datos que se basen en los consentimientos.</li> </ul> <p><b>DPD:</b></p> <ul style="list-style-type: none"> <li>- Asesorar en la elaboración de procedimientos para el tratamiento de datos personales que se basen en el consentimiento.</li> </ul> <p><b>Responsable Funcional del Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Implantar y vigilar el cumplimiento de procedimientos para la solicitud de consentimiento</li> <li>- Implantar la utilización en la recogida de información con formularios las cláusulas correspondientes al consentimiento.</li> </ul> <p><b>Dependencia Gestora de la PD:</b></p> <ul style="list-style-type: none"> <li>- Coordinar la elaboración de las cláusulas para consentimiento en la recogida de información mediante formularios.</li> </ul> <p><b>Encargado Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Seguir las directrices del Responsable.</li> </ul> <p><b>Usuarios:</b></p> <ul style="list-style-type: none"> <li>- Cumplir con los procedimientos para la solicitud de consentimiento</li> <li>- Utilizar en la recogida de información los formularios las cláusulas correspondientes al consentimiento.</li> </ul>	L1/L2
212	<p>DIP_AYT-Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas</p> <p><b>Descripción Medida de seguridad</b></p> <p>Es necesario informar y formar al personal que trata datos Personales en la solicitud de Consentimiento para tratamiento de datos personales, así se tiene que tener en cuenta lo siguiente:</p> <p>El considerando 43 del RGPD indica claramente que no es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de datos ya que cuando el responsable del tratamiento es una autoridad pública, siempre hay un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado. Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable. El GT29 considera que hay otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas.</p> <p>Sin perjuicio de estas consideraciones generales, el uso del consentimiento como una base jurídica para el tratamiento de datos por parte de las autoridades públicas no queda totalmente excluido en virtud del marco jurídico del RGPD. Los siguientes ejemplos muestran que el uso del consentimiento puede ser adecuado en determinadas circunstancias.</p> <p>Ejemplo: Una escuela pública pide a sus alumnos el consentimiento para utilizar sus fotografías en una revista escolar impresa. El consentimiento en estas situaciones sería una elección real siempre que no se negara a los alumnos la educación u otros servicios y ellos pudieran negarse al uso de dichas fotografías sin sufrir ningún perjuicio.</p> <p>Más información sobre consentimiento en: <a href="https://www.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf">https://www.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf</a></p> <p><b>Normativa a la que afecta</b></p> <p>Capítulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Establecer procedimientos e instrucciones claras sobre la solicitud del consentimiento.</li> <li>- Informar y formar al personal que trate Datos Personales.</li> </ul> <p><b>DPD:</b></p> <ul style="list-style-type: none"> <li>- Asesorar y dinamizar para conseguir que los procedimientos e instrucciones lleguen a todo el Personal.</li> <li>- Atender todas las cuestiones sobre este tema.</li> </ul> <p><b>Responsable Funcional del Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Cumplir y hacer cumplir los procedimientos y normas sobre el consentimiento.</li> <li>- Difundir y vigilar que todo el personal a su cargo cumple correctamente con los procedimientos y normas de solicitud del Consentimiento.</li> </ul> <p><b>Dependencia Gestora de la PD:</b></p> <ul style="list-style-type: none"> <li>- Coordinar la difusión de los Procedimientos y normas a todo el personal implicado.</li> </ul> <p><b>Encargado Tratamiento:</b></p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
212	<p>DIP_AYT-Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas</p> <p><b>Descripción Medida de seguridad</b></p> <p>Es necesario informar y formar al personal que trata datos Personales en la solicitud de Consentimiento para tratamiento de datos personales, así se tiene que tener en cuenta lo siguiente: El considerando 43 del RGPD indica claramente que no es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de datos ya que cuando el responsable del tratamiento es una autoridad pública, siempre hay un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado. Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable. El GT29 considera que hay otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas. Sin perjuicio de estas consideraciones generales, el uso del consentimiento como una base jurídica para el tratamiento de datos por parte de las autoridades públicas no queda totalmente excluido en virtud del marco jurídico del RGPD. Los siguientes ejemplos muestran que el uso del consentimiento puede ser adecuado en determinadas circunstancias. Ejemplo: Una escuela pública pide a sus alumnos el consentimiento para utilizar sus fotografías en una revista escolar impresa. El consentimiento en estas situaciones sería una elección real siempre que no se negara a los alumnos la educación u otros servicios y ellos pudieran negarse al uso de dichas fotografías sin sufrir ningún perjuicio. Mas informacion sobre consentimiento en: <a href="https://www.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf">https://www.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf</a></p> <p><b>Normativa a la que afecta</b></p> <p>Capitulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <ul style="list-style-type: none"> <li>- Cumplir y hacer cumplir los procedimientos y normas sobre el consentimiento que aplican el Responsable.</li> <li>- Difundir y vigilar que todo el personal a su cargo cumple correctamente con los procedimientos y normas de solicitud del Consentimiento.</li> </ul> <p>Usuarios: - Cumplir las normas sobre el consentimiento que dicte el Responsable.</p>	L1/L2
213	<p>DIP_AYT-Establecer procedimientos claros para manifestar la revocación del consentimiento o la solicitud de oposición a un determinado tratamiento. Si la organización realiza acciones publicitarias, tener en cuenta las reglas especiales existentes para las comunicaciones comerciales y, en particular, cuando estas se llevan a cabo a través de comunicaciones electrónicas.</p> <p><b>Descripción Medida de seguridad</b></p> <p>Establecer procedimientos para posibilitar la revocación del consentimiento. En los procedimientos electrónicos que se pide consentimiento, se debe establecer procedimientos electrónicos para su revocación, y se establecerá avisos automáticos para informar sobre el procedimiento para la revocación del consentimiento.</p> <p><b>Normativa a la que afecta</b></p> <p>Capitulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> - Establecer los procedimientos y protocolos para la revocación del consentimiento.</p> <p><b>DPD:</b> - Apoyar y asesorar en los procedimientos y normas sobre la revocación del consentimiento.</p> <p><b>Responsable Funcional del Tratamiento:</b> - Aplicar los procedimientos sobre revocación del consentimiento. - Y transmitir al personal a su cargo los procedimientos y normas para la revocación.</p> <p><b>Dependencia Gestora de la PD:</b> - Coordinar la difusión de los procedimientos y normas al personal</p> <p><b>Encargado Tratamiento:</b> - Cumplir con las normas y procedimientos de revocación del consentimiento que aplique el Responsable.</p> <p>Usuarios: - Cumplir con las normas y procedimientos de revocación.</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
214	<p>DIP_AYT-Exigir garantías de que los datos personales provenientes de terceros se han obtenido y cedido lealmente.</p> <p><b>Descripción Medida de seguridad</b></p> <p>Establecer procedimientos que permitan garantizar que los datos cedidos por terceros se hacen de forma legal y cumpliendo con las normas de protección de datos, para ello se deben realizar en base a garantía legales, convenios, etc.. En el caso la cesión de información de otras Administraciones se utilizara en lo posible los sistemas de Intermediación.</p> <p><b>Normativa a la que afecta</b></p> <p>Capitulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Establecer los Procedimientos para la Obtención de Datos por Terceros, y dar instrucciones claras al respecto.</li> <li>- Establecer los Procedimientos para la Cesión de Información a Terceros, y dar instrucciones claras al respecto.</li> </ul> <p><b>DPD:</b></p> <ul style="list-style-type: none"> <li>- Apoyar y asesoran el los Procedimientos e Instrucciones que se dicten.</li> <li>- Proponer opciones de mejoras.</li> </ul> <p><b>Responsable Funcional del Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Revisar los Convenios y Contratos con terceros para que quede claro tanto la Obtención de los datos que nos ceden de terceros, como los que ceden a terceros, para que quede claro el tratamiento de dichos datos.</li> </ul> <p><b>Dependencia Gestora de la PD:</b></p> <ul style="list-style-type: none"> <li>- Difundir al personal afectado la información sobre la cesión de información.</li> </ul> <p><b>Encargado Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Cumplir las instrucciones del Responsables sobre la Cesión de la Información.</li> </ul> <p><b>Usuarios:</b></p> <ul style="list-style-type: none"> <li>- Cumplir las instrucciones del Responsables sobre la Cesión de la Información.</li> </ul>	L1/L2
209	<p>DIP_AYT-Si se ceden datos personales, establecer por escrito acuerdos que contemplen las condiciones bajo las que se produce la cesión y, en su caso, las relativas a cesiones posteriores así como las posibilidades de supervisión y control del cumplimiento del acuerdo.</p> <p><b>Descripción Medida de seguridad</b></p> <p>La cesión de datos personales deberá estar bien documentada, y cada dependencia que realice cesiones de datos personales deberá documentar bien dichos cesiones y tener justificación de las mismas. Se llevar un control de las cesiones de datos personales, posibilitando una supervisan o auditoria sobre las cesiones. Así cuando se cedan datos a un tercero distinto del interesado, se deberá documentar la Autorización o justificación del porque se ha autorizado dicha cesión, archivando el el correspondiente expediente las autorización o documentos que autorizan dicha cesión. Igualmente si la cesión es a otra Administración, se debe documentarla en la base legal por la que se realiza dicha cesión.</p> <p><b>Normativa a la que afecta</b></p> <p>Capitulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Establecer y aprobar los procedimientos de cesión de datos.</li> </ul> <p><b>DPD:</b></p> <ul style="list-style-type: none"> <li>- Colaborar en la elaboración de procedimientos de cesión de información</li> <li>- Velar por el cumplimiento de los procedimientos de cesión de información.</li> </ul> <p><b>Responsable Funcional del Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Velar por el cumplimiento de los procedimientos de cesión de información.</li> <li>- Comunicar a todo el personal a su cargo sobre los procedimientos de cesión de información</li> </ul> <p><b>Dependencia Gestora de la PD:</b></p> <ul style="list-style-type: none"> <li>- Coordinar la comunicación de la aprobación de los procedimientos de cesión de información</li> </ul> <p><b>Encargado Tratamiento:</b></p> <ul style="list-style-type: none"> <li>- Cumplir con los procedimientos de cesión de información.</li> </ul> <p><b>Usuarios:</b></p> <ul style="list-style-type: none"> <li>- Cumplir con los procedimientos de cesión de información.</li> </ul>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
215	<p>DIP_AYT-Verificar que el tratamiento de datos especialmente protegidos es absolutamente imprescindible para la finalidad o finalidades perseguidas y se realiza según la normativa de protección de datos</p> <p><b>Descripción Medida de seguridad</b></p> <ul style="list-style-type: none"> <li>- Establecer procedimientos y protocolos para verificar que el tratamiento de datos especialmente protegidos se realiza, cumpliendo la normativa de protección de datos, y en su caso comprobar que se realiza con el consentimiento adecuado del interesado.</li> </ul> <p><b>Normativa a la que afecta</b></p> <p>Capítulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>Responsable Tratamiento: - Establecer procedimientos y protocolos para verificar que el tratamiento de datos especialmente protegidos se realiza.</p> <p>DPD: - Asesorar en al Responsables y a todo el personales en los protocolos de verificación sobre tratamiento de datos especialmente protegidos.</p> <p>Responsable Funcional del Tratamiento: - Velar por que se traten los mínimos datos especialmente protegidos. - Transmitir al personal las normas y protocolos al respecto.</p> <p>Dependencia Gestora de la PD: - Coordinar y traslada a todo el personal las normas y procedimientos sobre el tratamiento de datos especialmente protegidos.</p> <p>Encargado Tratamiento: - Cumplir con las normas y procedimientos que dicte el Responsable.</p> <p>Usuarios: - Cumplir con las normas y procedimientos que dicte el responsable.</p>	L1/L2
216	<p>DIP_AYT-Verificar la legitimidad de la interconexión de datos prevista y Definir claramente los datos personales resultantes del tratamiento y verificar tras el proceso que son los únicos que se han generado</p> <p><b>Descripción Medida de seguridad</b></p> <p>Revisión y verificación de los Procesos de interconexión de datos se realizan legítimamente y cumpliendo con la normativa de protección de datos. Un ejemplo claro es la interconexión y uso de los datos de Padrón de Habitantes que solo se puede hacer cuando existe argumentos de legitimación y legales para realizar.</p> <p><b>Normativa a la que afecta</b></p> <p>Capítulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>Responsable Tratamiento: - Establecer la revisión y verificación de los Proceso de interconexión.</p> <p>DPD: - Asesorar y supervisar que los procesos de interconexión cumplan con la legitimidad del tratamiento.</p> <p>Responsable Funcional del Tratamiento: - Cumplir los procesos de interconexión y velar por que cumplan con la legitimación del los tratamiento.</p> <p>Dependencia Gestora de la PD: - Coordinar y notificar los procedimientos de interconexión que se vayan aprobando.</p> <p>Encargado Tratamiento: - Cumplir con los procedimientos establecidos por el Responsable.</p> <p>Usuarios: - Cumplir con los procesos de interconexión establecidos y aprobados por el Responsable, y no realizar interconexión de datos personales que no estén establecidos por el Responsable.</p>	L1/L2
217	<p>DIP_AYT-Evitar el uso de cookies u otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos cortos de caducidad de las cookies, etc.).</p> <p><b>Descripción Medida de seguridad</b></p> <p>Establecer procedimientos para la aprobación del uso de las cookies cuando sea estrictamente necesario. Y establecer y aprobar la Política de Cookies.</p> <p><b>Normativa a la que afecta</b></p> <p>Capítulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
217	DIP_AYT-Evitar el uso de cookies u otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos cortos de caducidad de las cookies, etc.).	L1/L2
Descripción Medida de seguridad		
Establecer procedimientos para la aprobación del uso de las cookies cuando sea estrictamente necesario. Y establecer y aprobar la Política de Cookies.		
Normativa a la que afecta		
Capítulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
Actuaciones de cada Rol		
Responsable Tratamiento: - Establecer la Política de Cookies y los procedimientos de aprobación de su uso. DPD: - Asesorar y coordinar la Elaboración y modificación de Políticas y procedimiento de uso de cookies. Responsable Funcional del Tratamiento: - Velar por el cumplimiento de Políticas y Procedimientos del uso de las cookies. Dependencia Gestora de la PD: - Coordinar la elaboración de Políticas y Procedimientos del uso de cookies, así como su difusión entre el personal implicado. Encargado Tratamiento: - Cumplir con las Políticas y Procedimientos de Uso de cookies establecidas por el Responsable. Usuarios: - Cumplir con las Políticas y Procedimientos de Uso de cookies establecidas por el Responsable.		
218	DIP_AYT-Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas	L1/L2
Descripción Medida de seguridad		
Establecer una política de cookies correcta y que cumpla con la protección de datos, y dar información de la misma por capas y cumpliendo la normativa.		
Normativa a la que afecta		
Capítulo II RGPD - Principios. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
Actuaciones de cada Rol		
Responsable Tratamiento: - Establecer los mecanismos y procedimientos para dar la información sobre las Políticas de Cookies que se implanten DPD: - Asesora de como informar sobre la Política de Cookies. Responsable Funcional del Tratamiento: - Velar por que se implante los sistemas de información de las Políticas de Cookies. Dependencia Gestora de la PD: - Coordinar y difundir los sistemas de información de las Políticas de Cookies que se implante entre el personal afectado. Encargado Tratamiento: - Cumplir con los sistemas y medios de comunicación de las políticas de Cookies que implante el Responsable. Usuarios: - Cumplir con los sistemas y medios de comunicación de las políticas de Cookies que implante el Responsable.		

### AYTO-04-Notificación y Registro de las Actividades

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
221	DIP_AYT-Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo	L1/L2
Descripción Medida de seguridad		
Definir procesos y metodologías para revisión del cumplimiento de la normativa de protección de datos en el desarrollo de nuevos proyectos, especialmente proyectos de Sistemas de Información.		
Normativa a la que afecta		
Artículo 30 RGPD - Registro de las actividades de tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
Actuaciones de cada Rol		

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
221	DIP_AYT-Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo	L1/L2
Descripción Medida de seguridad		
Definir procesos y metodologías para revisión del cumplimiento de la normativa de protección de datos en el desarrollo de nuevos proyectos, especialmente proyectos de Sistemas de Información.		
Normativa a la que afecta		
Artículo 30 RGPD - Registro de las actividades de tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
Actuaciones de cada Rol		
Responsable Tratamiento: - Implantar y establecer los procedimientos y metodologías para desarrollo de nuevos proyectos. DPD: - Asesorar y colaborar en la elaboración de los procedimientos y metodologías para desarrollo de nuevos proyectos. Responsable Funcional del Tratamiento: - Velar por el cumplimiento de los procedimientos y metodología que se implanten. Dependencia Gestora de la PD: - Coordinar la elaboración de los procedimientos y metodologías y difusión de los mismos entre el personal afectado. Encargado Tratamiento: - Cumplir con los procedimientos y metodologías implantados por el Responsable. Usuarios: - Cumplir con los procedimientos y metodologías implantados por el Responsable.		

### AYTO-05-Transparencia de los tratamientos

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
222	DIP_AYT-Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas.	L1/L2
Descripción Medida de seguridad		
Establecer una política de cookies correcta y que cumpla con la protección de datos, y dar información de la misma por capas y cumpliendo la normativa.		
Normativa a la que afecta		
Artículo 12 RGPD - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
Actuaciones de cada Rol		
Responsable Tratamiento: - Establecer los mecanismos y procedimientos para dar la información sobre las Políticas de Cookies que se implanten DPD: - Asesora de como informar sobre la Política de Cookies. Responsable Funcional del Tratamiento: - Velar por que se implante los sistemas de información de las Políticas de Cookies. Dependencia Gestora de la PD: - Coordinar y difundir los sistemas de información de las Políticas de Cookies que se implante entre el personal afectado. Encargado Tratamiento: - Cumplir con los sistemas y medios de comunicación de las políticas de Cookies que implante el Responsable. Usuarios: - Cumplir con los sistemas y medios de comunicación de las políticas de Cookies que implante el Responsable.		
223	DIP_AYT-Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada y Estructurada, y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión.	L1/L2
Descripción Medida de seguridad		
Establecer procedimientos ágiles para generación de cláusulas modelos para cada Actividad de Tratamiento de Datos personales. Utilizar la aplicación proDatos de Diputación para acceder de forma rápida a las cláusulas de información desde el Registro de Actividades de Tratamiento publicado en la aplicación. Ejemplo en formularios electrónicos hacer que se accede de forma online a las cláusulas de la actividad de tratamiento.		
Normativa a la que afecta		

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
223	<p>DIP_AYT-Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada y Estructurada, y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión.</p> <p><b>Descripción Medida de seguridad</b></p> <p>Establecer procedimientos ágiles para generación de cláusulas modelos para cada Actividad de Tratamiento de Datos personales. Utilizar la aplicación proDatos de Diputación para acceder de forma rápida a las cláusulas de información desde el Registro de Actividades de Tratamiento publicado en la aplicación. Ejemplo en formularios electrónicos hacer que se accede de forma online a las cláusulas de la actividad de tratamiento.</p> <p><b>Normativa a la que afecta</b></p> <p>Artículo 12 RGPD - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>Responsable Tratamiento: - Establecer los procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad. DPD: - Asesorar para elaborar los procedimientos de revisión de formularios de recogida de datos personales. Responsable Funcional del Tratamiento: - Velar por que se cumplan los procedimientos de revisión de formularios de recogida de datos personales. Dependencia Gestora de la PD: - Coordinar y difundirlos procedimientos de revisión de formularios de recogida de datos personales. Encargado Tratamiento: - Cumplir con procedimientos de revisión de formularios de recogida de datos personales que implante el Responsable. Usuarios: - Cumplir con los sistemas y medios de comunicación de las políticas de Cookies que implante el Responsable.</p>	L1/L2
224	<p>DIP_AYT-Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión.</p> <p><b>Descripción Medida de seguridad</b></p> <p>Utilizar la aplicación proDatos de Diputación para acceder de forma rápida a las cláusulas de información desde el Registro de Actividades de Tratamiento publicado en la aplicación. Ejemplo en formularios electrónicos hacer que se accede de forma online a las cláusulas de la actividad de tratamiento.</p> <p><b>Normativa a la que afecta</b></p> <p>Artículo 12 RGPD - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>Responsable Tratamiento: - Establecer los procedimientos para estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles. DPD: - Asesorar para elaborar los procedimientos para estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles. Responsable Funcional del Tratamiento: - Velar por que se cumplan los procedimientos para estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles. Dependencia Gestora de la PD: - Coordinar y difundirlos procedimientos para estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles. Encargado Tratamiento: - Cumplir con procedimientos para estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles que implante el Responsable. Usuarios: - Cumplir con procedimientos para estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles que implante el Responsable.</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
225	DIP_AYT-Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización.	L1/L2
Descripción Medida de seguridad		
Ejemplo: Poner carteles con códigos QR con acceso a las Política de Privacidad, así como la las política de Seguridad y normativa aprobada sobre tratamiento de datos personales.		
Normativa a la que afecta		
Artículo 12 RGPD - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
Actuaciones de cada Rol		
Responsable Tratamiento: - Establecer políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización. DPD: - Asesorar para elaborar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización. Responsable Funcional del Tratamiento: - Velar por que se cumplan las políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización. Dependencia Gestora de la PD: - Coordinar y difundirlos las políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización. Encargado Tratamiento: - Cumplir con las políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización. que implante el Responsable. Usuarios: -- Cumplir con las políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización. que implante el Responsable.		

### AYTO-06-Calidad de los datos

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
226	DIP_AYT-Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que que luego no son utilizados en ningún proceso.	L1/L2
Descripción Medida de seguridad		
Establecer en los Procedimientos, normas claras sobre la recogida de datos personales y de la minimización en la recogida, para evitar la recogida de datos que no se utilicen		
Normativa a la que afecta		
Capítulo II RGPD - Principios. Artículo 4. LOPDGDD - Exactitud de los datos. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
Actuaciones de cada Rol		
Responsable Tratamiento: - Establecer en los Procedimientos, normas claras sobre la recogida de datos personales y de la minimización en la recogida DPD: - Asesorar para elaborar los Procedimientos, normas claras sobre la recogida de datos personales y de la minimización en la recogida. Responsable Funcional del Tratamiento: - Velar por que se cumplan los Procedimientos, normas claras sobre la recogida de datos personales y de la minimización en la recogida. Dependencia Gestora de la PD: - Coordinar y difundirlos los Procedimientos, normas claras sobre la recogida de datos personales y de la minimización en la recogida. Encargado Tratamiento: - Cumplir con los Procedimientos, normas claras sobre la recogida de datos personales y de la minimización en la recogida. que implante el Responsable. Usuarios: Cumplir con los Procedimientos, normas claras sobre la recogida de datos personales y de la minimización en la recogida. que implante el Responsable.		

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
227	<p>DIP_AYT-Establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización que estén autorizados a utilizarlo</p> <p><b>Descripción Medida de seguridad</b></p> <p>Revisar los procedimientos que actualicen datos personales para que se actualicen en lo posible de de forma automática por los Sistemas de Información que los usen, y si no es posible establecer los mecanismos para realizar una comunicación a otras dependencias para que actualicen</p> <p><b>Normativa a la que afecta</b></p> <p>Capitulo II RGPD - Principios. Artículo 4. LOPDGDD - Exactitud de los datos. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> - Establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización que estén autorizados a utilizarlo.</p> <p><b>DPD:</b> - Asesorar para establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización que estén autorizados a utilizarlo</p> <p><b>Responsable Funcional del Tratamiento:</b> - Velar por que se cumplan las medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización.</p> <p><b>Dependencia Gestora de la PD:</b> - Coordinar y difundirlos las medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización.</p> <p><b>Encargado Tratamiento:</b> - Cumplir con las medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización, que implante el Responsable.</p> <p><b>Usuarios:</b> Cumplir con las medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización, que implante el Responsable.</p>	L1/L2
228	<p>DIP_AYT-Siempre que sea posible, utilizar datos anónimos, disociados o pseudónimos. Y garantizar que se apliquen las medidas de seguridad adecuadas</p> <p><b>Descripción Medida de seguridad</b></p> <p>En los expedientes en Papel utilizar códigos o referencias de expediente para archivar los expedientes, realizando la relación entre el código y referencia en los sistemas de información o en documentos controlados y solo accesible por el personal autorizado. En los expedientes gestionados en Sistemas de Información intentar que los datos personales se relacionen con los expedientes a través de la ref. de expedientes, de forma que en los datos del expediente no aparezcan los datos personales del interesado.</p> <p><b>Normativa a la que afecta</b></p> <p>Capitulo II RGPD - Principios. Artículo 4. LOPDGDD - Exactitud de los datos. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> - Establecer medidas técnicas y organizativas para utilizar datos anónimos, disociados o pseudónimos siempre que sea posible</p> <p><b>DPD:</b> - Asesorar para establecer medidas técnicas y organizativas para utilizar datos anónimos, disociados o pseudónimos siempre que sea posible.</p> <p><b>Responsable Funcional del Tratamiento:</b> - Velar por que se cumplan las medidas técnicas y organizativas para utilizar datos anónimos, disociados o pseudónimos siempre que sea posible.</p> <p><b>Dependencia Gestora de la PD:</b> - Coordinar y difundirlos las medidas técnicas y organizativas para utilizar datos anónimos, disociados o pseudónimos siempre que sea posible.</p> <p><b>Encargado Tratamiento:</b> - Cumplir con las medidas técnicas y organizativas para utilizar datos anónimos, disociados o pseudónimos siempre que sea posible, que implante el Responsable.</p> <p><b>Usuarios:</b> Cumplir con las medidas técnicas y organizativas para utilizar datos anónimos, disociados o pseudónimos siempre que sea posible, que implante el Responsable.</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
229	<p>DIP_AYT-Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas</p> <p><b>Descripción Medida de seguridad</b></p> <p>Utilizar códigos para identificación de interesados en lugar de datos personales que identifiquen a las personas. Ejemplo: En sistema de citas previas utilizar código en lugar del NIF o Nombre.</p> <p><b>Normativa a la que afecta</b></p> <p>Capítulo II RGPD - Principios. Artículo 4. LOPDGDD - Exactitud de los datos. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> - Establecer medidas técnicas y organizativas para utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos.</p> <p><b>DPD:</b> - Asesorar para establecer medidas técnicas y organizativas para utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos.</p> <p><b>Responsable Funcional del Tratamiento:</b> - Velar por que se cumplan las medidas técnicas y organizativas utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos.</p> <p><b>Dependencia Gestora de la PD:</b> - Coordinar y difundirlos las medidas técnicas y organizativas para utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos.</p> <p><b>Encargado Tratamiento:</b> - Cumplir con las medidas técnicas y organizativas para utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, que implante el Responsable.</p> <p><b>Usuarios:</b> - Cumplir con las medidas técnicas y organizativas para utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, que implante el Responsable.</p>	L1/L2
230	<p>DIP_AYT-Suministra información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en particular, a través de una política de privacidad visible y accesible</p> <p><b>Descripción Medida de seguridad</b></p> <p>Poner carteles con información sobre las actividades de tratamiento y de las políticas de privacidad, con enlace vía códigos QR o dirección web para acceso a la información mas detallada sobre el tratamiento de los datos personales que se realizan para los servicios que se prestan</p> <p><b>Normativa a la que afecta</b></p> <p>Capítulo II RGPD - Principios. Artículo 4. LOPDGDD - Exactitud de los datos. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> - Establecer sistemas y procedimientos para suministrar información transparente y clara sobre tratamiento de datos personales.</p> <p><b>DPD:</b> - Asesorar para elaborar sistemas y procedimientos para suministrar información transparente y clara sobre tratamiento de datos personales.</p> <p><b>Responsable Funcional del Tratamiento:</b> - Velar por que se implementen los sistemas y procedimientos para suministrar información transparente y clara sobre tratamiento de datos personales.</p> <p><b>Dependencia Gestora de la PD:</b> - Coordinar y difundirlos los sistemas y procedimientos para suministrar información transparente y clara sobre tratamiento de datos personales.</p> <p><b>Encargado Tratamiento:</b> - Cumplir con los sistemas y procedimientos para suministrar información transparente y clara sobre tratamiento de datos personales que implante el Responsable.</p> <p><b>Usuarios:</b> -- Cumplir con los sistemas y procedimientos para suministrar información transparente y clara sobre tratamiento de datos personales que implante, que implante el Responsable.</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
231	<p>DIP_AYT-Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer.</p> <p>Descripción Medida de seguridad</p> <p>Revisar y mejorar los procedimientos para establecer mecanismos para la detección de errores y corrección.</p> <p>Normativa a la que afecta</p> <p>Capítulo II RGPD - Principios. Artículo 4. LOPDGDD - Exactitud de los datos. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer. DPD: - Asesorar para elaborar mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer.</p> <p>Responsable Funcional del Tratamiento: - Velar por que se implementen los mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer.</p> <p>Dependencia Gestora de la PD: - Coordinar y difundirlos los mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer .</p> <p>Encargado Tratamiento: - Cumplir con los mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer, que implante el Responsable.</p> <p>Usuarios: -- Cumplir con los mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer, que implante el Responsable.</p>	L1/L2
232	<p>DIP_AYT-Definir claramente los plazos de cancelación de todos los datos personales de los sistemas de información, y establecer los controles adecuados.</p> <p>Descripción Medida de seguridad</p> <p>Realizar normas y procedimientos para establecer los plazos de cancelación de los datos personales.</p> <p>Normativa a la que afecta</p> <p>Capítulo II RGPD - Principios. Artículo 4. LOPDGDD - Exactitud de los datos. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Establecer mecanismos y procedimientos que definan claramente los plazos de cancelación de todos los datos personales de los sistemas de información, y establecer los controles adecuados</p> <p>DPD: - Asesorar para elaborar mecanismos y procedimientos que definan claramente los plazos de cancelación de todos los datos personales de los sistemas de información, y establecer los controles adecuados.</p> <p>Responsable Funcional del Tratamiento: - Velar por que se implementen los mecanismos y procedimientos que definan claramente los plazos de cancelación de todos los datos personales de los sistemas de información, y establecer los controles adecuados.</p> <p>Dependencia Gestora de la PD: - Coordinar y difundirlos los mecanismos y procedimientos que definan claramente los plazos de cancelación de todos los datos personales de los sistemas de información, y establecer los controles adecuados.</p> <p>Encargado Tratamiento: - Cumplir con los mecanismos y procedimientos que definan claramente los plazos de cancelación de todos los datos personales de los sistemas de información, y establecer los controles adecuados, que implante el Responsable.</p> <p>Usuarios: -- Cumplir con los mecanismos y procedimientos que p que definan claramente los plazos de cancelación de todos los datos personales de los sistemas de información, y establecer los controles adecuados, que implante el Responsable.</p>	L1/L2

### AYTO-07-Categorías Especiales de Datos

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
--------	---------------------	-------------------

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
233	DIP_AYT-Evitar el uso de datos especialmente protegidos salvo que resulte absolutamente necesario y si es necesario. Y establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él.	L1/L2
Descripción Medida de seguridad		
Establecer normas y procedimientos para la gestión del consentimiento en el tratamiento de datos especialmente protegidos.		
Normativa a la que afecta		
Artículo 9 RGPD - Tratamiento de categorías especiales de datos personales. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
Actuaciones de cada Rol		
Responsable Tratamiento: DPD: Responsable Funcional del Tratamiento: Dependencia Gestora de la PD: Encargado Tratamiento: Usuarios:		

### AYTO-08-Deber de secreto

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
234	DIP_AYT-Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales.	L1/L2
Descripción Medida de seguridad		
Formar y concienciar a las personas que tratan datos personales sobre la obligación de guardar secreto.		
Normativa a la que afecta		
Artículo 5. LOPDGDD - Deber de confidencialidad. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		
Actuaciones de cada Rol		
Responsable Tratamiento: - Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales. DPD: - Asesorar para elaborar mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales. Responsable Funcional del Tratamiento: - Realizar y colaborar con la de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales. Dependencia Gestora de la PD: - Coordinar la de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales. Encargado Tratamiento: - Realizar concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales entre el personal que trate datos personales Usuarios: - Asistir en las acciones de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales., que realice el Responsable.		

235	DIP_AYT-Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores que acceden a datos personales de la obligación de guardar secreto sobre aquellos datos personales que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento	L1/L2
Descripción Medida de seguridad		
Establecer los procedimientos de recabar la confidencialidad y el deber de secreto a todo el personal que trate datos personales.		
Normativa a la que afecta		
Artículo 5. LOPDGDD - Deber de confidencialidad. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.		

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
235	<p>DIP_AYT-Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores que acceden a datos personales de la obligación de guardar secreto sobre aquellos datos personales que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento</p> <p>Descripción Medida de seguridad</p> <p>Establecer los procedimientos de recabar la confidencialidad y el deber de secreto a todo el personal que trate datos personales.</p> <p>Normativa a la que afecta</p> <p>Artículo 5. LOPDGDD - Deber de confidencialidad. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Establecer los procedimientos de recabar la confidencialidad y el deber de secreto a todo el personal que trate datos personales.. DPD: - Asesorar para establecer los procedimientos de recabar la confidencialidad y el deber de secreto a todo el personal que trate datos personales.. Responsable Funcional del Tratamiento. - Realizar y colaborar en los procedimientos de recabar la confidencialidad y el deber de secreto a todo el personal que trate datos personales.. Dependencia Gestora de la PD: - Coordinar en los procedimientos de recabar la confidencialidad y el deber de secreto a todo el personal que trate datos personales.. Encargado Tratamiento: - Cumplir con los procedimientos de recabar la confidencialidad y el deber de secreto a todo el personal que trate datos personales.. Usuarios: - Cumplir con la confidencialidad y el deber de secreto sobre el tratamiento de datos personales.</p>	L1/L2
236	<p>DIP_AYT-Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales</p> <p>Descripción Medida de seguridad</p> <p>Realizar norma y procedimiento para la destrucción de soportes desechados con datos personales.</p> <p>Normativa a la que afecta</p> <p>Artículo 5. LOPDGDD - Deber de confidencialidad. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Realizar norma y procedimiento para la destrucción de soportes desechados con datos personales. DPD: - Asesorar para realizar norma y procedimiento para la destrucción de soportes desechados con datos personales. Responsable Funcional del Tratamiento. - Realizar y colaborar en la elaboración de normas y procedimientos para la destrucción de soportes desechados con datos personales. Dependencia Gestora de la PD: - Coordinar en la elaboración de normas y procedimientos para la destrucción de soportes desechados con datos personales. Encargado Tratamiento: - Cumplir con las normas y procedimientos para la destrucción de soportes desechados con datos personales.. Usuarios: - Cumplir con las normas y procedimientos para la destrucción de soportes desechados con datos personales..</p>	L1/L2
237	<p>DIP_AYT-Formación adecuada de los empleados sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información</p> <p>Descripción Medida de seguridad</p> <p>Los Responsables de la Entidad, junto con los Responsables de las Dependencias, propondrán y diseñarán acciones formativas para el Personal a su cargo, velando por que todo el personal a su cargo se forme en las materias de Protección de datos y Seguridad de las TIC, de forma que queden claras sus obligaciones y responsabilidades respecto a la confidencialidad de la Información. Todo el Personal acceder a las acciones formativas que se propongan, para concienciarse y formarse en estas materias.</p> <p>Normativa a la que afecta</p> <p>Artículo 5. LOPDGDD - Deber de confidencialidad. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
237	DIP_AYT-Formación adecuada de los empleados sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información	L1/L2
Descripción Medida de seguridad		
<p>Los Responsables de la Entidad, junto con los Responsables de las Dependencias, propondrán y diseñarán acciones formativas para el Personal a su cargo, velando por que todo el personal a su cargo se forme en las materias de Protección de datos y Seguridad de las TIC, de forma que queden claras sus obligaciones y responsabilidades respecto a la confidencialidad de la Información. Todo el Personal acceder a las acciones formativas que se propongan, para concienciarse y formarse en estas materias.</p>		
Normativa a la que afecta		
<p>Artículo 5. LOPDGDD - Deber de confidencialidad. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p>		
Actuaciones de cada Rol		
<p>Responsable Tratamiento: - Realizar planes y acciones formativas sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información. DPD: - Asesorar para realizar planes y acciones formativas sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información. Responsable Funcional del Tratamiento. - Realizar y colaborar en la elaboración planes y acciones formativas sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información. Dependencia Gestora de la PD: - Coordinar los planes y acciones formativas sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información. Encargado Tratamiento: - Realizar acciones formativas sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información, entre el personal a su cargo. Usuarios: - Asistir a las acciones formativas sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información, que realice el Responsable.</p>		

238	DIP_AYT-Establecimiento de sanciones disuasorias para los empleados que violen la confidencialidad de los datos personales y comunicación clara y completa de las mismas.	L1/L2
Descripción Medida de seguridad		
<p>Realizar una norma sobre sanciones por incumplimiento de la confidencialidad de los datos personales.</p>		
Normativa a la que afecta		
<p>Artículo 5. LOPDGDD - Deber de confidencialidad. Artículo 32 RGPD - Seguridad del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p>		
Actuaciones de cada Rol		
<p>Responsable Tratamiento: - Realizar una norma sobre sanciones por incumplimiento de la confidencialidad de los datos personales. - Asesorar para realizar Realizar una norma sobre sanciones por incumplimiento de la confidencialidad de los datos personales. - Realizar y colaborar en la elaboración de norma sobre sanciones por incumplimiento de la confidencialidad de los datos personales. Dependencia Gestora de la PD: - Coordinar y difundir las normas sobre sanciones por incumplimiento de la confidencialidad de los datos personales que se aprueben Encargado Tratamiento: - Establecer las sanciones que apruebe el Responsable Usuarios: - Cumplir con las sanciones en caso de incumplimiento de la confidencialidad de los datos personales.</p>		

### AYTO-09-Tratamientos por Encargo

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
--------	---------------------	-------------------

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
239	<p>DIP_AYT-Establecer procedimientos que garanticen que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos</p> <p><b>Descripción Medida de seguridad</b></p> <p>Establecer modelos de contratos y convenios de encargo de tratamiento de datos personales que sean fácilmente accesible para incluirlos en los pliegos de contratación o en los convenios de colaboración. Ejemplo es la publicación de esos modelos en la aplicación proDatos</p> <p><b>Normativa a la que afecta</b></p> <p>Artículo 28 RGPD - Encargado del tratamiento Artículo 33. LOPDGDD- Encargado del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> Establecer modelos de contratos y convenios de encargo de tratamiento de datos personales que sean fácilmente accesible para incluirlos en los pliegos de contratación o en los convenios de colaboración.</p> <p><b>DPD:</b> Asesorar en la realización de modelos de contratos y convenios de encargo de tratamiento de datos personales que sean fácilmente accesible para incluirlos en los pliegos de contratación o en los convenios de colaboración.</p> <p><b>Responsable Funcional del Tratamiento:</b> Velar por aplicar los modelos de contratos y convenios de encargo de tratamiento de datos personales que sean fácilmente accesible para incluirlos en los pliegos de contratación o en los convenios de colaboración.</p> <p><b>Dependencia Gestora de la PD:</b> Coordinar y difundir modelos de contratos y convenios de encargo de tratamiento de datos personales que sean fácilmente accesible para incluirlos en los pliegos de contratación o en los convenios de colaboración.</p> <p><b>Encargado Tratamiento:</b> Cumplir con los contratos y convenios de encargo de tratamiento de datos personales que se aplique.</p> <p><b>Usuarios:</b> Colaborar en la aplicación de modelos de contratos y convenios de encargo de tratamiento de datos personales que sean fácilmente accesible para incluirlos en los pliegos de contratación o en los convenios de colaboración.</p>	L1/L2
240	<p>DIP_AYT-Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad. Establecer contractualmente mecanismos de supervisión, verificación y auditoría de los tratamientos encargados a terceros estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación homologados y de acreditada solvencia</p> <p><b>Descripción Medida de seguridad</b></p> <p>Establecer normas claras para la elaboración los pliegos de contratación para seleccionar a encargados de tratamiento que proporcionen garantías suficientes de cumplimiento sobre la normativa de protección de datos</p> <p><b>Normativa a la que afecta</b></p> <p>Artículo 28 RGPD - Encargado del tratamiento Artículo 33. LOPDGDD- Encargado del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> -Establecer procedimientos y modelos de contratos y convenios para seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento y de la adopción de las medidas de seguridad</p> <p><b>DPD:</b> -Asesorar en la realización de procedimientos y modelos de contratos y convenios para seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento y de la adopción de las medidas de seguridad</p> <p><b>Responsable Funcional del Tratamiento:</b> -Velar por aplicar procedimientos y modelos de contratos y convenios para seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento y de la adopción de las medidas de seguridad</p> <p><b>Dependencia Gestora de la PD:</b> -Coordinar y difundir procedimientos y modelos de contratos y convenios para seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento y de la adopción de las medidas de seguridad.</p> <p><b>Encargado Tratamiento:</b> -Cumplir con los contratos y convenios de encargo de tratamiento de datos personales que se aplique.</p> <p><b>Usuarios:</b> -Cumplir con procedimientos y modelos de contratos y convenios para seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento y de la adopción de las medidas de seguridad</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
241	<p>DIP_AYT-Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado de tratamiento.</p> <p>Descripción Medida de seguridad</p> <p>Redactar modelos de contratos para el tratamiento de datos personales por terceros y vigilar que se apliquen en los procesos de contratación, y las actividades de subcontratistas.</p> <p>Normativa a la que afecta</p> <p>Artículo 28 RGPD - Encargado del tratamiento Artículo 33. LOPDGDD- Encargado del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Establecer modelos de contratos para el tratamiento de datos personales por terceros y vigilar que se apliquen en los procesos de contratación, y las actividades de subcontratistas.</p> <p>DPD: - Asesorar en la realización de modelos de contratos para el tratamiento de datos personales por terceros y vigilar que se apliquen en los procesos de contratación, y las actividades de subcontratistas.</p> <p>Responsable Funcional del Tratamiento: - Velar por aplicar procedimientos y modelos de contratos para el tratamiento de datos personales por terceros y vigilar que se apliquen en los procesos de contratación, y las actividades de subcontratistas.</p> <p>Dependencia Gestora de la PD: - Coordinar y difundir procedimientos y modelos de contratos para el tratamiento de datos personales por terceros y vigilar que se apliquen en los procesos de contratación, y las actividades de subcontratistas.</p> <p>Encargado Tratamiento: - Cumplir con los contratos y convenios de encargo de tratamiento de datos personales que se aplique.</p> <p>Usuarios: - Cumplir con procedimientos y modelos de contratos para el tratamiento de datos personales por terceros y vigilar que se apliquen en los procesos de contratación, y las actividades de subcontratistas.</p>	L1/L2
242	<p>DIP_AYT-Definir acuerdos de nivel de servicio que garanticen el correcto cumplimiento de las instrucciones del responsable y la adopción de las medidas de seguridad adecuadas</p> <p>Descripción Medida de seguridad</p> <p>Aprobar modelos de Acuerdos de Nivel de Servicios, y vigilar que se aplican en los procesos de contratación.</p> <p>Normativa a la que afecta</p> <p>Artículo 28 RGPD - Encargado del tratamiento Artículo 33. LOPDGDD- Encargado del tratamiento. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: DPD: Responsable Funcional del Tratamiento: Dependencia Gestora de la PD: Encargado Tratamiento: Usuarios:</p>	L1/L2
243	<p>DIP_AYT-Incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados. Y Definir los procedimientos operativos para que esta comunicación se lleve a cabo de forma ágil y eficiente.</p> <p>Descripción Medida de seguridad</p> <p>Vigilar en los procesos de contratación que se incluye la obligación de comunicar las peticiones de ejercicio de derechos, así como definir los procedimientos para que se realice de forma ágil y eficiente.</p> <p>Normativa a la que afecta</p> <p>Artículo 28 RGPD - Encargado del tratamiento Artículo 33. LOPDGDD- Encargado del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: -Establecer procedimientos y modelos de contratos y convenios para incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados.</p> <p>DPD: -Asesorar en la realización de procedimientos y modelos de contratos y convenios para incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados.</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
243	<p>DIP_AYT-Incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados. Y Definir los procedimientos operativos para que esta comunicación se lleve a cabo de forma ágil y eficiente.</p> <p>Descripción Medida de seguridad</p> <p>Vigilar en los procesos de contratación que se incluye la obligación de comunicar las peticiones de ejercicio de derechos, así como definir los procedimientos para que se realice de forma ágil y eficiente.</p> <p>Normativa a la que afecta</p> <p>Artículo 28 RGPD - Encargado del tratamiento Artículo 33. LOPDGDD- Encargado del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Funcional del Tratamiento: -Velar por aplicar procedimientos y modelos de contratos y convenios para incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados. Dependencia Gestora de la PD: -Coordinar y difundir procedimientos y modelos de contratos y convenios para incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados. Encargado Tratamiento: -Cumplir con los contratos y convenios de encargo de tratamiento de datos personales que se aplique. Usuarios: -Cumplir con procedimientos y modelos de contratos y convenios para seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento y de la adopción de las medidas de seguridad</p>	L1/L2
244	<p>DIP_AYT-Incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio. Y Establecer medidas técnicas y organizativas que garanticen la portabilidad</p> <p>Descripción Medida de seguridad</p> <p>Vigilar que se establecen en los pliegos de contratación la obligación de la portabilidad de la información.</p> <p>Normativa a la que afecta</p> <p>Artículo 28 RGPD - Encargado del tratamiento Artículo 33. LOPDGDD- Encargado del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: -Establecer procedimientos y modelos de contratos y convenios para incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio. Y Establecer medidas técnicas y organizativas que garanticen la portabilidad DPD: -Asesorar en la realización de procedimientos y modelos de contratos y convenios para incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio. Y Establecer medidas técnicas y organizativas que garanticen la portabilidad. Responsable Funcional del Tratamiento: -Velar por aplicar procedimientos y modelos de contratos y convenios para incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio. Y Establecer medidas técnicas y organizativas que garanticen la portabilidad. Dependencia Gestora de la PD: -Coordinar y difundir procedimientos y modelos de contratos y convenios para incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio. Y Establecer medidas técnicas y organizativas que garanticen la portabilidad. Encargado Tratamiento: -Cumplir con los contratos y convenios de encargo de tratamiento de datos personales que se aplique. Usuarios: -Cumplir con procedimientos y modelos de contratos y convenios para seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento y de la adopción de las medidas de seguridad</p>	L1/L2

### AYTO-10-Derechos de los Interesados

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
--------	---------------------	-------------------

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
245	<p>DIP_AYT-Implantar sistemas transparentes que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos</p> <p><b>Descripción Medida de seguridad</b></p> <p>Utilizar cláusulas de Información en formularios de recogida que informen sobre los derechos de los afectados y como ejercerlos. Utilizar carteles de información que informe y permita con código QR acceder a la información de como ejercer los derechos sobre protección de datos. Y establecer vías de acceso electrónico para acceso de forma segura a la información de datos personales por los interesados.</p> <p><b>Normativa a la que afecta</b></p> <p>CAPÍTULO III - RGPD - Derechos del interesado Capítulo II. LOPDGDD - Ejercicio de los derechos En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> - Implantar sistemas transparentes que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos DPD: - Asesorar para implantar sistemas transparentes que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos <b>Responsable Funcional del Tratamiento:</b> - Velar por cumplimiento de sistemas transparentes que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos implantados por el responsable <b>Dependencia Gestora de la PD:</b> - Coordinar y difundir la Implantación de sistemas transparentes que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos <b>Encargado Tratamiento:</b> - Aplicar los sistemas transparentes que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos que implante el Responsable. <b>Usuarios:</b> - Aplicar los sistemas transparentes que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos que implante el Responsable.</p>	L1/L2
246	<p>DIP_AYT-Formar a todo personal para que conozca qué ha de hacer si recibe una petición de derecho de los interesados o ha de informar a los afectados sobre cómo ejercerla.</p> <p><b>Descripción Medida de seguridad</b></p> <p>Realizar cursos de formación y jornadas de concienciación sobre el ejercicio de derecho de los interesados.</p> <p><b>Normativa a la que afecta</b></p> <p>CAPÍTULO III - RGPD - Derechos del interesado Capítulo II. LOPDGDD - Ejercicio de los derechos En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> - Realizar cursos de formación y jornadas de concienciación sobre el ejercicio de derecho de los interesados. DPD: - Asesorar en cursos de formación y jornadas de concienciación sobre el ejercicio de derecho de los interesados. <b>Responsable Funcional del Tratamiento:</b> - Colaborar en cursos de formación y jornadas de concienciación sobre el ejercicio de derecho de los interesados. <b>Dependencia Gestora de la PD:</b> - Coordinar y difundir cursos de formación y jornadas de concienciación sobre el ejercicio de derecho de los interesados. <b>Encargado Tratamiento:</b> - Realizar cursos de formación y jornadas de concienciación sobre el ejercicio de derecho de los interesados entre su personal. <b>Usuarios:</b> - Asistir a los cursos de formación y jornadas de concienciación sobre el ejercicio de derecho de los interesados.</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
247	<p>DIP_AYT-Definir qué personas o departamentos se ocuparán de gestionar los derechos de los interesados y atenderlos adecuadamente</p> <p>Descripción Medida de seguridad</p> <p>Establecer la Dependencia y Responsables que se ocuparán de gestionar los derechos de los interesados y atenderlos adecuadamente</p> <p>Normativa a la que afecta</p> <p>CAPÍTULO III - RGPD - Derechos del interesado Capítulo II. LOPDGDD - Ejercicio de los derechos En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Establecer la Dependencia y Responsables que se ocuparán de gestionar los derechos de los interesados y atenderlos adecuadamente DPD: - Asesorar a las Dependencia y Responsables que se ocuparán de gestionar los derechos de los interesados y atenderlos adecuadamente. Responsable Funcional del Tratamiento: - Contactar con Dependencia y Responsables que se ocuparán de gestionar los derechos de los interesados y atenderlos adecuadamente Dependencia Gestora de la PD: - Coordinar con Dependencia y Responsables que se ocuparán de gestionar los derechos de los interesados y atenderlos adecuadamente Encargado Tratamiento: - Colaborar con Dependencia y Responsables que se ocuparán de gestionar los derechos de los interesados y atenderlos adecuadamente Usuarios: - Colaborar con Dependencia y Responsables que se ocuparán de gestionar los derechos de los interesados y atenderlos adecuadamente</p>	L1/L2
248	<p>DIP_AYT-Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados</p> <p>Descripción Medida de seguridad</p> <p>Establecer los procedimiento y protocolos para que todo el personal conozca cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados</p> <p>Normativa a la que afecta</p> <p>CAPÍTULO III - RGPD - Derechos del interesado Capítulo II. LOPDGDD - Ejercicio de los derechos En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Establecer los procedimiento y protocolos para que todo el personal conozca cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados DPD: - Asesorar sobre los procedimiento y protocolos para que todo el personal conozca cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados Responsable Funcional del Tratamiento: - Difundir entre su personal los procedimiento y protocolos para que todo el personal conozca cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados Dependencia Gestora de la PD: - Coordinar y difundir los procedimiento y protocolos para que todo el personal conozca cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados Encargado Tratamiento: - Cumplir con los procedimiento y protocolos para que todo el personal conozca cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados que implante el Responsable Usuarios: - Conocer y aplicar los procedimientos de cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados que implante el Responsable</p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
249	<p>DIP_AYT-Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.</p> <p>Descripción Medida de seguridad</p> <p>Establecer los procedimientos para la gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.</p> <p>Normativa a la que afecta</p> <p>CAPÍTULO III - RGPD - Derechos del interesado Capítulo II. LOPDGDD - Ejercicio de los derechos En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento:</p> <ul style="list-style-type: none"> <li>- Establecer los procedimientos para la gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.</li> </ul> <p>DPD:</p> <ul style="list-style-type: none"> <li>- Asesorar en establecer los procedimientos para la gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.</li> </ul> <p>Responsable Funcional del Tratamiento:</p> <ul style="list-style-type: none"> <li>- Velar por cumplimiento de los procedimientos para la gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.</li> </ul> <p>Dependencia Gestora de la PD:</p> <ul style="list-style-type: none"> <li>- Coordinar y difundir los procedimientos para la gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.</li> </ul> <p>Encargado Tratamiento:</p> <ul style="list-style-type: none"> <li>- Cumplir con los procedimientos para la gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.</li> </ul> <p>Usuarios:</p> <ul style="list-style-type: none"> <li>- Cumplir con los procedimientos para la gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.</li> </ul>	L1/L2

### AYTO-11-Registro y notificación de incidentes y violaciones de seguridad

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
267	<p>DIP_AYT- Establecer procedimiento y medidas necesarias para registro de incidencias y violaciones de seguridad y en su caso notificación a órgano de control correspondiente.</p> <p>Descripción Medida de seguridad</p> <p>Elaborar los procedimiento y medidas necesarias para registro de incidencias y violaciones de seguridad y en su caso notificación a órgano de control correspondiente.</p> <p>Normativa a la que afecta</p> <p>Artículo 33 RGPD - Notificación de una violación de la seguridad de los datos personales a la autoridad de control Artículo 34 RGPD - Comunicación de una violación de la seguridad de los datos personales al interesado En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento:</p> <ul style="list-style-type: none"> <li>- Elaborar los procedimiento y medidas necesarias para registro de incidencias y violaciones de seguridad y en su caso notificación a órgano de control correspondiente.</li> </ul> <p>DPD:</p> <ul style="list-style-type: none"> <li>- Asesorar en elaborar los procedimiento y medidas necesarias para registro de incidencias y violaciones de seguridad y en su caso notificación a órgano de control correspondiente.</li> </ul> <p>Responsable Funcional del Tratamiento:</p> <ul style="list-style-type: none"> <li>- Velar por cumplimiento de los procedimiento y medidas necesarias para registro de incidencias y violaciones de seguridad y en su caso notificación a órgano de control correspondiente.</li> </ul> <p>Dependencia Gestora de la PD:</p> <ul style="list-style-type: none"> <li>- Coordinar y difundir los procedimiento y medidas necesarias para registro de incidencias y violaciones de seguridad y en su caso notificación a órgano de control correspondiente.</li> </ul> <p>Encargado Tratamiento:</p> <ul style="list-style-type: none"> <li>- Cumplir los procedimiento y medidas necesarias para registro de incidencias y violaciones de seguridad y en su caso notificación a órgano de control correspondiente, que apruebe el Responsable.</li> </ul> <p>Usuarios:</p> <ul style="list-style-type: none"> <li>- Cumplir los procedimiento y medidas necesarias para registro de incidencias y violaciones de seguridad y en su caso notificación a órgano de control correspondiente, que apruebe el Responsable.</li> </ul>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
<b>AMENAZAS - USO SISTEMA DE INFORMACION</b>		

### AYTO-12-Seguridad. Medidas del ENS

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
250	DIP_AYT-Implantar las Medidas de seguridad del Esquema Nacional de Seguridad (ENS)	L1/L2
<p><b>Descripción Medida de seguridad</b></p> <p>Implantar las Medidas de Seguridad del Nivel correspondiente a la Categorización ENS de las Actividades de Tratamiento de datos personales. Ver medidas a implantar en siguiente enlace: <a href="https://app.dipalme.org/proDatos/downloadDocAlfresco?id=workspace://SpacesStore/a316d599-79c1-480d-9771-f5e70b9bd26f;1.0">https://app.dipalme.org/proDatos/downloadDocAlfresco?id=workspace://SpacesStore/a316d599-79c1-480d-9771-f5e70b9bd26f;1.0</a></p> <p><b>Normativa a la que afecta</b></p> <p>Artículo 32 - RGPD - Seguridad del tratamiento Disposición adicional primera. LOPDGDD - Medidas de seguridad en el ámbito del sector público. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional. En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>Responsable Tratamiento: - Aprobar Plan de Adecuación al ENS DPD: - Velar por el cumplimiento de las medidas del ENS a la Protección de Datos Personales Responsable Funcional del Tratamiento: - Velar por que el personal a su cargo cumplan con las medidas de seguridad del ENS. Dependencia Gestora de la PD: - Coordinar la implantación de las medidas de seguridad del ENS. Encargado Tratamiento: - Cumplir con las medidas de seguridad del ENS que se implanten Usuarios: - Cumplir con las medidas de seguridad del ENS que se implanten</p>		

### AMENAZAS - TRATAMIENTO DATOS EN PAPEL

#### AYTO-15-Seguridad - Medidas para tratamiento y gestión en Papel

Id.Med	Medida de Seguridad	Madurez (Act/Obj)
251	DIP_AYT-Definir los procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.)	L1/L2
<p><b>Descripción Medida de seguridad</b></p> <p>Establecer los procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.)</p> <p><b>Normativa a la que afecta</b></p> <p>Artículo 32 - RGPD - Seguridad del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>Responsable Tratamiento: - Establecer los procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.) DPD: - Asesorar en establecer los procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.) Responsable Funcional del Tratamiento: - Velar por el cumplimiento de los procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.) Dependencia Gestora de la PD: - Coordinar y difundir procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.) Encargado Tratamiento: - Cumplir con procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de</p>		

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
251	<p>DIP_AYT-Definir los procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.)</p> <p><b>Descripción Medida de seguridad</b></p> <p>Establecer los procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.)</p> <p><b>Normativa a la que afecta</b></p> <p>Artículo 32 - RGPD - Seguridad del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p>datos personales (Informar, Minimización de datos, etc.) Usuarios: - Cumplir con procedimientos y Adecuar los formularios de recogida en Papel para cumplir con los principios adecuados del tratamiento de datos personales (Informar, Minimización de datos, etc.)</p>	L1/L2
252	<p>DIP_AYT-Utilizar archivadores o salas de archivo con llaves o sistemas de cerrado, así como de registro del personal que accede a los documentos en papel.</p> <p><b>Descripción Medida de seguridad</b></p> <p>Establecer procedimientos y controles sobre el uso de archivadores o salas de archivo con llaves o sistemas de cerrado, así como de registro del personal que accede a los documentos en papel.</p> <p><b>Normativa a la que afecta</b></p> <p>Artículo 32 - RGPD - Seguridad del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> - Establecer procedimientos y controles sobre el uso de archivadores o salas de archivo con llaves o sistemas de cerrado, así como de registro del personal que accede a los documentos en papel. DPD: - Asesorar en establecer procedimientos y controles sobre el uso de archivadores o salas de archivo con llaves o sistemas de cerrado, así como de registro del personal que accede a los documentos en papel. <b>Responsable Funcional del Tratamiento:</b> - Velar por el cumplimiento de los procedimientos y controles sobre el uso de archivadores o salas de archivo con llaves o sistemas de cerrado, así como de registro del personal que accede a los documentos en papel. <b>Dependencia Gestora de la PD:</b> - Coordinar y difundir los procedimientos y controles sobre el uso de archivadores o salas de archivo con llaves o sistemas de cerrado, así como de registro del personal que accede a los documentos en papel. <b>Encargado Tratamiento:</b> - Cumplir con los procedimientos y controles sobre el uso de archivadores o salas de archivo con llaves o sistemas de cerrado, así como de registro del personal que accede a los documentos en papel. <b>Usuarios:</b> - Cumplir con los procedimientos y controles sobre el uso de archivadores o salas de archivo con llaves o sistemas de cerrado, así como de registro del personal que accede a los documentos en papel.</p>	L1/L2
253	<p>DIP_AYT-Política de mesas Limpias, y cajones en las mesas con llaves</p> <p><b>Descripción Medida de seguridad</b></p> <p>Elaborar Política de mesas Limpias, y cajones en las mesas con llaves</p> <p><b>Normativa a la que afecta</b></p> <p>Artículo 32 - RGPD - Seguridad del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p><b>Actuaciones de cada Rol</b></p> <p><b>Responsable Tratamiento:</b> - Elaborar Política de mesas Limpias, y cajones en las mesas con llaves DPD: -Asesorar en elaborar Política de mesas Limpias, y cajones en las mesas con llaves <b>Responsable Funcional del Tratamiento:</b> -Velar por el cumplimiento de Política de mesas Limpias, y cajones en las mesas con llaves que apruebe el Responsables <b>Dependencia Gestora de la PD:</b> - Coordinar y difundir Política de mesas Limpias, y cajones en las mesas con llaves que se apruebe. <b>Encargado Tratamiento:</b> - Cumplir con la Política de mesas Limpias, y cajones en las mesas con llaves que apruebe el responsable <b>Usuarios:</b></p>	L1/L2

# MEDIDAS DE SEGURIDAD

## 4057 - AYUNTAMIENTO DE LAUJAR DE ANDARAX

Id.Med	Medida de Seguridad / Descripción Medida de seguridad	Madurez (Act/Obj)
253	DIP_AYT-Política de mesas Limpias, y cajones en las mesas con llaves	L1/L2
	<p>Descripción Medida de seguridad</p> <p>Elaborar Política de mesas Limpias, y cajones en las mesas con llaves</p> <p>Normativa a la que afecta</p> <p>Artículo 32 - RGPD - Seguridad del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>- Cumplir con la Política de mesas Limpias, y cajones en las mesas con llaves que apruebe el responsable</p>	
254	DIP_AYT-Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias.	L1/L2
	<p>Descripción Medida de seguridad</p> <p>Elaborar los Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias.</p> <p>Normativa a la que afecta</p> <p>Artículo 32 - RGPD - Seguridad del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Elaborar los Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias.</p> <p>DPD: - Asesora en elaborar los Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias.</p> <p>Responsable Funcional del Tratamiento: - Velar por cumplimiento de los Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias.</p> <p>Dependencia Gestora de la PD: - Coordinar y difundir los Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias.</p> <p>Encargado Tratamiento: - Cumplir con los Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias, que apruebe el Responsable.</p> <p>Usuarios: - Cumplir con los Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias, que apruebe el Responsable.</p>	
255	DIP_AYT-Definir los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales.	L1/L2
	<p>Descripción Medida de seguridad</p> <p>Elaborar los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales.</p> <p>Normativa a la que afecta</p> <p>Artículo 32 - RGPD - Seguridad del tratamiento En general al cumplimiento de toda la Normativa de protección de datos personales y de la Seguridad de la Información.</p> <p>Actuaciones de cada Rol</p> <p>Responsable Tratamiento: - Elaborar los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales.</p> <p>DPD: - Asesorar en elaborar los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales.</p> <p>Responsable Funcional del Tratamiento: - Velar por cumplimiento de los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales.</p> <p>Dependencia Gestora de la PD: - Coordinar y difundir los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales.</p> <p>Encargado Tratamiento: - Cumplir con los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales, que apruebe el responsable.</p> <p>Usuarios: - Cumplir con los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales, que apruebe el responsable.</p>	