Calle Navarro Rodrigo, 17
Almería - (04001) Almería
Telefono: 950211100
Email: dpd@dipalme.org
www.dipalme.org

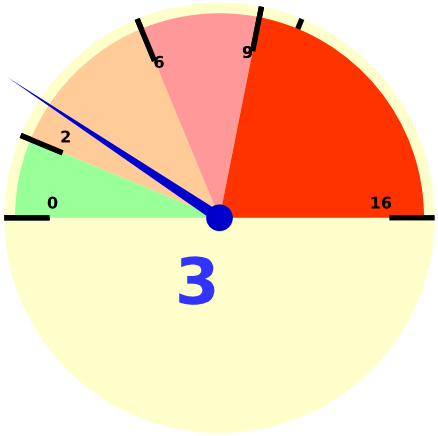
ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

400000 - DIPUTACIÓN PROVINCIAL DE ALMERÍA

10 - AREA DE DEPORTES, VIDA SALUDABLE Y JUVENTUD - SERVICIO JURÍDICO Y ADMTIVO DE DEPORTES, VIDA SALUDABLE Y JUVENTUD

NIVEL DE RIESGO

NIVEL MAXIMO DE RIESGO POTENCIAL



Tratamiento Valorados	Num.Ame	N.Ame.BAJO	N.Ame.MEDIO	N.Ame.ALTO	N.Ame.MUY ALTO
2	13	9	4	0	0

Calle Navarro Rodrigo, 17
Almería - (04001) Almería
Telefono: 950211100
Email: dpd@dipalme.org
www.dipalme.org

ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

400000 - DIPUTACIÓN PROVINCIAL DE ALMERÍA

10 - AREA DE DEPORTES, VIDA SALUDABLE Y JUVENTUD - SERVICIO

Id.Ame	Amenaza / Descripcion Amenaza	Num.Act. Tratami.	Riesgo Potencial
Id.Med	Medida de Seguridad / Descripcion Medida de seguridad		

AMENAZAS - CUMPLIMIENTO NORMATIVO

DIPU-01-Generales

101	DIPU-Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.	1	3
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. 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 .		
202	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. 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.		
103	DIPU-Poco conocimiento y concienciación del personal de la Entidad en la Protección de Datos Personales	2	2
199	DIP_AYT-Formación apropiada del personal sobre protección de datos , seguridad y uso adecuado de las TIC. 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.		

DIPU-02-Legitimacion y cesion

104	DIPU-Tratar datos personales cuando no es necesario para la finalidad perseguida	1	1
206	DIP_AYT-Usar datos disociados o pseudonimos siempre que sea posible y no implique un esfuerzo desproporcionado 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.		
207	DIP_AYT-Evitar el uso de datos biométricos salvo que resulte imprescindible o esté absolutamente justificada No se utilizaran datos biométricos, a no ser que este bien justificado su uso, y además en el caso que se traten datos biométricos se realizaran las correspondientes justificaciones, y su tratamiento deberá ser aprobada por el órgano competente (Resolución de Alcalde-Presidente)		

Diputación de Almería

Calle Navarro Rodrigo, 17
Almería - (04001) Almería
Telefono: 950211100
Email: dpd@dipalme.org
www.dipalme.org

ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

400000 - DIPUTACIÓN PROVINCIAL DE ALMERÍA

10 - AREA DE DEPORTES, VIDA SALUDABLE Y JUVENTUD - SERVICIO

Id.Ame	Amenaza / Descripcion Amenaza	Num.Act. Tratami.	Riesgo Potencial
105	DIPU-Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales	1	3

Id.Med	Medida de Seguridad / Descripcion Medida de seguridad
210	DIP_AYT-Asegurarse de que no existen otras causas de legitimación más adecuadas Los tratamiento 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 mas adecuada. Hay que tener presente que la legitimación de las Administraciones publicas es casi siempre la Obligación Legal (en este caso debe haber una norma con rango de ley que justifique el tratamiento), Interés Publico y Poder Publico (en estos caso existe una competencia que justifica su tratamiento), siendo el Consentimiento una legitimación menos empelada, así con Contratos y el Interés Legitimo. Hay que documentar bien la BAse Legitima 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.
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 Si la base legitima 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. Ejemplo en los contrato de empleados (Laborales o funcionariales), si se piden datos personales que no estén bien contemplados en el contrato, se utilizara el consentimiento, ejemplo solicitar datos de contactos de familiares, datos biometricos, etc.
212	DIP_AYT-Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas Es necesario informar y formar al personal que trata datos Personales en la solicitud de Consentimiento para tratamiento de datos personales, asi 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: https://www.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf

107	DIPU-Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros	2	1

214	DIP_AYT-Exigir garantías de que los datos personales provenientes de terceros se han obtenido y cedido lealmente. Establecer procedimientos que permitan garantizar que los datos cedidos por terceros se hacen de forma legal y cumpliendo con las normas de proteccion de datos, para ello se deben realizar en base a garantía legales, convenios, etc.. En el caso la cesión de informacion de otras Administraciones se utilizara en lo posible los sistemas de Intermediación.

DIPU-06-Calidad de los datos

118	DIPU-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	1

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 Revisar los procedimientos que actualicen datos personales para que se actualicen en lo posible de de forma automática por los Sistemas de Informacion que los usen, y si no es posible establecer los mecanismos para realizar una comunicación a otras dependencias para que actualicen

Diputación de Almería

Calle Navarro Rodrigo, 17
Almería - (04001) Almería
Telefono: 950211100
Email: dpd@dipalme.org
www.dipalme.org

ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

400000 - DIPUTACIÓN PROVINCIAL DE ALMERÍA

10 - AREA DE DEPORTES, VIDA SALUDABLE Y JUVENTUD - SERVICIO

Id.Ame	Amenaza / Descripcion Amenaza	Num.Act. Tratami.	Riesgo Potencial
	Id.Med / Medida de Seguridad / Descripcion Medida de seguridad		
119	DIPU-Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos	2	1
	228 DIP_AYT-Siempre que sea posible, utilizar datos anónimos, disociados o pseudónimos. Y garantizar que se apliquen las medidas de seguridad adecuadas 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.		
	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 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.		
121	DIPU-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	2
	232 DIP_AYT-Definir claramente los plazos de cancelación de todos los datos personales de los sistemas de información, y establecer los controles adecuados. Realizar normas y procedimientos para establecer los plazos de cancelación de los datos personales.		
	DIPU-08-Deber de secreto		
123	DIPU-Accesos no autorizados a datos personales.	2	1
	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. Formar y concienciar a las personas que tratan datos personales sobre la obligación de guardar secreto.		
	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 Establecer los procedimientos de recabar la confidencialidad y el deber de secreto a todo el personal que trate datos personales.		
	236 DIP_AYT-Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales Realizar norma y procedimiento para la destrucción de soportes desechados con datos personales.		
	AMENAZAS - TRATAMIENTO DATOS EN PAPEL		
	DIPU-15-Seguridad - Medidas para tratamiento y gestión en Papel		
134	DIPU-Recogida de datos personales en formularios en Papel sin adoptar las medidas adecuadas	2	1
	251 DIP_AYT-Definir los procedimientos y Adecuar los formularios de recogida para cumplir con los principios adecuados del tratamiento de datos personales (Deber de Informar, Minimizacion de datos, etc.) Establecer los procedimientos y Adecuar los formularios de recogida para cumplir con los principios adecuados del tratamiento de datos personales (Deber de Informar, Minimizacion de datos, etc.)		
135	DIPU-Archivo y almacenamiento de datos personales en Papel sin adoptar las medidas adecuadas	2	3

Diputación de Almería

Calle Navarro Rodrigo, 17
Almería - (04001) Almería
Telefono: 950211100
Email: dpd@dipalme.org
www.dipalme.org

ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

400000 - DIPUTACIÓN PROVINCIAL DE ALMERÍA

10 - AREA DE DEPORTES, VIDA SALUDABLE Y JUVENTUD - SERVICIO

Id.Ame	Amenaza / Descripcion Amenaza	Num.Act. Tratami.	Riesgo Potencial
	Id.Med / Medida de Seguridad / Descripcion Medida de seguridad		
	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. 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.		
	253 DIP_AYT-Política de mesas Limpias, y cajones en las mesas con llaves Elaborar Política de mesas Limpias, y cajones en las mesas con llaves		
137	DIPU-Destrucción de papel con datos personales sin adoptar las medidas adecuadas	2	2
	255 DIP_AYT-Definir los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales. Elaborar los procedimientos y normas para la destrucción de documentos en papel que contienen datos personales.		

AMENAZAS - USO SISTEMA DE INFORMACION

DIPU-12-Seguridad. Medidas del ENS

133	DIPU-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:	1	3
	250 DIP_AYT-Implantar las Medidas de seguridad del Esquema Nacional de Seguridad (ENS) 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: https://app.dipalme.org/proDatos/descargarDocAlfresco?id=workspace://SpacesStore/a316d599-79c1-480d-9771-f5e70b9bd26f;1.0		