Firmado digitalmene por bop.dival.es
Boletín Oficial de la Provincia de Valencia
Razón: Se certifica la precisión e integridad de este documento
Ubicación: c/Beato Nicolás Factor nº1 - 46007 Valencia

Excelentísima Diputación Provincial de Valencia

Anuncio de la Excelentísima Diputación Provincial de Valencia sobre aprobación inicial del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de esta Diputación.

ANUNCIO

El Pleno de esta Diputación Provincial, en sesión del día 18 de junio, ha adoptado el siguiente acuerdo:

"El Pleno de la Diputación de Valencia, en sesión celebrada el 16 de octubre de 2012, aprobó el Plan de Adecuación de la Corporación al Esquema Nacional de Seguridad, en el que se establecen las actuaciones necesarias y la planificación para que los sistemas de información de la Corporación se ajusten a las prescripciones del Real Decreto 3/2010, de 8 de Nero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Atendido que una de las actuaciones fundamentales que conforman el citado Plan es la implementación de la Política de Seguridad y de la Protección de Datos Personales de la organización.

Visto que conforme a lo establecido en el Plan uno de los principales hitos a acometer en la ejecución del mismo es la aprobación de la Política de Seguridad y de la Protección de Datos Personales de la Diputación de Valencia.

Visto el informe emitido por el Sr. Secretario, que obra en el expediente.

Atendido que el Pleno de la Corporación es el órgano competente para la aprobación del reglamento orgánico, las ordenanzas y demás disposiciones de carácter general que sean de la competencia provincial, según dispone el artículo 70.4 del Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.

SE ACUERDA

Primero. Aprobar inicialmente el Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia, cuyo texto debidamente autenticado por el Sr. Secretario figura en el expediente.

Segundo. Exponer al público el presente acuerdo y el reglamento por el plazo de 30 días hábiles, mediante publicación de anuncio en el Boletín Oficial de la Provincia, a efectos de reclamaciones y sugerencias. Transcurrido dicho plazo sin que se hubiesen presentado reclamaciones, el reglamento se entenderá definitivamente aprobado."

TÍTULO PRELIMINAR

Ámbito de aplicación y disposiciones generales

Capítulo Primero

Disposiciones comunes

Artículo 1. OBJETO

Artículo 2. DEFINICIONES

Artículo 3. ALCANCE

Artículo 4. ÁMBITO SUBJETIVO DE APLICACIÓN

Capítulo Segundo

Misión y marco legal

Artículo 5. MISIÓN

Artículo 6. MARCO LEGAL

TÍTULO PRIMERO

Principios de seguridad TIC y de la protección de datos de carácter personal

Capítulo Primero

Principios comunes

Artículo 7. ACCESO A LA INFORMACIÓN

Artículo 8. CICLO VITAL DE LA INFORMACIÓN

Artículo 9. DEBER DE SECRETO

Artículo 10. MAYOR PROTECCIÓN

Capítulo Segundo

Principios de seguridad TIC

Artículo 11. PROCESO INTEGRAL

Artículo 12. GESTIÓN BASADA EN RIESGOS

Artículo 13. PREVENCIÓN

Artículo 14. DETECCIÓN

Artículo 15. RESPUESTA

Artículo 16. RECUPERACIÓN

Capítulo Tercero

Principios de la protección de datos de carácter personal

Artículo 17. CALIDAD DE LOS DATOS

Artículo 18. INFORMACIÓN Y CONSENTIMIENTO

Artículo 19. DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

Artículo 20. COMUNICACIÓN DE DATOS

Artículo 21. ACCESO A DATOS POR CUENTA DE TERCEROS

TÍTULO SEGUNDO

Organización de la seguridad y de la protección de datos personales

Capítulo Primero

Principios comunes

Artículo 22. RESPONSABILIDAD GENERAL Y ESPECÍFICA

Artículo 23. ESTRUCTURA ORGANIZATIVA

Artículo 24. RESOLUCIÓN DE CONFLICTOS

Capítulo Segundo

Figuras de naturaleza unipersonal

Artículo 25. RESPONSABLE DEL SERVICIO

Artículo 26. RESPONSABLE DE LA INFORMACIÓN

Artículo 27. DISPOSICIONES COMUNES AL RESPONSABLE DEL SERVICIO Y AL RESPONSABLE DE LA INFORMACIÓN

Artículo 28. RESPONSABLE DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Artículo 29. RESPONSABLE DE LOS SISTEMAS DE INFORMACIÓN TIC

Artículo 30. ADMINISTRADOR DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN TIC

Artículo 31. RESPONSABLE DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Capítulo Tercero

Órganos de carácter colegiado

Artículo 32. COMITÉ DE SEGURIDAD TIC

TÍTULO TERCERO

Disposiciones relativas al personal

Capítulo Primero

Obligaciones y responsabilidades

Artículo 33. OBLIGACIONES DEL PERSONAL

Artículo 34. TERCERAS PARTES

Artículo 35. INCUMPLIMIENTOS

Capítulo Segundo

Recursos formativos

Artículo 36. FORMACIÓN Y CONCIENCIACIÓN

TÍTULO CUARTO

Desarrollo y modificación de la Política de Seguridad y de Protección de Datos de Carácter Personal

Capítulo Primero

Instrumentos de desarrollo

Artículo 37. DESARROLLO NORMATIVO

Artículo 37.1. NIVEL A

Artículo 37.2. NIVEL B

Artículo 37.3. NIVEL C

Artículo 38. DOCUMENTO DE SEGURIDAD

Capítulo Segundo

Competencias de desarrollo

Artículo 39. ASIGNACIÓN DE COMPETENCIAS DE DESARROLLO

Artículo 39.1. INSTRUMENTOS DE NIVEL A y B

Artículo 39.2. INSTRUMENTOS DE NIVEL C

Capítulo Tercero

Modificación de la Política

Artículo 40. ACTUALIZACIÓN PERMANENTE

Artículo 41. PROCEDIMIENTO PARA LA MODIFICACIÓN
DISPOSICION DEROGATORIA
Única. DEROGACIÓN NORMATIVA
DISPOSICION TRANSITORIA
Única. NORMATIVA INTERNA VIGENTE
DISPOSICIONES FINALES
Primera. CONSTITUCIÓN DEL COMITÉ DE SEGURIDAD TIC
Segunda. DESARROLLO NORMATIVO
Tercera. POLITICAS DE ÁMBITO MUNICIPAL
Cuarta. ENTRADA EN VIGOR

Para el cumplimiento de su misión, la prestación de los servicios identificados y el cumplimiento de sus objetivos, la Diputación de Valencia depende de los sistemas TIC (Tecnologías de la Información y Comunicaciones). Estos sistemas deben ser administrados con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada o de los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de ésta y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC 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 mayor abundancia, en el específico marco de la administración electrónica, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, proclama como uno de sus fines crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

Es por ello que el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, establece que Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de 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 Corporación, en tanto responsable de ficheros y tratamientos de esta naturaleza, la necesaria adopción de una serie de medidas de carácter técnico y organizativo tendentes a garantizar los derechos de los titulares de dichos datos personales.

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 Valencia ha decidido aprobar en una misma norma los principios y directrices básicas que han de regir las actuaciones en materia de seguridad y protección de datos personales de los sistemas de información utilizados en el marco de sus competencias.

El Pleno de la Diputación de Valencia, en sesión celebrada el 16 de octubre de 2012, aprobó el Plan de Adecuación de la Corporación al ENS. Una de las actuaciones fundamentales que conforman el citado Plan es la implementación de la Política de Seguridad y de la Protección de Datos Personales de la organización.

Para la elaboración de la presente disposición se ha tenido en consideración la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, el 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, la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y las denominadas guías de seguridad de las tecnologías de la información y las comunicaciones (serie CCN-STIC) elaboradas por el Centro Criptológico Nacional para el mejor cumplimiento de lo establecido en el ENS –artículo 29 ENS-, adecuando todo ello a la realidad orgánica y funcional de la Diputación de Valencia.

TÍTULO PRELIMINAR

Ámbito de aplicación y disposiciones generales

Capítulo Primero

Disposiciones comunes

Artículo 1. OBJETO

El presente reglamento tiene por objeto definir y regular, en el ámbito de la Diputación de Valencia, la Política de seguridad y de protección de datos de carácter personal aplicable a los sistemas de información que intervengan en el tratamiento de la información que resulte necesaria para el ejercicio de sus competencias.

Artículo 2. DEFINICIONES

A efectos de la presente disposición 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.

• 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.

• 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.

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

• Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

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

• 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.

• Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Artículo 3. ALCANCE

Esta Política se aplica a todos los sistemas de información TIC, así como a aquellos sistemas de información de cualquier naturaleza que traten datos de carácter personal, que sean de la titularidad de la Diputación de Valencia o cuya gestión o responsabilidad tenga encomendada.

Cuando la información cuya titularidad, gestión o responsabilidad corresponda a la Diputación de Valencia se encuentre o trate en entornos ajenos, la Diputación exigirá las mismas garantías y requisitos que las determinadas en la presente Política.

Sin perjuicio de lo anterior, la Diputación aplicará la presente Política en el marco de sus relaciones con las entidades locales de su territorio, 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. 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.

Artículo 4. ÁMBITO SUBJETIVO DE APLICACIÓN

Las presentes disposiciones son de aplicación a todos los departamentos y unidades de la Diputación de Valencia. Los entes u organismos públicos vinculados o dependientes de la Diputación de Valencia adoptarán su propia Política de seguridad y de protección de datos de carácter personal, que deberá adecuarse en la medida de lo posible a las presentes prescripciones.

Capítulo Segundo

Misión y marco legal

Artículo 5. MISIÓN

La Diputación de Valencia es una entidad local de ámbito provincial que tiene las siguientes competencias:

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 mínimos 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. En general, el fomento y la administración de los intereses peculiares de la provincia.

f. Cualesquiera otras que les sean atribuidas por las leyes del Estado y de la Comunidad Autónoma en los diferentes sectores de acción pública.

Artículo 6. MARCO LEGAL

En su calidad de administración pública, la Diputación de Valencia lleva a cabo las competencias que le son propias con pleno sometimiento al Ordenamiento Jurídico, en general, y en especial:

a. A la normativa sobre régimen jurídico local - Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local; Real Decreto Legislativo 781/1986, de 18 de abril, por el que se aprueba el texto refundido de las disposiciones legales vigentes en materia de Régimen Local; Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales; Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales; y Ley 8/2010, de 23 de junio, de la Generalitat, de Régimen Local de la Comunitat Valenciana-

b. A la normativa sobre procedimiento administrativo - Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común-

c. A la normativa sobre contratación administrativa –Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público-

De igual forma, en la utilización de medios tecnológicos para el desarrollo de sus actividades, le son de especial aplicación:

a. La normativa sobre administración electrónica -Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos; Ley 3/2010, de 5 de mayo, de la Generalitat, de Administración Electrónica de la Comunitat Valenciana; 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-

b. La normativa sobre firma electrónica -Ley 59/2003, de 19 de diciembre, de firma electrónica-

c. La normativa sobre protección de datos de carácter personal -Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

TÍTULO PRIMERO

Principios de seguridad TIC y de la protección de datos de carácter personal

Capítulo Primero

Principios comunes

Artículo 7. ACCESO A LA INFORMACIÓN

Los derechos de acceso de los usuarios a la información se regirán por los siguientes principios:

a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones.

b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Artículo 8. CICLO VITAL DE LA INFORMACIÓN

La seguridad y la protección de los datos de carácter personal estarán presentes durante todo el ciclo de vida de la información.

La normativa que desarrolle la presente Política deberá establecer los criterios y requisitos que deberá cumplir la recogida, utilización, publicación, transferencia e intercambio de la información, así como su destrucción o destino final tras cumplir su ciclo de vida útil, con el objetivo de garantizar los anteriores principios de seguridad y de protección de datos de carácter personal.

Artículo 9. DEBER DE SECRETO

Todos los usuarios están obligados a guardar secreto profesional de toda aquella información de la que tengan conocimiento con ocasión del ejercicio de su cargo o actividad profesional. Esta obligación se mantendrá incluso después de haber finalizado la relación con la Diputación de Valencia.

El deber de confidencialidad y secreto profesional se establecerá de forma expresa en todo tipo de relaciones –administrativas, civiles o mercantiles - que impliquen o supongan acceso o tratamiento de la información, incluidos los servicios de simple alojamiento, transporte o soporte técnico.

Artículo 10. MAYOR PROTECCIÓN

Cuando en un mismo sistema de información se traten datos de carácter personal y datos que no tengan esta naturaleza, las medidas de seguridad a implementar, por aplicación simultánea del ENS y del RD 1720/2007, serán las que ofrezcan mayor nivel de protección o de exigencia.

Capítulo Segundo

Principios de seguridad TIC

Artículo 11. PROCESO INTEGRAL

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

En su virtud, cualquier acción dirigida al objetivo de la seguridad debe considerar la interacción de todos los elementos citados, lo cual excluye cualquier actuación puntual o tratamiento coyuntural.

Para evitar que la ignorancia, la falta de organización y coordinación, o instrucciones inadecuadas, sean fuentes de riesgo para la seguridad deberá procederse, en especial, a la concienciación y formación adecuada de las personas que intervienen en el proceso y a sus responsables jerárquicos.

Artículo 12. GESTIÓN BASADA EN RIESGOS

La gestión de la seguridad se apoyará en un proceso continuo de análisis y tratamiento de riesgos. Este proceso deberá mantenerse actualizado de modo permanente.

La gestión de riesgos debe permitir 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.

Todos los sistemas de información sujetos a esta Política de seguridad deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Artículo 13. PREVENCIÓN

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de la evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la presente Política, se deberá:

▪ Autorizar los sistemas antes de entrar en operación.

▪ Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

▪ Solicitar la revisión periódica por parte de terceros con el fin de obtener una

evaluación independiente.

Artículo 14. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte, que lleguen a los responsables regularmente, y cuándo se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Artículo 15. RESPUESTA

Deberán establecerse mecanismos para responder eficazmente a los incidentes de seguridad, designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en los departamentos, y establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

En el ámbito de la Diputación de Valencia deberá crearse un Grupo de Respuesta a Incidentes TIC, cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos de la Corporación.

Artículo 16. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos deberán desarrollarse planes de continuidad de los sistemas TIC.

Capítulo Tercero

Principios de la protección de datos de carácter personal

Artículo 17. CALIDAD DE LOS DATOS

Los datos tienen que ser adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades explícitas y legítimas para los que hayan sido obtenidos por la Diputación de Valencia.

Se velará para que en todo momento los datos sean exactos y puestos al día, de forma que respondan de modo veraz a la situación actual de sus titulares. Se establecerán procedimientos internos para garantizar dicha exactitud y actualidad, con independencia de los derechos de rectificación y cancelación que asisten a los interesados.

Se procederá a la cancelación de oficio de los datos en el momento hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

Artículo 18. INFORMACIÓN Y CONSENTIMIENTO

Todos los medios que sean utilizados para recabar datos de carácter personal deberán proporcionar al interesado la información a que hace referencia el artículo 5 de la LOPD, con las excepciones legalmente contempladas.

Tanto la sede electrónica de la Diputación de Valencia, como cualquier espacio en Internet o tecnologías similares de cuyos contenidos sea responsable la Corporación, contendrá referencia a las políticas y normativas internas sobre protección de datos de carácter personal y, en particular, de los derechos que asisten a los titulares de los datos.

Cuando resulte preceptivo recabar el consentimiento del interesado para la recogida, tratamiento o cesión de sus datos, se utilizarán medios que permitan dejar constancia fehaciente del mismo.

Mediante procedimientos internos se garantizará, previamente a su activación, que los medios y espacios anteriormente citados cumplen debidamente los requisitos establecidos.

Artículo 19. DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

Deberá establecerse un procedimiento interno que asegure el ejercicio de los derechos de acceso, rectificación, cancelación y oposición a los titulares de los datos de carácter personal. Este procedimiento deberá ser común a todos los ficheros de los que sea responsable la Corporación, salvo que las leyes aplicables a determinados ficheros establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos.

Se adoptarán las medidas oportunas para garantizar que el personal de la Corporación que tiene acceso a datos de carácter personal pueda informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

En sede electrónica se habilitará un espacio para ofrecer información a los afectados sobre el contenido de dichos derechos y el procedimiento a seguir para ejercitarlos, así como un canal electrónico para su ejercicio, preferentemente a través del Registro electrónico de la Corporación.

Artículo 20. COMUNICACIÓN DE DATOS

Solo con el consentimiento del interesado o al amparo de alguno de los supuestos recogidos expresamente en la normativa sobre protección de datos personales podrá procederse a la comunicación o cesión de los datos.

Cuando, con soporte legal y sin ser preceptivo el consentimiento del interesado, deba publicarse información considerada como dato de carácter personal, el contenido de dicha publicación será el estrictamente necesario para cumplir el objetivo perseguido, preservando lo máximo posible la intimidad del afectado. De igual forma, se optará por aquellos medios de publicidad que comporten menor nivel de injerencia en el derecho a la intimidad y a la protección de datos de carácter personal.

Siempre que sea posible se procederá a la disociación de la información, aplicando el procedimiento definido en el artículo 3.f) de la LOPD.

Artículo 21. ACCESO A DATOS POR CUENTA DE TERCEROS

Para que la Diputación de Valencia otorgue a terceros el acceso a datos de carácter personal, cuando el citado acceso sea necesario para que dichos terceros presten un servicio a la Diputación, deberá mediar un documento escrito que regule la prestación y en cual se hará constar el contenido establecido en el artículo 12 de la LOPD.

La Diputación de Valencia se abstendrá de actuar en calidad de prestador de servicios a terceros, cuando dicha prestación requiera el acceso a datos de carácter personal, si no media el documento referido en el párrafo anterior, aunque dicho documento no fuera exigido por el tercero receptor del servicio.

TÍTULO SEGUNDO

Organización de la seguridad y de la protección de datos personales

Capítulo Primero

Principios comunes

Artículo 22. RESPONSABILIDAD GENERAL Y ESPECÍFICA

Todos y cada uno de los usuarios de los sistemas de información de la Diputación de Valencia son responsables de la seguridad de los activos informáticos mediante un uso correcto los mismos, así como de la seguridad de la información y de los datos de carácter personal que manejan, siempre de acuerdo con sus atribuciones profesionales.

No obstante, el mantenimiento y gestión de la seguridad de los sistemas de información y de la protección de datos personales van íntimamente ligados al establecimiento de una organización. Dicha organización se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas de información y de la protección de datos personales, y la implantación de una estructura que las soporte.

Artículo 23. ESTRUCTURA ORGANIZATIVA

En los siguientes apartados se especifica la estructura básica de la organización de la seguridad y de la protección de datos personales en los sistemas de información que regirá en la Diputación de Valencia. Las figuras y las responsabilidades a ellas asociadas tienen carácter de mínimos, pudiéndose desarrollar los contenidos a través de la normativa interna de seguridad y de la protección de datos personales, que respetará, en cualquier caso, lo establecido en la presente disposición.

Artículo 24. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre las diferentes figuras de naturaleza unipersonal que componen la estructura organizativa, prevalecerá la decisión del Comité de Seguridad TIC.

En caso de que los citados conflictos afecten a datos de carácter personal, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Capítulo Segundo

Figuras de naturaleza unipersonal

Artículo 25. RESPONSABLE DEL SERVICIO

El responsable del servicio es quien tiene la potestad de establecer las características de un servicio, a los efectos de determinar los requisitos en materia de seguridad y de protección de datos personales.

Al responsable del servicio le corresponde:

- 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 pudiera serle de aplicación.
- la propiedad de los riesgos sobre los servicios.
- aceptar el riesgo residual sobre los servicios que le competen.

Artículo 26. RESPONSABLE DE LA INFORMACIÓN

El responsable de la información es quien tiene la potestad de establecer las características de una información, a los efectos de determinar los requisitos en materia de seguridad y de protección de datos personales.

Al responsable de la información le corresponde:

- la valoración de la información en todas las dimensiones de seguridad –disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad- teniendo en cuenta la naturaleza de dicha información y la normativa que pudiera serle de aplicación.
- 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, aquellas que sean autorizadas por él para acceder a la información.
- la propiedad de los riesgos sobre la información.
- aceptar el riesgo residual sobre la información que le compete.
- autorizar los accesos de los usuarios a la información, respetando los principios de mínimo privilegio y necesidad de conocer establecidos en la presente Política.
- la responsabilidad última del cumplimiento de todas las garantías establecidas por la legislación y la normativa interna de la Corporación, especialmente cuando la información consista en datos de carácter personal.
- la responsabilidad última de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad de la información, cuando no haya atendido debidamente el deber de velar por el cumplimiento de las garantías aludidas en el apartado anterior.

Artículo 27. DISPOSICIONES COMUNES AL RESPONSABLE DEL SERVICIO Y AL RESPONSABLE DE LA INFORMACIÓN

Serán responsables del servicio y de la información el personal directivo –Jefes/as de Servicio, Directores/as, etc- bajo cuya dirección se encuentre el correspondiente servicio y la información.

La responsabilidad de la valoración de la información y de los servicios es exclusivamente del responsable correspondiente. La valoración podrá ser propuesta por el Responsable de Seguridad de los Sistemas de Información, y aprobada por el responsable de la información y del servicio correspondiente si éste la considera adecuada.

La normativa que desarrolle la presente Política establecerá los criterios y los instrumentos que permitan una adecuada valoración de los servicios e informaciones por parte de sus correspondientes responsables.

Artículo 28. RESPONSABLE DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

El Responsable de Seguridad es el máximo responsable de la seguridad de los sistemas de información de la Diputación de Valencia, siendo quien determina las medidas de seguridad que han de ser implantadas y quien las supervisa.

Para el mejor cumplimiento de las funciones relacionadas con las medidas de seguridad implantadas y, especialmente, por razones de complejidad o inmediatez, el Responsable de Seguridad de los Sistemas de Información podrá delegar determinados aspectos de dichos cometidos en otras personas de la organización. En estos supuestos, los diferentes responsables de seguridad delegados actuarán ajustándose estrictamente al contenido de la delegación, la cual recogerá el alcance material y temporal, las obligaciones y responsabilidades de las tareas delegadas. De las posibles delegaciones deberá darse cuenta al Comité de Seguridad TIC.

Serán funciones del Responsable de Seguridad de los Sistemas de Información:

- Actuar como Secretario del Comité de Seguridad TIC.
- Convocar al Comité de Seguridad TIC, recopilando la información pertinente.
- Ser responsable, junto con los diferentes responsables de seguridad delegados, en su caso, de estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que puedan afectar directa o indirectamente a la seguridad de los sistemas de información de la Corporación, debiendo informarse de las consecuencias para las actividades de la Organización, alertando al Comité de Seguridad TIC y proponiendo las acciones oportunas de adecuación al nuevo marco normativo.
- Elaborar las pertinentes Declaraciones de Aplicabilidad de los sistemas de información.
- Llevar a cabo periódicamente auditorías para evaluar el cumplimiento de la normativa sobre seguridad y la efectividad de las medidas adoptadas.
- Ser el responsable de la toma de decisiones día a día entre las reuniones del Comité de Seguridad TIC. Estas decisiones estarán presididas por los principios de unidad de acción y coordinación de actuaciones en general y, en especial, en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres.
- En caso de desastre se incorporará al Grupo de Respuesta a Incidentes TIC y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad de los sistemas de información.

Respecto de las medidas de seguridad en materia de protección de datos personales:

- Definir el Plan Auditor de la organización para los ficheros de datos de carácter personal; analizar los informes de auditoría emanados de dicho Plan y elevar las conclusiones pertinentes al Comité

de Seguridad TIC y a la Dirección de la Corporación, con el fin de adoptar las medidas que pudieran derivarse de dichos informes.

- Impulsar y participar en el diseño de políticas de seguridad para los sistemas de información que contengan datos de carácter personal en el entorno de la Corporación.

- En general, coordinar y controlar las medidas de seguridad implantadas, relacionadas con el tratamiento de datos personales, en el ámbito de la Diputación de Valencia, asumiendo el rol de responsable de seguridad establecido en el RD 1720/2007.

Y cualesquiera otros cometidos que le sean encargados por la presente Política y por la Dirección de la Corporación.

Será Responsable de Seguridad de los Sistemas de Información en el ámbito de la Diputación de Valencia el Jefe de la Unidad Técnica de Protección de Datos, adscrita al Servicio de Informática y Organización.

Artículo 29. RESPONSABLE DE LOS SISTEMAS DE INFORMACIÓN TIC

Corresponderá al Responsable de los Sistemas de Información TIC:

- Desarrollar, operar y mantener los Sistemas de Información TIC durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

- Definir la topología y sistema de gestión de los Sistemas de Información TIC estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

- Acordar la suspensión del manejo de una cierta información o la prestación de un determinado servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con el Responsable de la Información afectada, del Servicio afectado y el Responsable de Seguridad de los Sistemas de Información antes de ser ejecutada.

Será Responsable de los Sistemas de Información TIC en el ámbito de la Diputación de Valencia el Jefe de Servicio de Informática y Organización.

Considerando la complejidad, distribución, separación física de sus elementos o número de usuarios que habitualmente comporta la gestión de los actuales sistemas de información, así como la realidad funcional de quienes han de compaginar las responsabilidades derivadas de la presente disposición con sus competencias habituales, el Responsable de los Sistemas de Información TIC podrá delegar determinados aspectos de sus cometidos en otras personas de la organización. En estos supuestos, los diferentes responsables de sistemas de información delegados actuarán ajustándose estrictamente al contenido de la delegación, la cual recogerá el alcance material y temporal, las obligaciones y responsabilidades de las tareas delegadas. De las posibles delegaciones deberá darse cuenta al Comité de Seguridad TIC.

En ningún caso podrá ser objeto de delegación la competencia para acordar la suspensión del manejo de cierta información o la prestación de un determinado servicio, en los términos citados en el presente artículo.

Artículo 30. ADMINISTRADOR DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN TIC

El Administrador de Seguridad es el responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables a los Sistemas de Información TIC.

Será Administrador de Seguridad de los sistemas de información TIC en el ámbito de la Diputación de Valencia el Jefe de Servicio de Informática y Organización.

El Administrador de Seguridad de los Sistemas de Información TIC podrá delegar determinados aspectos de sus cometidos en otras personas de la organización. En estos supuestos, los diferentes administradores de seguridad delegados actuarán ajustándose estrictamente al contenido de la delegación, la cual recogerá el alcance material y temporal, las obligaciones y responsabilidades de las tareas delegadas. De las posibles delegaciones deberá darse cuenta al Comité de Seguridad TIC.

Artículo 31. RESPONSABLE DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El responsable de protección de datos de carácter personal es el responsable de la coordinación, gestión y control de las acciones necesarias para el debido cumplimiento de la Corporación de la normativa sobre protección de datos personales.

Al responsable de protección de datos de carácter personal le corresponde:

- Centralizar y llevar a cabo la declaración de ficheros y tratamientos de datos de carácter personal de la Corporación ante la Agencia Española de Protección de Datos (AEPD) o, en su caso, ante la autoridad de control de ámbito autonómico.

- Mantener actualizado el inventario de ficheros de datos de carácter personal de la Diputación de Valencia, y revisar periódicamente la concordancia y consistencia del mismo.

- La recepción, estudio, evaluación y propuesta de resolución de reclamaciones y solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición, relacionadas con los ficheros o tratamientos de datos personales de la Corporación, y de denuncias ante la AEPD o autoridad de control de ámbito autonómico.

- Llevar a cabo auditorías internas en relación con tratamientos de datos de carácter personal, procediendo a la evaluación y propuesta de medidas para el ajuste a la normativa vigente en la materia.

- El diseño y elaboración de formularios, guías, manuales y protocolos de actuación en el seno de la Corporación que proporcionen o faciliten el cumplimiento de la legalidad sobre protección de datos personales.

- Evacuar todo tipo de informes y/o estudios técnicos que sobre el particular puedan solicitarse en el entorno de la Corporación y, en general, proporcionar asesoramiento al conjunto de departamentos de la Corporación.

- La implementación, actualización y custodia del Documento de Seguridad de la Diputación de Valencia.

- Coordinar las relaciones institucionales en materia de protección de datos personales entre la Corporación y las autoridades de protección de datos, y con otras administraciones, entes, organismos o instituciones, públicas o privadas, el intercambio de información en la materia con el resto de administraciones públicas, y la promoción de suscripción de convenios de colaboración, acuerdos o programas que resulten beneficiosos para la Corporación y/o para los municipios de la provincia.

Será Responsable de protección de datos de carácter personal en el ámbito de la Diputación de Valencia la Unidad Técnica de Protección de Datos, adscrita al Servicio de Informática y Organización.

Capítulo Tercero

Órganos de carácter colegiado

Artículo 32. COMITÉ DE SEGURIDAD TIC

Es el órgano que gestiona y coordina la Seguridad de los sistemas de información TIC a nivel de organización.

Se crea el Comité de Seguridad TIC de la Diputación de Valencia, como un órgano colegiado de carácter horizontal, que se regirá en su funcionamiento por esta disposición y, en lo no previsto en ella, será de aplicación supletoria la normativa reguladora de los órganos colegiados contenida en el Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

El Comité de Seguridad TIC se reunirá con carácter ordinario, al menos, una vez por semestre. Por razones de urgencia podrá reunirse siempre que la Presidencia del Comité lo estime conveniente. Las reuniones tendrán lugar dentro de la jornada de trabajo establecida reglamentariamente.

El Comité podrá acordar la constitución de comisiones delegadas de trabajo, para tratar temas, elaborar estudios o informes, o llevar a cabo cualquier otra gestión que por su especificidad o complejidad técnica así se considere.

El Comité podrá regular su propio régimen de funcionamiento, el cual deberá respetar, en cualquier caso, lo dispuesto en la presente disposición y la normativa que resulte de aplicación.

El Comité esta compuesto por:

- El Jefe de Servicio de Informática y Organización, que asumirá la Presidencia del Comité.
- Una persona designada por el/la Diputado/a delegado/a del área de Administración General, que ostentará la Vicepresidencia del Comité.
- El Responsable de Seguridad de los Sistemas de Información, que actuará como Secretario del Comité.
- Los diferentes Responsables de Sistemas de Información, Responsables de seguridad y Administradores de seguridad delegados.

El Comité desempeñará las siguientes funciones:

• Coordinar todas las funciones de seguridad de los sistemas de información TIC de la Corporación.

• Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.

• Proponer las modificaciones o revisiones de la presente Política de Seguridad que considere oportunas, dando traslado de las mismas al Pleno de la Corporación para su toma en consideración.

• Recabar del Responsable de Seguridad informes regulares del estado de la seguridad de la Organización y de los posibles incidentes. Estos informes se consolidan y resumen para la Dirección de la Corporación.

• Coordinar y dar respuesta a las inquietudes transmitidas a través del Responsable de Seguridad.

• Dinamizar la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas de información, promoviendo inversiones de carácter horizontal.

• El Comité nombrará entre sus miembros el Grupo de Respuesta a Incidentes TIC indicado en el artículo 15 de la presente disposición.

Y cualesquiera otros cometidos que les sean encargados por la presente Política y por la Dirección de la Corporación.

El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones.

TÍTULO TERCERO

Disposiciones relativas al personal

Capítulo Primero

Obligaciones y responsabilidades

Artículo 33. OBLIGACIONES DEL PERSONAL

Todos los miembros de la Diputación de Valencia tienen la obligación de conocer y cumplir esta Política de seguridad y de protección de datos de carácter personal y la normativa que la desarrolle, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

La normativa interna que desarrolle la presente Política contendrá las especificaciones necesarias para que todo el personal conozca perfectamente las obligaciones que, en atención a las funciones que desempeña, le son exigibles en el marco de la presente disposición.

Artículo 34. TERCERAS PARTES

Cuando la Diputación de Valencia preste servicios a otros organismos o maneje información de otros organismos, se les hará participes de esta Política, estableciéndose canales para reporte y coordinación de los respectivos Comités de Seguridad TIC, en su caso, y procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Diputación de Valencia utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política y de la normativa de seguridad y de protección de datos personales que ataña a dichos servicios o información. Dichos terceros quedarán sujetos a las obligaciones establecidas en la citada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad y protección de datos personales, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se recabará un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

Todos los instrumentos mediante los que se regulen las relaciones entre la Diputación de Valencia y terceros –convenios, contratos, pliegos técnicos, etc- contendrán cumplida referencia de esta Política y de las obligaciones y responsabilidades de las partes en materia de seguridad de la información y protección de datos de carácter personal.

Artículo 35. INCUMPLIMIENTOS

A los incumplimientos de la presente Política, así como de la normativa que la desarrolle, cometidos por el personal al servicio de la Diputación de Valencia les será de aplicación el régimen disciplinario legalmente establecido por la normativa vigente.

Cuando los incumplimientos fuesen cometidos por terceros, sobre los que recaiga la obligación de cumplimiento en virtud de contrato o cualquier otro tipo de relación acordada, la responsabilidad les será exigida en los términos previstos en los instrumentos que regulen dichas relaciones y por la normativa legal que pueda resultar de aplicación.

Capítulo Segundo

Recursos formativos

Artículo 36. FORMACIÓN Y CONCIENCIACIÓN

La Diputación de Valencia garantizará la formación y concienciación a todos sus empleados públicos a través del Servicio de Formación incluyendo las acciones formativas necesarias en los planes de formación interna. Las personas con responsabilidad en el uso, operación o administración de los sistemas de información recibirán la formación adecuada para el manejo seguro de los sistemas y para un adecuado tratamiento de los datos de carácter personal, en la medida en que la necesite para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto o de responsabilidad del mismo.

Al personal con responsabilidades muy especificas en materia de seguridad o de protección de datos de carácter personal, se les facilitará de modo preferente la asistencia a actividades formativas que tengan relación directa con dichas responsabilidades.

La asistencia y cumplimentación de estas acciones formativas tiene carácter obligatorio, salvo circunstancias excepcionales debidamente acreditadas. El personal que no pueda concurrir a las mismas por estos supuestos será incluido con carácter preferente en siguientes convocatorias.

El Servicio de Informática, a través de la Unidad Técnica de Protección de Datos, colaborará con el Servicio de Formación en el diseño y elaboración de las acciones formativas necesarias, las cuales una vez elaboradas se trasladarán al Comité de Seguridad TIC para su aprobación.

TÍTULO CUARTO

Desarrollo y modificación de la Política de Seguridad y de Protección de Datos de Carácter Personal

Capítulo Primero

Instrumentos de desarrollo

Artículo 37. DESARROLLO NORMATIVO

El desarrollo de la presente Política se llevará a cabo mediante instrumentos pertenecientes a tres niveles, denominados A, B y C. Cuando se apruebe un instrumento de desarrollo deberá especificarse el nivel al que pertenece.

Artículo 37.1. NIVEL A

Pertenecen al nivel A las denominadas Normas de Seguridad y de Protección de Datos de Carácter Personal.

Están conformadas por el conjunto de reglas y directrices de carácter obligatorio que desarrollan directamente el contenido de la presente Política o trasladan al orden interno, mediante las correspondientes normas, el cumplimiento de la normativa legal aplicable en la materia.

Se integran en este nivel:

- El Documento de Seguridad (artículos 88 y 105 del RDLOPD)
- La Normativa de Seguridad (apartado 3.2 org.2 del ENS)
- Las Normas de Seguridad (artículo 89.2 del RDLOPD)
- La Normativa de Protección de Datos de Carácter Personal

De igual modo, se integrará en este nivel cualquier otra normativa interna que el órgano o autoridad competente, según lo establecido

en el artículo 39.1 de la presente disposición, considere necesaria para cumplir los objetivos expuestos en el presente artículo.

Artículo 37.2. NIVEL B

Pertenecen al nivel B los denominados Procedimientos de Seguridad y de Protección de Datos de Carácter Personal.

Están constituidos por el conjunto de procedimientos técnicos de carácter obligatorio orientados a resolver las tareas, procesos de trabajo o modos de actuación considerados más relevantes atendiendo al perjuicio que causaría una actuación inadecuada de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información, o de protección de datos de carácter personal, o por venir impuestos por la legislación aplicable.

Se integran en este nivel:

- Los Procedimientos de Seguridad (apartado 3.3 org.3 del ENS)
- El Procedimiento para el control del acceso fisico a instalaciones (artículo 17 del ENS)
- El Procedimiento para asegurar la recuperación y conservación a largo plazo de los documentos electrónicos (artículo 21.2 del ENS)
- El Procedimiento para la declaración de ficheros que contengan datos de carácter personal
- El Procedimiento de realización de copias de respaldo y de recuperación de los datos (artículo 94 del RDLOPD)
- Los Procedimientos para el archivo de soportes y documentos (artículo 106 del RDLOPD)
- El Procedimiento para atender el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (artículo 25.6 del RDLOPD)
- El Procedimiento de notificación, gestión y respuesta ante las incidencias (artículo 90 del RDLOPD y 4.3.7 op.exp.7 del ENS)
- El Procedimiento de asignación, distribución y almacenamiento de contraseñas (artículo 93.3 del RDLOPD)
- Los Procedimientos para el control de las medidas de seguridad y de auditoría (artículo 88.4.b del RDLOPD y anexo III del ENS)

De igual modo, se integrará en este nivel cualquier otro procedimiento que el órgano o autoridad competente, según lo establecido en el artículo 39.1 de la presente disposición, considere necesario para cumplir los objetivos expuestos en el presente artículo.

Artículo 37.3. NIVEL C

Pertenecen al nivel C las denominadas Guías de Seguridad y de Protección de Datos de Carácter Personal.

Están conformadas por el conjunto de recomendaciones y especificaciones técnicas y jurídicas, de carácter esclarecedor u orientativo, tendentes a ilustrar con mayor detalle aspectos concretos de la seguridad y la protección de datos personales. Su objetivo último es ayudar a la correcta aplicación de las normas y procedimientos recogidos en los niveles A y B, o complementar su contenido, así como contribuir a una mejor información y difusión de las mismas.

Se integran en este nivel:

- Las Guías técnicas de seguridad
- Los Manuales, informes, monografías, cuadernos, estudios técnicos y recomendaciones

Artículo 38. DOCUMENTO DE SEGURIDAD

El tratamiento de datos de carácter personal comporta la obligación de elaborar el Documento de Seguridad. El Documento de Seguridad de la Diputación de Valencia, al que tendrán acceso sólo las personas autorizadas, recogerá los ficheros o tratamientos afectados y los responsables correspondientes, así como las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que sean de obligado cumplimiento para el personal con acceso a los sistemas de información.

Todos los sistemas de información de la Diputación de Valencia se ajustarán a los niveles de seguridad requeridos por la normativa en función de la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

Las medidas de seguridad contempladas en el Documento de Seguridad tendrán en consideración lo dispuesto en el artículo 10 de la presente disposición –principio de mayor protección- cuando deban aplicarse simultáneamente con las derivadas del cumplimiento del ENS.

En cualquier caso, el contenido del Documento de Seguridad deberá armonizarse con el conjunto de la normativa interna elaborada en desarrollo de la presente Política.

Capítulo Segundo

Competencias de desarrollo

Artículo 39. ASIGNACIÓN DE COMPETENCIAS DE DESARROLLO

Las competencias para la elaboración y aprobación de los instrumentos de desarrollo de la presente Política se asignan en función de los diferentes niveles en que se encuadran, de conformidad con el artículo 37 de la presente disposición.

Artículo 39.1. INSTRUMENTOS DE NIVEL A y B

La competencia para la aprobación de las Normas de Seguridad y de Protección de Datos de Carácter Personal, así como de los Procedimientos de Seguridad y de Protección de Datos de Carácter Personal corresponde al Presidente de la Diputación de Valencia o Diputado/a en quien éste delegue.

El Comité de Seguridad TIC, el Responsable de Seguridad de los Sistemas de Información y la Unidad Técnica de Protección de Datos, cada cual en el marco de sus competencias, formularán las propuestas que consideren adecuadas.

Artículo 39.2. INSTRUMENTOS DE NIVEL C

Corresponde al Comité de Seguridad TIC, al Responsable de Seguridad de los Sistemas de Información y a la Unidad Técnica de Protección de Datos, cada cual en el marco de sus competencias, la elaboración de las Guías de Seguridad y de Protección de Datos de Carácter Personal.

Capítulo Tercero

Modificación de la Política

Artículo 40. ACTUALIZACIÓN PERMANENTE

La presente Política deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de Administración Electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a las previsiones legales que pudiesen afectarle.

Artículo 41. PROCEDIMIENTO PARA LA MODIFICACIÓN

Las propuestas de las sucesivas revisiones de la presente Política se elaborarán por el Comité de Seguridad TIC y se trasladarán, a través del Diputado/a Delegado/a de Modernización, al Pleno de la Corporación, único órgano competente para acordar cualquier modificación de dicha Política.

DISPOSICION DEROGATORIA

Única. DEROGACIÓN NORMATIVA

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en la presente disposición.

DISPOSICION TRANSITORIA

Única. NORMATIVA INTERNA VIGENTE

En tanto la Política prevista en la presente disposición no sea objeto de desarrollo continuará vigente, con carácter subsidiario, la Normativa y Procedimientos de Trabajo en relación con el tratamiento de datos de carácter personal recogida en el Decreto 3032, de 3 de mayo de 2011, del Presidente de la Diputación de Valencia.

DISPOSICIONES FINALES

Primera. CONSTITUCIÓN DEL COMITÉ DE SEGURIDAD TIC

Deberá procederse a la constitución del Comité de Seguridad TIC en un plazo no superior a tres meses desde la entrada en vigor de la presente disposición.

Segunda. DESARROLLO NORMATIVO

El desarrollo de la presente Política, a través de los instrumentos establecidos en el artículo 37.1, deberá llevarse a cabo a la mayor brevedad posible, sin que en ningún caso se supere el plazo del 30 de enero de 2014.

Cuando se trate de los instrumentos contemplados en el artículo 37.2, se intentará tener aprobados dentro del plazo citado anteriormente aquellos procedimientos considerados como críticos para la seguridad de los sistemas de información afectados.

Tercera. POLITICAS DE ÁMBITO MUNICIPAL

La Diputación de Valencia podrá elaborar, al amparo del párrafo segundo del artículo 11.2 ENS, Políticas de Seguridad y de Protección

de Datos Personales comunes para los municipios de la provincia que deseen adherirse a ellas.

En la configuración de dichas Políticas se tendrán en consideración aquellos elementos que resulten homogéneos a la hora de determinar el conjunto de sus destinatarios, tales como la población, el nivel de infraestructuras y servicios TIC, los recursos organizativos, el grado de dependencia de la asistencia de la Diputación o la posible transferencia de competencias del ámbito municipal al provincial.

Cuarta. ENTRADA EN VIGOR

La presente disposición entrará en vigor a los 15 días hábiles desde la fecha de su publicación en el BOP.

2013/18814