Política de Seguridad y Privacidad de la Información

Junio de 2020

DIPUTACIÓN DE ALMERÍA

Índice

1 INTRODUCCIÓN:

La Diputación de Almería, para el cumplimiento de las competencias que tiene asignadas por ley, necesita de los sistemas TIC (Tecnologías de la Información y Comunicaciones) necesarios para prestar servicios de administración electrónica.

Los sistemas de la Diputación de Almería, deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas se requiere una estrategia que se adapte a los cambios en las condiciones del entorno, para garantizar la prestación continua de los servicios a las EE.LL. de la provincia a través de la RPC

A mayor abundamiento, en el específico marco de la administración electrónica, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las AA.PP., señala en el artículo 12.1 que *"Las Administraciones Públicas deberán garantizar que los interesados puedan relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios, así como los sistemas y aplicaciones que en cada caso se determinen"*. De conformidad con lo establecido en el artículo 13. h) de la citada Ley, quien tenga capacidad de obrar ante la Administración Pública, tiene derecho *"A la protección de los datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas"*.

Por su lado, la ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público, establece, en el artículo 156.2 que "*El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".*

Es por ello que el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) por el que se desarrolla las exigencias de seguridad de la información en el ámbito subjetivo de aplicación de las leyes 39 y 40/2015, establece en el artículo 11.1, que *"Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente..."*

Por su parte, la aplicación de la normativa sobre protección de datos de carácter personal supone para esta Diputación, tanto como responsable y como encargado de tratamiento de datos personales, la necesaria adopción de una serie de medidas de carácter técnico y organizativo tendentes a garantizar los derechos y las libertades de los titulares de dichos datos personales. Así la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, que regula las Medidas de seguridad en el ámbito del sector público, establece que "Los responsables enumerados en el artículo 77.1 de esta ley orgánica" (entre los que se encuentran las entidades que integran la Administración Local) "deberán aplicar a los tratamientos de datos

personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

La convergencia de los requisitos de seguridad sobre los sistemas de información TIC y de los reclamados por la protección de datos de carácter personal hace aconsejable no acometer acciones desagregadas, que atiendan a cada dimensión por separado, pues ello podría provocar duplicidades, antinomias, confusión y descoordinación internas, además de resultar más oneroso desde el punto de vista de la inversión de recursos humanos, económicos, técnicos y organizativos.

En este sentido, y para dar respuesta a las necesidades expuestas anteriormente, la Diputación de Almería ha decidido elaborar en una misma política los principios y directrices básicas que han de regir las actuaciones en materia de seguridad de la información y de las actividades de tratamiento de datos personales que se vean afectadas por el análisis de activos de los sistemas de información utilizados en el ejercicio de sus competencias.

Si bien, todas las actuaciones relacionadas con las actividades de tratamiento se regularan a través del RGPD y la LO 3/2018 (Tratamos de justificar la relación entre política de seguridad y protección de datos personales).

2 OBJETO:

La presente política tiene por objeto definir y regular, en el ámbito de la Diputación de Almería, la política de Seguridad y Privacidad de la información (en adelante PSPI) aplicable a los sistemas de información que intervengan en el tratamiento de la información que resulte necesaria para el ejercicio de sus competencias

La Política de Seguridad y Privacidad de la Información de la Diputación de Almería nace con la vocación de servir de modelo a las Entidades Locales de la provincia de Almería para la implantación de sus políticas de seguridad

3 DEFINICIONES:

A efectos de la presente política se entenderá por:

- Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

- Amenaza. Eventos que pueden desencadenar un incidente de seguridad en la Diputación o Entes que utilicen los sistemas de la Red Provincial, produciendo daños materiales o pérdidas inmateriales en sus activos

- Análisis de riesgos. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

- Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

- Categoría del sistema. Es un nivel, dentro de la escala Bajo Medio Alto, con lo que se califica un sistema, con el fin de seleccionar las medidas de seguridad necesarias por el mismo según el Anexo II de la ENS.

- Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

- Datos de carácter personal. Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

- Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

- Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos que le son aplicables según su naturaleza y su entorno, así como las tecnologías de la información y la comunicación utilizadas.

- Incidente de seguridad. Evento inesperado o no deseado que tiene consecuencias en detrimento de la seguridad del sistema de información.

- Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

- Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Pueden tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

- Minimización de datos. Principio por el que se deben tratar sólo los datos necesarios para la finalidad para el que se ha previsto el servicio o el procedimiento ejecutado por la Diputación o Entes que utilicen los sistemas de la Red Provincial en el ejercicio de sus funciones atribuidas por ley.

- Política de seguridad. Conjunto de directrices plasmadas en un documento escrito que rigen la forma en que la Diputación y los Entes que utilizan los sistemas de la Red Provincial gestionan y protegen la información y los servicios que lo utilizan.

- Responsable de Seguridad. Persona encargada de velar por la seguridad de la información de la Diputación y los Entes que utilizan los sistemas de la Red Provincial.

- Responsable de la Información. Persona que tiene la potestad de establecer los requerimientos de una información en materia de seguridad.

- Responsable del Servicio. Persona que tiene la potestad de establecer los requerimientos de un servicio en materia de seguridad de la información.

- Responsable del Sistema. Persona que se encarga de la explotación del sistema de la información desde la perspectiva de la seguridad de la información.

- Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización de la que es responsable la Diputación y los Entes que utilizan los sistemas de la Red Provincial.

- Riesgo residual. Es el riesgo resultante de la aplicación de contramedidas y, por tanto, constituye el riesgo a asumir de forma consciente.

- Seguridad de la información. Es la protección de la información y los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas, con el fin de proporcionar confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

- Seguridad desde el diseño. Principio por el cual los aspectos de seguridad se consideran en el momento de definición del servicio prestado o procedimiento ejecutado por la Diputación y los Entes que usan los sistemas de la Red Provincial en el ejercicio de sus funciones, así como de los sistemas que lo apoyarán.

- Seguridad por defecto. Principio por el cual los sistemas de información deben ser sometidos a un proceso de análisis y configuración inicial, previo a su puesta en producción, por el que sean considerados seguros sin que cuenten con errores conocidos y garanticen que sólo el personal autorizado podrá acceder para realizar las funciones que tengan atribuidas, así como darán respuesta a las funcionalidades estrictamente necesarias para la prestación de los servicios y el ejercicio de las funciones de la Diputación y los Entes que usan los sistemas de la Red Provincial.

- Sistema de información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

- Sistema de información TIC. Sistema de información que emplea tecnologías de la información y de las comunicaciones para conseguir su finalidad.
- Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad y se pueden identificar y reconstruir adecuadamente las acciones que se han realizado sobre la información.
- Usuario de la Red Provincial, Cualquier entidad, persona física o titular del dispositivo electrónico que se conecte a la misma o utilice cualesquiera de sus dispositivos.
- Vulnerabilidad. Una debilidad del sistema de información que puede ser aprovechada por una amenaza y mitigada mediante la aplicación de medidas de seguridad.

4 ALCANCE:

Esta Política se aplica a cualquier elemento o activo del sistema de información:

- Elementos Software. Aplicaciones, bases de datos, etc.
- Elementos Hardware. Servidores, PCs de usuarios, portátiles, dispositivos de red, dispositivos perimetrales, dispositivos de seguridad, etc.
- Soportes de Información. Cualquier soporte donde se almacene información, ya sea en formato papel o electrónico
- Personas. Personas que acceden a los sistemas de información: usuarios internos, usuarios externos, personal informático, proveedores, otros terceros, etc.
- Redes de comunicaciones. LAN, conectividad a Internet desde la DMZ, Intranet Provincial, VPN para conexiones remotas, etc.
- Instalaciones. Salas donde se almacenan las copias de seguridad o material informático, salas donde se ubican los servidores, etc.

Por otro lado, debe quedar claro que la Política afecta a todos los sistemas que traten información, independientemente que dicha información sean datos personales o no, así como a la información vinculada a la ejecución del procedimiento administrativo y cualquier otra relacionada con las actividades realizadas por la Diputación y los Entes que usan los sistemas de la Red Provincial en el ejercicio de sus funciones.

Adicionalmente, la Diputación aplicará la presente Política en el marco de sus relaciones con las entidades locales de la provincia que utilizan los sistemas de la Red Provincial de Comunicaciones como proveedora y gestora de la red en modo nube respetando en cualquier caso la autonomía de aquéllas y sus facultades de gestión y control sobre la información y los servicios que les son propios. En este sentido, la Diputación promoverá acuerdos con dichas entidades locales para el intercambio de la información necesaria que facilite las garantías y el cumplimiento legal en materia de seguridad y de protección de datos personales en los sistemas de información afectados.

5 AMBITO SUBJETIVO DE APLICACION:

Las presentes disposiciones son de aplicación a todos los departamentos y unidades de la Diputación de Almería, a los entes u organismos públicos vinculados o dependientes de la Diputación de Almería.

Las EE.LL. y sus organismos dependientes que utilicen los sistemas de la Red Provincial de Comunicaciones, podrán adherirse a la presente política o adoptar su propia política de seguridad y de protección de datos de carácter personal, siempre que se adecue a las presentes prescripciones y normas e instrucciones de desarrollo aprobadas por la Comisión Permanente de la Red Provincial

6 MISION:

La Diputación de Almería es una entidad local de ámbito provincial que tiene las competencias atribuidas por la legislación vigente en materia de Régimen Local (Ley 7/1985, Reguladora de las Bases de Régimen Local; Ley 5/2010, de Autonomía Local de las Entidades Locales de Andalucía, etc), entre las que podemos las siguientes:

a) La coordinación de los servicios municipales entre sí para la garantía de la prestación integral y adecuada en la totalidad del territorio provincial de los servicios de competencia municipal.

b) La asistencia y la cooperación jurídica, económica y técnica a los Municipios, especialmente los de menor capacidad económica y de gestión.

c) La prestación de servicios públicos de carácter supramunicipal y, en su caso, supracomarcal.

d) La cooperación en el fomento del desarrollo económico y social y en la planificación en el territorio provincial, de acuerdo con las competencias de las demás Administraciones Públicas en este ámbito.

e) La prestación de los servicios de administración electrónica y la contratación centralizada en los municipios con población inferior a 20.000 habitantes.

f) En general las que con carácter específico y para el fomento y la administración de los intereses peculiares de la provincia le vengan atribuidas por la legislación básica del Estado y por la legislación que dicte la Comunidad Autónoma en desarrollo de la misma.

7 Legislación y normativa de referencia

El marco normativo de las actividades de la Diputación de Almería en el ámbito de esta Política de Seguridad de la Información y Protección de Datos está integrado por las siguientes normas:

- Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.
- Ordenanza de transparencia, acceso a la información, reutilización y buen gobierno de la Diputación de Almería, publicado en BOP número 199 de 16 de octubre de 2018.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

- Reglamento Europeo de Firma Electrónica (eIDAS). Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejos de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas;
- Demás disposiciones reglamentarias de la Diputación, reguladoras de aspectos relacionados con la administración electrónica en general, y en especial las referentes a organización y funcionamiento, documento, expediente y archivo electrónico, registro, tablón de anuncios, Boletín Oficial, actuación administrativa automatizada y sede electrónica

8 Principios.

8.1 Principios básicos para garantizar la Seguridad de la Información.

La finalidad última de la seguridad de la información es asegurar que una organización, en este caso la Diputación de Almería, pueda cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Por lo tanto, toda acción dirigida al objetivo de la seguridad debe considerar la interacción de todos los elementos mencionados, lo que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Gestión de riesgos. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado. La gestión de riesgos permitirá el mantenimiento de un entorno

controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Prevención, reacción y recuperación. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, y no afecten gravemente a la información que maneja, o los servicios que se prestan.

Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.

Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

Líneas de defensa. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
c) Minimizar el impacto final sobre el sistema.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Reevaluación periódica. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, así como del estado de la técnica y el coste económico de implantación de las medidas de seguridad, llegando incluso a un replanteamiento de la seguridad, si fuese necesario

Función diferenciada. En los sistemas de información que son responsabilidad de la Diputación de Almería se observará el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y roles:

En el ámbito de la protección de datos personales:

- Responsable del tratamiento: determina los fines y medios del tratamiento de datos personales.
- Encargado del tratamiento: trata datos personales por cuenta del responsable del tratamiento.
- Delegado de protección de datos: informa y asesora al responsable del tratamiento de las obligaciones en materia de cumplimiento de la normativa de protección de datos personales.

- Responsable funcional de cada una de las actividades de tratamiento: informa al ciudadano del tratamiento de sus datos y adopta las medidas técnicas y organizativas que garanticen la privacidad de sus datos personales. Son técnicos, máxima jerarquía de los servicios, o dependencias que en el ejercicio de sus funciones está la responsabilidad de tratamientos de datos personales.

En el ámbito del procedimiento administrativo y otras actividades de la Diputación realizadas en el seno de las competencias que tiene atribuidas legalmente:

- Responsable de la información: determina los requisitos de seguridad de la información tratada.
- Responsable del servicio: determina los requisitos de seguridad de los servicios prestados.
- Responsable de seguridad: determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Responsable del sistema: se encarga de la explotación del sistema de información desde la perspectiva de la seguridad de la información.

8.2 Principios en el tratamiento de datos personales.

El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las normas aplicables en cada momento, siendo especialmente importantes el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (LOPDGDD).

La Diputación de Almería tratará la información y los datos personales bajo su responsabilidad conforme a los siguientes principios de protección de datos:

Licitud, lealtad y transparencia: los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.

Legitimación en el tratamiento de datos personales: solo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las condiciones establecidas en los artículos 6 y 9 del RGPD.

Limitación de la finalidad: los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

Minimización de datos: los datos de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Exactitud: los datos de carácter personal serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

Limitación del plazo de conservación: los datos de carácter personal serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines que justificaron su tratamiento.

Integridad y confidencialidad: los datos de carácter personal serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido aquel.

Responsabilidad proactiva: la Diputación de Almería será responsable del cumplimiento de los principios anteriormente señalados y adoptará las medidas técnicas y organizativas que le permitan estar en condiciones de demostrar dicho cumplimiento.

Atención de los derechos de los afectados: se adoptarán medidas en la organización que garanticen el adecuado ejercicio por los afectados, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal.

Protección de datos y seguridad desde el diseño: la Diputación de Almería promoverá la implantación del principio de protección de datos desde el diseño con el objetivo de cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados de forma que la protección de datos se encuentre presente en las primeras fases de concepción de un tratamiento de datos personales o de los sistemas de información que deberán tratarlos.

Protección de datos por defecto: la Diputación de Almería promoverá que los sistemas de información de su titularidad se diseñen y configuren de forma que garanticen la protección de datos por defecto garantizando que solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento y que los sistemas configuren de forma segura antes de su puesta en funcionamiento.

9 Requisitos mínimos de seguridad.

Esta política de seguridad, se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos de seguridad:

Organización e implantación del proceso de seguridad: La seguridad deberá comprometer a todos los miembros de la organización. La presente Política identificará unos claros responsables de velar por su cumplimiento y deberá ser conocida por todos los miembros de la organización administrativa.

Análisis y gestión de los riesgos: La Diputación de Almería realizará su propia gestión de riesgos mediante el análisis y tratamiento de los riesgos a los que está expuesto el sistema de información de acuerdo a una

metodología reconocida por el ENS o internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Gestión de personal: Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones tendrán como objetivo ejercitar y aplicar los principios de seguridad establecidos por la presente Política y serán supervisadas para verificar que se siguen los procedimientos establecidos. Para corregir, o exigir responsabilidades, en su caso, cada usuario que acceda a la información del sistema estará identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos y quién ha realizado determinada actividad.

Profesionalidad: La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento. El personal de la Diputación de Almería, recibirán la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de dichas Organizaciones. La Diputación de Almería exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados

Autorización y control de los accesos: Los accesos a los sistemas de información deberán ser controlados y limitados a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

Protección de las instalaciones: Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Adquisición de productos y servicios de seguridad: En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por la Diputación de Almería se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad. Dicha certificación estará de acuerdo con las normas y estándares de mayor reconocimiento internacional en el ámbito de la seguridad, así como las emitidas por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Integridad y actualización del sistema: Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Protección de la información almacenada y en tránsito: En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, dispositivos móviles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por la Diputación en el ámbito de sus competencias.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica del alcance de la presente Política, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de estos.

Prevención ante otros sistemas de información interconectados: Los sistemas de la Diputación de han de proteger el perímetro, en particular, si se conectan a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión de los sistemas, a través de redes, con otros sistemas, y se controlará su punto de interconexión.

Registro de actividad: Con la finalidad exclusiva de lograr el cumplimiento del Esquema Nacional de Seguridad, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación a la Diputación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Incidentes de seguridad: Se establecerá un sistema de detección y reacción frente a incidentes de seguridad y de un procedimiento para su gestión. Se registrarán los incidentes de seguridad que se produzcan y las acciones de remediación que se apliquen. Estos registros se emplearán para la mejora continua de la seguridad del sistema.

Continuidad de la actividad: Los sistemas de la Diputación de Almería dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Mejora continua del proceso de seguridad: La Diputación de Almería implantará un proceso integral de seguridad que deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

Cumplimiento de los requisitos mínimos:

La Diputación de Almería para dar cumplimiento a los requisitos mínimos establecidos aplicará las medidas de seguridad indicadas en el Anexo II del Esquema Nacional de Seguridad, así como las indicadas en la Normativa de Protección de Datos de carácter personal, teniendo en cuenta:

a. Los activos que constituyen el sistema.
b. La categoría del sistema, según lo previsto en el artículo 43 del ENS
c. Los tratamientos de datos personales que se realicen.
d. Las decisiones que se adopten para gestionar los riesgos identificados.

Estas medidas tendrán la condición de mínimos exigibles y podrán se ampliadas o substituidas por medidas compensatorias de acuerdo con el prudente arbitrio del responsable de la seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada y los riesgos a que están expuestos y el coste económico de implantación de las medidas de seguridad.

Las medidas compensatorias podrán reemplazar las medidas de seguridad exigibles por el Anexo II del ENS siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre la información y los servicios y se satisfacen los principios básicos y los requisitos mínimos previstos por la presente Política.

En cualquier caso, las medidas de seguridad aplicadas se formalizarán en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de seguridad donde, en su caso, se identificará las medidas compensatorias a cuáles sustituyen de las exigidas por el Anexo II del ENS.

10 Registro de actividades de tratamiento de datos personales.

La Diputación de Almería y EE.LL: que se adhieran a esta PSIPD dispondrán de un Registro de las Actividades de Tratamiento de datos personales que incluye las actividades de tratamiento de datos de carácter personal de las que es responsable, y también de las que sea encargado del tratamiento y trata datos responsabilidad de un tercero bajo sus directrices. Este Registro de Actividades del Tratamiento incluye toda la información a la que se refiere el artículo 30 del RGPD.

El registro de actividades de tratamiento se mantendrá continuamente actualizado y podrá consultarse en el apartado de Privacidad de la página web y la sede electrónica de la Diputación de Almería. Adicionalmente, a través del Registro de Actividades de Tratamiento se podrá acceder a las cláusulas informativas de cada actividad del tratamiento.

Algunas de estas actividades de tratamiento se identifican como sistemas de información o activos de la Diputación de Almería y, por tanto, se verán afectados, aparte de por el marco jurídico en materia de protección de datos, por el ENS.

11 Análisis de riesgos y evaluación de impacto en la protección de datos personales.

1. El análisis de riesgos permite identificar y gestionar los riesgos minimizándolos hasta los niveles que puedan considerarse aceptables. Esta evaluación se llevará a cabo de forma periódica, incluirá un análisis de los riesgos para los derechos y libertades de las personas físicas respecto de las actividades de tratamiento con datos personales que lleve a cabo la Diputación de Almería, así como los sistemas de información que sirven de soporte para dichas actividades de tratamiento.

   Será necesario realizar un análisis de riesgos cuando se apruebe una nueva actividad de tratamiento, una modificación de la formación de la información de una actividad ya existente en el RAT, cuando ocurra un incidente de seguridad o se identifiquen vulnerabilidades graves y, sistemáticamente, una vez cada año previamente a la aprobación por resolución de Presidencia del RAT.

   Asimismo, la Diputación de Almería llevará a cabo una evaluación de impacto de las actividades de tratamiento en la protección de datos personales cuando del análisis realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas, conforme a lo previsto en el artículo 35 del RGPD.

2. La gestión de riesgos de seguridad de la información debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

   El Responsable de Seguridad es el encargado de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

   El Responsable de la Información y los responsables de los Servicios son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

3. Para el análisis y gestión de riesgos se utilizarán las herramientas facilitadas por el Centro Criptológico Nacional (CCN), en particular las herramientas PILAR y µPILAR o las que se desarrollasen

en el futuro, así como las guías, recomendaciones y herramientas elaboradas por la AEPD en lo que respecta al tratamiento de datos de carácter personal.

12 Notificación de violaciones de seguridad.

La Diputación de Almería adoptará las medidas necesarias para garantizar el registro y la notificación de los incidentes y las violaciones de seguridad, de conformidad con lo dispuesto en los artículos 33 y 34 del RGPD y del artículo 24 del Esquema Nacional de Seguridad

Igualmente adoptará las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal o cualquier información o incidencia sobre un sistema de información que maneje datos sensibles y confidenciales de la dependencia u organismo correspondiente conforme a lo dispuesto en el artículo 34 del RGPD.

Los ciberincidentes de seguridad detectados se registrarán, analizarán, clasificarán y gestionarán, tanto si afectan a datos personales como a cualquier tipo de información.

13 Revisión y auditoria.

La Diputación de Almería llevará a cabo de forma periódica, y al menos una vez cada dos años, una auditoría encaminada a la verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los sistemas de información y del tratamiento de datos personales.

En todo caso realizará una auditoría específica y extraordinaria cuando se lleven a cabo modificaciones sustanciales en los sistemas de información o en los tratamientos de datos personales, que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Las auditorías serán supervisadas por el responsable de seguridad de la información y por el delegado de protección de datos.

14 Organización de la Seguridad de la Información

1. La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la PSIDP de la Diputación de Almería está compuesta por los siguientes agentes:
    a) Órganos de Gobierno
    b) El Comité de Seguridad de la Información
    c) Responsable de Seguridad

d) Responsables de la Información y de los Servicios
e) Responsable del Sistema
f) Responsable del Sistema Delegado para Sistemas y Comunicaciones.
g) Responsable del Sistema Delegado para gestores de BD y Servidores de Aplicaciones.
h) Delegado de Protección de Datos
i) Responsable del Tratamiento
j) Responsables funcionales de los Tratamientos

2. La estructura organizativa será competente para mantener, actualizar y hacer cumplir, la PSIDP de la Diputación de Almería.

14.1 Órganos de Gobierno

Son los responsables de aprobar las normas y procedimientos de seguridad.

14.2 Comité de Seguridad de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de Seguridad, dentro del ámbito de la presente PSIDP, formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en la Organización y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de seguridad de la información, protección de datos de carácter personal y transparencia.

Son funciones del Comité de Seguridad las siguientes:

a) Identificar los objetivos de la Organización en el ámbito de la Seguridad de la Información.

b) Proponer al órgano competente de la Diputación de Almería la Política de Seguridad de la Información de esta Administración, así como otros documentos que definan las distintas actuaciones a desarrollar dentro del marco legislativo que regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (Real Decreto 3/2010), la protección de datos (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales) y la transparencia (Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, y Ley 1/2014 de 24 de junio, de Transparencia Pública de Andalucía).

c) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en la Organización.

d) Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnicos y de control, los sistemas y servicios de la Organización.

e) Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.

f) Velar porque la seguridad de la información se tenga en cuenta en todos los Proyectos TIC, desde su especificación inicial hasta su puesta en operación

g) Informar regularmente al Pleno sobre el estado de la seguridad de la información y la protección de datos personales.

h) Recabar del responsable de Seguridad informes regulares del estado de la seguridad de la organización y de los posibles incidentes

i) Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de la misma conforme a los exigidos en el ENS.

j) Proponer al órgano competente la designación de los nombramientos de responsables y responsabilidades en materia de seguridad de la información.

k) Definir y proponer las funciones de los integrantes del Comité de Seguridad

l) Definir y proponer las funciones a incluir en el catálogo de puestos de trabajo de la Diputación de Almería, relacionadas con las materias objeto de estudio por el Comité

m) Valorar el grado de conformidad de los procedimientos implantados en la Organización con las normas definidas en la PSIDP, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.

n) Supervisar las normativas y procedimientos de seguridad que se definan para dar cumplimiento y desarrollo a la PSIDP.

o) Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

p) Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la PSIDP.

q) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la Diputación en materia de Seguridad.

r) Resolver los conflictos de seguridad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir

s) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados

t) Promover la formación y concienciación en materia de Seguridad de la Información y Protección de Datos Personales a todo el personal.

u) Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de la Organización.

v) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en la Organización.

w) Quienes tengan atribuidas las funciones del Servicio de Organización e Información apoyarán al Comité de Seguridad de la Información en todas aquellas actuaciones necesarias para la preparación, instrumentalización, difusión e implantación de las decisiones que se vayan adoptando por el Comité

x) Proponer a la Delegación correspondiente los indicadores de transparencia a incluir en el Portal de Transparencia de la WEB de la Diputación de Almería, para su aprobación por el Pleno.

y) El Comité de Seguridad tiene asignadas las funciones del Delegado de Protección de Datos recogidas en el artículo 39 del el Reglamento (UE) 2016/679 (RGPD), en los términos previstos en el régimen transitorio de esta política

La composición del Comité de Seguridad se aprobará por resolución de Presidencia atendiendo a las necesidades en materia del ENS, Protección de datos y Transparencia.

Se informará a los representantes de las Entidades locales usuarias de la Red Provincial de la PSIDP de la Diputación y de las normativas que emanan de la misma y que sean de aplicación en su ámbito, así como de posibles acuerdos del Comité de Seguridad que pudieran afectarles.

El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez al mes, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

14.3 Responsable de Seguridad

Es el responsable de que los servicios y sistemas de información de la Organización se mantengan con el mayor grado de seguridad atendiendo a los principios de la presente Política siendo quien determina y supervisa las medidas de seguridad que deben ser implantadas de acuerdo con la valoración de los servicios y de la información por los responsables de los servicios y de la información, respectivamente.

Son funciones del Responsable de Seguridad:

a) Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.
b) Ser el responsable de la toma de decisiones día a día en materia de seguridad de la información entre las reuniones del Comité de Seguridad. Estas decisiones respetarán los principios de unidad de acción

y coordinación de actuaciones en general y, en su caso, se elevarán al Comité de Seguridad mediante la convocatoria extraordinaria del mismo.

c) Asesorar en materia de seguridad al personal de la Diputación de Almería que así lo requieran.
d) Coordinar la interacción con otros organismos especializados.
e) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
f) Ser responsable, junto con los diferentes responsables de seguridad delegados, en su caso, de estar al tanto de los cambios normativos que puedan afectar directa o indirectamente, a la seguridad de los sistemas de información del Ayuntamiento, comunicándolo al Comité de Seguridad y proponiendo las acciones oportunas para la adecuación al nuevo marco normativo.
g) Elaborar las pertinentes Declaraciones de Aplicabilidad de medidas de seguridad en cada sistema de información de acuerdo con la valoración de la información y los servicios a los que apoyan según determinen el responsable de la información y del servicio correspondientes.
h) Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
i) Asesorar, en colaboración con el Responsable del Sistema, los Responsables de los Servicios y de la Información en la realización de los análisis y gestión de riesgos, elevando el informe resultado al Comité de Seguridad.
j) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad, en concreto:
    a. un resumen consolidado de actuaciones en materia de seguridad,
    b. un resumen consolidado de incidentes relativos a la seguridad de la información,
    c. el estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.
k) Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
l) Actuar como secretario del Comité de Seguridad.

Respecto a la documentación, son funciones del Responsable de Seguridad:

a) Proponer al Comité de Seguridad la documentación de seguridad de segundo nivel (Normativas y Procedimientos de Seguridad) de obligado cumplimiento.
b) Supervisar la documentación de tercer nivel (Procedimientos Técnicos de Seguridad) de obligado cumplimiento.
c) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Respecto a la protección de datos de carácter personal, son funciones del Responsable de Seguridad:

a) Garantizar la seguridad de los datos, implantando y haciendo cumplir las medidas, procedimientos, instrucciones y normativas establecidas en el “Manual Jurídico” de referencia en cuanto a procedimientos relacionados con la normativa de privacidad y protección de datos personales, así

como sus anexos, definido en la Diputación de Almería, en colaboración con el Delegado de Protección de Datos.

b) Colaborar con el responsable del tratamiento en la difusión del Manual jurídico y de sus anexos.
c) Realizar los controles periódicos establecidos para verificar el cumplimiento del Manual jurídico y de sus anexos.
d) Analizar los informes de auditoría y proponer al responsable del sistema las medidas correctoras oportunas.
e) Cumplir con el procedimiento de ejercicio de derechos de los interesados según las solicitudes recibidas.
f) Autorizar la recuperación de datos tratados.

En aquellos sistemas de información que, por su complejidad, distribución, separación física de elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones del Responsable de Seguridad, el Responsable de Seguridad podrá designar cuantos Responsables de Seguridad Delegados considere necesarios. Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencia funcional directa con él.

El Responsable de Seguridad será designado por el Presidente a propuesta del Comité de Seguridad.

14.4 Responsables de la Información y/o de los Servicios

Estas responsabilidades recaerán en la máxima jerarquía técnica de la dependencia que gestione la información y/o servicio correspondiente, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione

Son los responsables de clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS.

Son los responsables de determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

Son los encargados, contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema de Información, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

Son los responsables de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Responsable del servicio

1. El responsable del servicio es quien tiene la potestad de establecer las características de un servicio, a los efectos de determinar los requerimientos en materia de seguridad y de la información.

2. Al responsable del servicio le corresponde:

a. la valoración del servicio en todas las dimensiones de seguridad -disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad- teniendo en cuenta la naturaleza del servicio y la normativa que pueda serle de aplicación.

b. la propiedad de los riesgos sobre los servicios

c. la aceptación del riesgo residual sobre los servicios que sean de su competencia.

Responsable de la información

1. El responsable de la información es quien tiene la potestad de establecer las características de la información, a los efectos de determinar los requerimientos en materia de seguridad de la información. Al responsable de la información le corresponde:

a. la valoración de la información en todas las dimensiones de seguridad -disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad- teniendo en cuenta la naturaleza de esta información y la normativa que pueda serle de aplicación.

b. la responsabilidad última de la protección de la información respecto al uso que de ella hagan las personas a su cargo, o las que dependan de su dirección, o en general, las que sean autorizadas por él para acceder a la información.

c. la propiedad de los riesgos sobre la información.

d. aceptar el riesgo residual sobre la información de la que es responsable.

e. autorizar los accesos de los usuarios a la información, respetando los principios de mínimo privilegio y necesidad de conocer establecidos en la presente Política.

f. la responsabilidad última del cumplimiento de todas las garantías establecidas por la legislación y la normativa interna de la Diputación, especialmente en cuanto a información que contenga datos de carácter personal.

g. la responsabilidad última de cualquier error o negligencia que derive en un incidente de seguridad en cualquiera de sus dimensiones, motivado por no atender con la debida diligencia el deber de velar por el cumplimiento de las medidas de seguridad establecidas.

14.5 Responsable del Sistema.

Personal designado cuyas responsabilidades son:

a) Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
c) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
d) Elaborar procedimientos técnicos de seguridad de los sistemas de información.
e) Elaborar planes de continuidad de los sistemas de información.

Podrá acordar la suspensión del manejo de determinada información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser acordada con el Responsable de la Información y servicio afectados y el Responsable de Seguridad antes de ser ejecutada.

14.6 Responsable de Sistema Delegado para Sistemas y Comunicaciones:

Personal designado cuyas funciones, en el ámbito de los sistemas y comunicaciones, son:

a) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los sistemas y comunicaciones.
b) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas y comunicaciones.
c) La gestión de las autorizaciones y privilegios concedidos a los usuarios de los sistemas, incluyendo la monitorización de que la actividad desarrollada en los sistemas se ajusta a lo autorizado.
d) La aplicación de los Procedimientos Operativos de Seguridad en los Sistemas e infraestructuras de comunicaciones.
e) Asegurar que los controles de seguridad establecidos son adecuadamente observados.
f) Asegurar que son aplicados los procedimientos aprobados para manejar los Sistemas y las infraestructuras de las comunicaciones.
g) Supervisar las instalaciones de hardware y software en Sistemas y equipos de comunicaciones, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
h) Monitorizar el estado de seguridad de los sistemas y equipos de comunicaciones proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados.
i) Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
j) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

14.7 Responsable de Sistema Delegado para Bases de Datos y Aplicaciones.

Personal designado cuyas funciones, en el ámbito de los Gestores de Bases de Datos y servidores de aplicaciones, son:

a) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los gestores de bases de datos y servidores de aplicaciones.
b) La gestión, configuración y actualización, en su caso, del software en los que se basan los mecanismos y servicios de seguridad de los Gestores de Bases de Datos y Servidores de Aplicaciones.
c) La gestión de las autorizaciones y privilegios concedidos a los usuarios en los gestores de bases de datos y servidores de Aplicaciones, incluyendo la monitorización de que la actividad desarrollada en los sistemas se ajusta a lo autorizado.
d) La aplicación de los Procedimientos Operativos de Seguridad en los gestores de bases de datos y servidores de Aplicaciones.
e) Asegurar que los controles de seguridad establecidos son adecuadamente observados.
f) Asegurar que son aplicados los procedimientos aprobados para manejar los los gestores de bases de datos y servidores de Aplicaciones.
g) Supervisar las instalaciones de software en los gestores de bases de datos y servidores de Aplicaciones, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
h) Monitorizar el estado de seguridad de los los gestores de bases de datos y servidores de Aplicaciones proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados.
i) Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
j) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

14.8 Delegado de Protección de Datos

En los términos previstos en el régimen transitorio de esta política se asigna al Comité de Seguridad de la Diputación de Almería las funciones de Delegado de Protección de Datos, recogidas en el artículo 39 del Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos - RGPD).

Son funciones del Delegado de Protección de Datos:

- Informar y asesorar a la Organización y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y de otras disposiciones relacionadas con la protección de datos.
- Supervisar el cumplimiento del Reglamento General de Protección de Datos en la Organización.
- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la Autoridad de control

- Actuar como punto de contacto de la Autoridad de Control y la ciudadanía. Se designa por el Presidente a propuesta del Comité de Seguridad, ejerciendo de Secretario del Comité de Seguridad de la Información de esta Diputación y actuando como interlocutor para la Agencia de Protección de Datos Personales y/u otras autoridades de control y como persona de contacto para la ciudadanía, en lo que respecta al ejercicio de sus derechos en materia de protección de datos personales respecto de la propia Diputación de Almería, y de las entidades locales sobre las que el Comité de Seguridad de la Información asuma las funciones del Delegado de Protección de Datos, en los términos previstos en el régimen transitorio de esta política.
- Garantizar la seguridad de los datos, implantando y haciendo cumplir las medidas, procedimientos, instrucciones y normativas establecidas en el Manual jurídico definido en la organización, así como sus anexos, en colaboración con el Responsable de Seguridad.
- El Comité de Seguridad desempeñará sus funciones de Delegado de Protección de Datos, en los términos previstos en el régimen transitorio de esta política, prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Además, asesorará y supervisará en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación Organización – encargado de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditorías de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento
- Análisis de riesgo de los tratamientos realizados
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos

- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal de la Organización en materia de protección de datos.

14.9 Responsable del Tratamiento

El responsable del tratamiento es la Diputación de Almería, que es quien determina los fines y medios del tratamiento.

14.10 Responsables funcionales del Tratamiento

El Responsable funcional del tratamiento es la máxima jerarquía técnica sobre la que recae las funciones del Responsable del tratamiento en uno o más tratamientos concretos de la Organización. En concreto son funciones del Responsable funcional del tratamiento:

- Garantizar la observancia de los principios relativos al tratamiento.
- Garantizar el cumplimiento de las medidas técnicas y organizativas definidas.
- Garantizar el cumplimiento de las políticas y normativas aprobadas e implementadas en la organización.
- Asegurar que la realización de tratamientos por cuenta de terceros esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.
- Adoptar las medidas correctoras adecuadas.

14.11 Grupo provincial de Seguridad de la Información y protección de Datos.

Al objeto de coordinar la gestión de la protección de datos personales y la seguridad de la información con las Entidades Adheridas a la Red Provincial de Comunicaciones se creará el presente órgano al objeto de difundir la protección de datos y la seguridad de la información a todos los miembros de las Entidades Adheridas, así como recoger propuestas de mejora para la gestión de la protección de datos y seguridad de la información.

Este órgano estará compuesto por técnicos de las Entidades que formen parte de la Comisión Permanente de la Red Provincial de Comunicaciones y podrán asistir cualquier personal perteneciente a las Entidades Adheridas, se reunirá con carácter trimestral.

Las funciones de este órgano son de difusión y concienciación de la protección de datos y seguridad de la información, así como la de realizar propuestas al Comité de Seguridad.

14.12 Asignación de tareas:

Los órganos de la Diputación de Almería, el Comité de Seguridad, el responsable de seguridad de la información y el delegado de protección de datos, dentro de su respectivo ámbito, podrán asignar tareas relativas a la mejora de los principios recogidos en la presente política a personas o grupos de trabajo En la asignación de tareas se tendrá en cuenta a todo el personal que presta sus servicios en la Diputación de Almería y a especialistas externos cuando sea necesario.

14.13 Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información y protección de datos corresponderá, en última instancia, a la Presidencia, asistida por el Comité de Seguridad de la Información y, cuando proceda, por el responsable de seguridad o delegado de protección de datos, la resolución de conflictos en calidad de máximo responsable de la Diputación.

14.14 Obligaciones del Personal

Todos los órganos y unidades de la Diputación de Almería, prestarán su colaboración en las actuaciones de implementación de esta Política.

Todas las personas que presten servicio en la Diputación de Almería, tienen la obligación de conocer y cumplir lo previsto en la presente Política, así como en las normas y procedimientos que la desarrollen.

Todo el personal que presta servicio en la Diputación de Almería, tienen asimismo el deber de colaborar en la mejora de los principios y requisitos en materia de protección de datos y seguridad de la información evitando y aminorando los riesgos a los que se encuentra expuesta la información y los datos personales de los que es titular la Diputación. A tal efecto, comunicarán a los integrantes de la estructura organizativa de la política de seguridad de la información y protección de datos, cualquier propuesta o sugerencia que ayude a preservar la confidencialidad, la integridad y la disponibilidad de la información.

15 Asesoramiento Especializado en Materia de Seguridad

15.1 Asesoramiento especializado

El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en la Diputación de Almería con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

15.2 Cooperación entre organismos y otras Administraciones Públicas

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, la Diputación de Almería mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad.

15.3 Revisión independiente de la Seguridad de la Información

El Comité de Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la PSIPD con el fin de garantizar que las prácticas en la Organización reflejan adecuadamente sus disposiciones.

16 Formación y concienciación

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación del personal que presta sus servicios en la Diputación de Almería, así como a la difusión entre los mismos de la PSIPD y de su desarrollo normativo.

La Diputación de Almería dispondrá los medios necesarios para que todas las personas con acceso a la información sean informadas acerca de sus deberes y obligaciones, así como de los riesgos existentes en el tratamiento de la información.

A fin de garantizar el cumplimiento de la PSIPD, las acciones de concienciación y formación serán supervisadas por:

- El Delegado de Protección de Datos para las acciones en materia de protección de datos personales.
- El Responsable de Seguridad para las acciones en materia de seguridad de la información.

17 Estructura normativa

La documentación relativa a la Seguridad de la Información y Protección de Datos Personales estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad de la Información y Protección de Datos Personales.
- Segundo nivel: Normativas y Procedimientos de Seguridad.
- Tercer nivel: Procedimientos Técnicos de Seguridad.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

17.1 Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de la Organización, y para cualquier tercero que se relacione con Diputación y deba acceder a los sistemas de información de Diputación por cualquier vía, que será recogido en el presente documento y aprobado mediante Acuerdo de Pleno.

17.2 Segundo Nivel: Normativas y Procedimientos de Seguridad

Documento de obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de estos documentos será por resolución de Presidencia o Acuerdo de Pleno, según proceda, a propuesta del Comité de Seguridad.

17.3 Tercer Nivel: Procedimientos Técnicos de Seguridad

Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Se aprobarán a través de resolución de Presidencia a propuesta del Comité de Seguridad.

17.4 Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito.

17.5 Otra documentación

Se podrán seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500 y 600. Así como las normas y guías de la AEPD.

18 Publicación de la política de seguridad

La presente política se publicará, además de en el "Boletín Oficial de la Provincia", en la sede electrónica de la Diputación de Almería y en el Portal de Transparencia.

19 Régimen transitorio

Hasta tanto la Diputación de Almería designa al Delegado de Protección de Datos, todos los cometidos que corresponden a éste serán desempeñados por el Comité de Seguridad de la Información

20 Entrada en vigor

La PSPI que se aprueba por decreto de Presidencia nº 2007, de 20 de julio de 2020será aplicable a partir del día siguiente al de su publicación en el Boletín Oficial de la Provincia.

Almería, 20 de julio de 2020.