

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

08/02/2021

DIPUTACIÓN PROVINCIAL DE ALMERÍA
AREA DE RECURSOS HUMANOS Y RÉGIMEN
SERVICIO DE ORGANIZACIÓN E INFORMACIÓN





00 - Índice 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 para la SERVICIO DE ORGANIZACIÓN E INFORMACIÓN, en adelante la Dependencia, 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 Riesgo, para SERVICIO DE ORGANIZACIÓN E INFORMACIÓN 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 DIPUTACIÓN PROVINCIAL DE ALMERÍA 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 (proDatos) 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, para ello se está contando con la colaboración de las empresas externas que está llevando un proyecto de adecuación al RGPD para Diputación y otra para 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 Dependencia, 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 SERVICIO DE ORGANIZACIÓN E INFORMACIÓN, 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 Adecuación 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 Adecuación 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 segun 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 Evaluación 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, Evaluación 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).Evaluación 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 Evaluación 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 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 especies 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 evaluación 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.

DIPUTACIÓN PROVINCIAL DE ALMERÍA como responsable del Tratamiento de Datos Personales, y SERVICIO DE ORGANIZACIÓN E INFORMACIÓN como responsable delegado, implementaran las Medidas de Control necesarias, y para ello realizara una gestion de dichas medidas por Dependencias, donde cada dependencia determinara el nivel de madurez de las Medidas que se adopten, y los Responsables de dichas Dependencias velarean 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 el [Anexo I-Valoracion Med.Seguridad que se aplicaran a las Actividades de Tratamiento y Madurez Actual](#).

La Categoría Global de las valoración de las Medidas de Seguridad a aplicar a las Actividades de Tratamiento de Datos Personales es de:.



Las Medidas de Seguridad a aplicar tendrá un Nivel global de implantación =
BAJA - Nivel de Implantación L2 (Repetible pero intuitivo)

La valoración para la Integridad, Disponibilidad y Confidencialidad se realizará conforme a lo dispuesto en el ENS, y se realizará en el Plan de Adecuación al ENS de la Entidad, donde también se realizará 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 SERVICIO DE ORGANIZACIÓN E INFORMACIÓN, un Análisis de la Necesidad de Realizar una EIPD en una muestra de las Actividades de Tratamiento de Datos Personales más relevantes, siendo:

-Número de Actividades de Tratamiento de Datos Personales con Análisis de Necesidad de realizar una EIPD = 5 de un total de 6

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 SERVICIO DE ORGANIZACIÓN E INFORMACIÓN ha sido el catálogo de la herramienta de gestión de datos personales de Diputación proDatos:

"DIPU - Catálogo de Amenazas para aplicar a Diputación más reducido que el de la AEPD".

- [Ver Listado del Catálogo](#) -

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.

Los valores de (probabilidad x impacto) que el catálogo propone por defecto, deben ser modificados por valores que se obtendrán de las entrevistas que se realicen con los responsables de los tratamientos 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 evaluación de los riesgos serán los descritos en los apartados anteriores.



La Evaluación 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 SERVICIO DE ORGANIZACIÓN E INFORMACIÓN las actividades de tratamiento de la muestran son:

- SERVICIO DE ORGANIZACIÓN E INFORMACIÓN
- SUGERENCIAS Y RECLAMACIONES (Riesgo Potencial=3)
- GESTIÓN DE INFORMACIÓN Y CONSULTAS (Riesgo Potencial=3)
- PRÁCTICAS DE ALUMNOS (Riesgo Potencial=3)
- ATENCIÓN DERECHOS DE TRANSPARENCIA Y PROTECCIÓN DE DATOS (Riesgo Potencial=3)
- GESTIÓN DE ACREDITACIONES PARA REPRESENTACIÓN ANTE OTRAS ADMINISTRACIONES DE EMPLEADOS DE DIPUTACIÓN Y DE CERTIFICADOS AP (Riesgo Potencial=3)
- GESTIÓN DE REUNIONES DE TRABAJO (Riesgo Potencial=3)

Los datos para la Dependencia son los siguientes:

- - Actividades de Tratamiento de Datos Personales valorados: **6**
- - Numero de Amenazas valoradas: **37**
- - Riesgo Potencial: **3**

Puede ver mas informacion sobre el Analisis de riesgos de DIPUTACIÓN PROVINCIAL DE ALMERÍA y de SERVICIO DE ORGANIZACIÓN E INFORMACIÓN 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 indicados en el [Anexo I-Valoracion Med.Seguridad que se aplicaran a las Actividades de Tratamiento y Madurez Actual](#).

En el - [Anexo II - Medidas de Seguridad](#)- 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.



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 SERVICIO DE ORGANIZACIÓN E INFORMACIÓN 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 dimension 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 llegará 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: **6**
- - Numero de Amenas valoradas: **37**
- - Numero de Medidas de Seguridad propuestas: **54**
- - Porcentaje de nivel de implantacion de las Medidas de Seguridad: **10**

Ver mas informacion sobre el Analisis de riesgos de DIPUTACIÓN PROVINCIAL DE ALMERÍA y SERVICIO DE ORGANIZACIÓN E INFORMACIÓN en el siguiente enlace (Ver informacion Analisis de Riesgos):
Ver mas informacion sobre los Niveles de madurez de las Medidas de Seguridad de DIPUTACIÓN PROVINCIAL DE ALMERÍA y de SERVICIO DE ORGANIZACIÓN E INFORMACIÓN en el siguiente enlace (Ver informacion 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 Analisis de Riesgos contenido en el presente documento.



13 - ANEXOS.

- ANEXO I.- Valoración Med.Seguridad que se aplicaran a las Actividades de Tratamiento y Madurez Actual.

- ANEXO II.- Medidas de Seguridad.

- ANEXO III .- 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>

DIPUTACIÓN PROVINCIAL DE ALMERÍA
SERVICIO DE ORGANIZACIÓN E INFORMACIÓN



Anexo I -Valoracion Medidas de Seguridad que se aplicaran a las
Actividades de Tratamiento y madurez actual.

| Id | Titulo Actividad de Tratamiento | Nivel Segu. | Madurez Actual |
|------|---|-------------|----------------|
| 115 | ATENCIÓN DERECHOS DE TRANSPARENCIA Y PROTECCIÓN DE DATOS | B | L2 |
| 403 | GESTIÓN DE ACREDITACIONES PARA REPRESENTACIÓN ANTE OTRAS ADMINISTRACIONES DE EMPLEADOS DE DIPUTACIÓN Y DE CERTIFICADOS AP | B | L1 |
| 104 | GESTIÓN DE INFORMACIÓN Y CONSULTAS | B | L1 |
| 1738 | GESTIÓN DE REUNIONES DE TRABAJO | B | L1 |
| 105 | PRÁCTICAS DE ALUMNOS | B | L2 |
| 9 | SUGERENCIAS Y RECLAMACIONES | B | L1 |

MEDIDAS DE SEGURIDAD

400000 - DIPUTACIÓN PROVINCIAL DE ALMERÍA 71 - SERVICIO DE ORGANIZACIÓN E INFORMACIÓN

AMENAZAS - CUMPLIMIENTO NORMATIVO

DIPU-01-Generales

| 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 |
| 200 | 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 |
| 201 | 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 |
| 202 | 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 |
| 203 | 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 |
| 204 | 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 |
| 199 | DIP_AYT-Formación apropiada del personal sobre protección de datos , seguridad y uso adecuado de las TIC. | L1/L2 |

DIPU-02-Legitimación y cesión

| Id.Med | Medida de Seguridad / Descripción Medida de seguridad | Madurez (Act/Obj) |
|--------|--|-------------------|
| 206 | DIP_AYT-Usar datos disociados o pseudónimos siempre que sea posible y no implique un esfuerzo desproporcionado | L1/L2 |
| 207 | DIP_AYT-Evitar el uso de datos biométricos salvo que resulte imprescindible o esté absolutamente justificada | L1/L2 |
| 210 | DIP_AYT-Asegurarse de que no existen otras causas de legitimación más adecuadas | L1/L2 |
| 211 | 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 |
| 212 | 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 |
| 213 | 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 |
| 214 | DIP_AYT-Exigir garantías de que los datos personales provenientes de terceros se han obtenido y cedido lealmente. | L1/L2 |
| 209 | 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 |
| 215 | 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 |

MEDIDAS DE SEGURIDAD

400000 - DIPUTACIÓN PROVINCIAL DE ALMERÍA 71 - SERVICIO DE ORGANIZACIÓN E INFORMACIÓN

| Id.Med | Medida de Seguridad / Descripción Medida de seguridad | Madurez (Act/Obj) |
|--------|--|-------------------|
| 215 | 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 |
| 216 | 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 |
| 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 |
| 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 |

DIPU-04-Notificación y Registro de las Actividades

| 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 y de la necesidad de registrar la creación, modificación o cancelación de actividades de tratamiento | L1/L2 |

DIPU-05-Transparencia de los tratamientos

| Id.Med | Medida de Seguridad / Descripción 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 |
| 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 ofrezca 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 |
| 224 | 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 |
| 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 |

DIPU-06-Calidad de los datos

| Id.Med | Medida de Seguridad / Descripción 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 |
| 227 | 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 |
| 228 | DIP_AYT-Siempre que sea posible, utilizar datos anónimos, disociados o pseudónimos. Y garantizar que se apliquen las medidas de seguridad adecuadas | L1/L2 |
| 229 | 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 |
| 230 | 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 |
| 231 | DIP_AYT-Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer. | L1/L2 |

MEDIDAS DE SEGURIDAD

400000 - DIPUTACIÓN PROVINCIAL DE ALMERÍA 71 - SERVICIO DE ORGANIZACIÓN E INFORMACIÓN

| Id.Med | Medida de Seguridad / Descripción Medida de seguridad | Madurez (Act/Obj) |
|--------|---|-------------------|
| 231 | DIP_AYT-Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer. | L1/L2 |

| | | |
|-----|--|-------|
| 232 | 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 |
|-----|--|-------|

DIPU-07-Categorías Especiales de Datos

| 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 |

DIPU-08-Deber de secreto

| Id.Med | Medida de Seguridad / Descripción 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 |
| 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 |
| 236 | DIP_AYT-Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales | L1/L2 |
| 237 | DIP_AYT-Formación adecuada de los empleados sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información | L1/L2 |
| 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 |

DIPU-09-Tratamientos por Encargo

| Id.Med | Medida de Seguridad / Descripción Medida de seguridad | Madurez (Act/Obj) |
|--------|--|-------------------|
| 239 | 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 |
| 240 | 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 |
| 241 | 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 |
| 242 | 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 |
| 243 | 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 |
| 244 | 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 |

DIPU-10-Derechos de los Interesados

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

MEDIDAS DE SEGURIDAD

400000 - DIPUTACIÓN PROVINCIAL DE ALMERÍA 71 - SERVICIO DE ORGANIZACIÓN E INFORMACIÓN

| Id.Med | Medida de Seguridad / Descripción Medida de seguridad | Madurez (Act/Obj) |
|--------|---|-------------------|
| 245 | 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 |
| 246 | 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 |
| 247 | DIP_AYT-Definir qué personas o departamentos se ocuparán de gestionar los derechos de los interesados y atenderlos adecuadamente | L1/L2 |
| 248 | 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 |
| 249 | 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 |

DIPU-11-Registro y notificación de incidentes y violaciones de seguridad

| Id.Med | Medida de Seguridad / Descripción Medida de seguridad | Madurez (Act/Obj) |
|--------|---|-------------------|
| 267 | 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

DIPU-12-Seguridad. Medidas del ENS

| Id.Med | Medida de Seguridad / Descripción Medida de seguridad | Madurez (Act/Obj) |
|--------|--|-------------------|
| 250 | DIP_AYT-Implantar las Medidas de seguridad del Esquema Nacional de Seguridad (ENS) | L1/L2 |

AMENAZAS - TRATAMIENTO DATOS EN PAPEL

DIPU-15-Seguridad - Medidas para tratamiento y gestión en Papel

| Id.Med | Medida de Seguridad / Descripción 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 |
| 252 | 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 |
| 253 | DIP_AYT-Política de mesas Limpias, y cajones en las mesas con llaves | L1/L2 |
| 254 | DIP_AYT-Procedimientos para el traslado de documentos en papel entre los distintos edificios y dependencias. | L1/L2 |
| 255 | DIP_AYT-Definir los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales. | L1/L2 |