POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN.

1.1. Misión y servicios prestados.

La Diputación de Alicante, cuyo nacimiento data del 15 de mayo de 1822, es un ente local volcado en la asistencia a los municipios para facilitar la gestión de sus competencias. Sirve a las corporaciones locales, y a través de ellas a todos los habitantes de la provincia de Alicante.

Entre otras, son competencias propias de la Diputación las siguientes:

1. 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.
2. La asistencia y la cooperación jurídica, económica y técnica a los Municipios, especialmente a los de menor capacidad económica y de gestión.
3. La prestación de servicios públicos de carácter supramunicipal y, en su caso, supracomarcal.
4. 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.
5. En general, el fomento y la administración de los intereses peculiares de la provincia.

2. JUSTIFICACIÓN POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

2.1. Necesidad de seguridad en los sistemas.

Para el cumplimiento de su Misión, la prestación de los Servicios identificados y el cumplimiento de sus objetivos, la Diputación de Alicante depende de los llamados 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 la información 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. Esto implica se deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (en adelante ENS), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados

Por ello el ENS (Real Decreto 3/2010, de 8 de enero), en su artículo 11 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".

2.2. Requisitos de seguridad en los Departamentos.

Todas las Áreas de la Diputación deben aplicar las medidas mínimas de seguridad exigidas por el ENS, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando

por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 7 del ENS.

3. MARCO NORMATIVO.

3.1. Responsabilidades derivadas de normativas.

La Ley 11/2007, de 22 de junio, de acceso de los ciudadanos a los servicios públicos, en su artículo 42.2, establece sobre el ENS, como uno de sus principios, que se debe disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos.

La Ley 3/2010, de 5 de mayo, de la Generalitat, de Administración Electrónica de la Comunitat Valenciana, establece en su artículo 37 que la utilización de técnicas electrónicas, informáticas y telemáticas por parte de las administraciones públicas de la Comunitat Valenciana deberá incorporar las medidas de seguridad, calidad y de control necesarias que garanticen la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información.

El Real Decreto 3/2010, de 8 de enero, de desarrollo del ENS, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.

Así mismo, la Ley 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, la dota de coherencia en todo lo relacionado con la trasposición de la directiva 95/46/CE del Parlamento Europeo y desarrolla aquellos aspectos novedosos o en que la experiencia ha aconsejado un cierto grado de precisión.

4. ORGANIZACIÓN DE LA SEGURIDAD.

4.1. Comité: funciones y responsabilidades.

El Comité de Seguridad de la Información, es el órgano que coordina la Seguridad de la Información a nivel de la Diputación de Alicante.

Estará constituido por el Jefe del departamento de Informática, el Jefe de la Unidad de Sistemas, el Administrador de Seguridad Informática y por representantes de las áreas afectadas por el ENS

Los miembros del Comité de Seguridad de la Información, serán nombrados por la Presidencia de esta Corporación.

Sus funciones son las siguientes:

- *Responsabilidades derivadas del tratamiento de datos de carácter personal.*
- *Atender las inquietudes de la Corporación y de los diferentes departamentos.*
- *Informar regularmente del estado de la seguridad de la información a la Alta Dirección.*
- *Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.*
- *Elaborar la estrategia de evolución de la Diputación de Alicante en lo que respecta a la seguridad de la información.*
- *Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.*
- *Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.*
- *Aprobar la normativa de seguridad de la información.*
- *Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.*
- *Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.*
- *Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones*

respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- 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. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

En caso de ocurrencia de incidentes de seguridad de la información aprobará el Plan de Mejora de la Seguridad.

El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

El Responsable de la Seguridad de la Información es el secretario del Comité de Seguridad de la Información y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.

- *Es responsable de la ejecución directa o delegada de las decisiones del Comité.*

4.2. Roles: funciones y responsabilidades.

La Política de Seguridad, según requiere el Anexo II del ENS en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

Se establecen los siguientes roles en la organización relacionados con la Seguridad de la Información.

4.2.1. Responsable de la Información.

Estas funciones serán asumidas por, la Presidencia o diputado en quien delegue, que entiende la misión de la Diputación de Alicante., determina los objetivos que se propone alcanzar y responde que se alcancen.

- *Funciones asociadas.*

Sus funciones serán las siguientes:

- *Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.*
- *Es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.*
- *Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.*
- *Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del ENS.*
- *Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.*

- *Compatibilidad con otros responsables.*

Este rol podrá coincidir:

- con el de Responsable de Servicio,
- y con el de Responsable de Fichero requerido por la Ley

15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Este rol no podrá coincidir:

- con el de Responsable de Seguridad,
- ni con el de Responsable de Sistema,
- ni con el de Administrador de la Seguridad del Sistema.

4.2.2. Responsable del Servicio.

Estas funciones serán asumidas por, la Presidencia o diputado en quien delegue, que entiende qué hace cada departamento, y cómo los departamentos se coordinan entre sí para alcanzar los objetivos marcados por la Dirección.

- *Funciones asociadas.*

Sus funciones serán las siguientes:

- Tiene la potestad de determinar los niveles de seguridad de los servicios dentro del marco establecido en el Anexo I del ENS.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- Es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios que gestiona.
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que éstos podrán heredarse, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

- *Compatibilidad con otros responsables.*

Este rol podrá coincidir:

- con el del Responsable de la Información,
- y con el de Responsable de Fichero requerido por la Ley

15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Este rol no podrá coincidir:

- con el de Responsable de Seguridad,
- con el de Responsable de Sistema,
- ni con el de Administrador de la Seguridad del Sistema.

4.2.3. Responsable de Seguridad de la Información.

El rol de Responsable de Seguridad de la Información, será desempeñado por el Jefe del Departamento de Informática.

Se nombrará formalmente como tal a una única persona en la organización.

Se podrá delegar parte de sus funciones en otras personas.

- *Funciones asociadas.*

Sus funciones serán las siguientes:

- *Informará directamente al Comité de Seguridad de la Información.*
- *Actuará como Secretario del Comité de Seguridad de la Información.*
- *Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.*
- *Pertenecerá al Comité de Seguridad de la información, para coordinar las necesidades de Seguridad de la Información en el marco del resto de necesidades de Seguridad Corporativa.*
- *Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.*
- *Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.*
- *Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.*
- *Realizará el Análisis de Riesgos.*

- *Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.*
- *Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.*
- *Coordinará la elaboración de la Documentación de Seguridad del Sistema.*
- *Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por Dirección.*
- *Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.*
- *Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.*
- *Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).*
- *Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.*
- *Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.*
- *Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.*
- *Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.*

- *En caso de ocurrencia de incidentes de seguridad de la información analizará y propondrá salvaguardas que prevengan incidentes similares en un futuro.*

- *Compatibilidad con otros roles.*

Este rol no podrá coincidir:

- con el de Responsable de la Información,
- con el de Responsable del Servicio,
- con el de Responsable del Sistema,
- y con el de Administrador de Seguridad del Sistema.

- *Delegación de funciones.*

Para determinados Sistemas de Información en los que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones del Responsable de la Seguridad, se podrán designar los Responsables de Seguridad Delegados que se consideren necesarios.

La designación corresponde al Responsable de la Seguridad. Por medio de la designación de Delegados, se delegan funciones. La responsabilidad final seguirá recayendo sobre el Responsable de la Seguridad.

Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad, pudiendo ser, por ejemplo, la seguridad de sistemas de información concretos o de sistemas de información horizontales.

Cada Responsable de Seguridad Delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.

4.2.4. Responsable del Sistema.

El rol de Responsable del Sistema será desempeñado por el Jefe de la Unidad de Sistemas.

Se nombrará formalmente como tal a una única persona en la organización.

Se podrá delegar parte de sus funciones en otras personas

- *Funciones asociadas.*

Sus funciones serán las siguientes:

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

- Definir la topología y sistema de gestión del Sistema de Información 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.

- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta 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 debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.

- Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.

- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.

- Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.

- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.

- Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

En caso de ocurrencia de incidentes de seguridad de la información:

- Planificará la implantación de las salvaguardas en el sistema.

- Ejecutará el plan de seguridad aprobado.

- *Compatibilidad con otros responsables.*

Este rol no podrá coincidir:

- con el de Responsable de Información,
- con el de Responsable de Servicio,
- con el de Responsable de Seguridad de la Información,
- ni con de Administrador de Seguridad del Sistema.

4.2.5. Administrador de la seguridad del Sistema.

Corresponde al nivel de un funcionario cualificado en seguridad informática de sistemas.

Podrá nombrarse formalmente como tal varias personas para cada Sistema.

Será propuesto por el Responsable del Sistema, a quien reportará en todo lo relacionado con seguridad de la información.

- *Funciones asociadas.*

Sus funciones serán las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la Política de Seguridad establecida por la Organización.
- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.

- *Aprobar los cambios en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.*
- *Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.*
- *Monitorizar el estado de la seguridad del sistema.*

En caso de ocurrencia de incidentes de seguridad de la información:

- *Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.*
- *Ejecutar el plan de seguridad aprobado.*
- *Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.*
- *Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).*
- *Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).*
- *Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.*
- *Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.*

- *Compatibilidad con otros responsables.*

Este rol no podrá coincidir:

- con el de Responsable de Información,
- con el de Responsable de Servicio,
- ni con el de Responsable de Seguridad Corporativa o de la Información.

Este rol podrá coincidir con el de Responsable del Sistema.

- *Delegación de funciones.*

En determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo sus funciones, se podrán designar Administradores de Seguridad del Sistema Delegados.

Los Administradores de Seguridad del Sistema Delegados serán responsables, en su ámbito, de aquellas acciones que delegue el Administrador de Seguridad del Sistema relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

El Administrador de Seguridad del Sistema Delegado será designado a solicitud del Administrador de Seguridad del Sistema, del que dependerá funcionalmente.

Su identidad aparecerá reflejada en la documentación de seguridad del sistema de información.

4.2.6. Gestión de personal.

Los responsables de gestión del personal se ajustarán a lo establecido por el ENS en materia de personal de forma análoga a lo establecido en los puntos anteriores.

Los responsables de personal implantarán las medidas de seguridad que les competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informarán a éste de su grado de implantación, eficacia e incidentes.

4.3. Jerarquía en el proceso de decisiones y mecanismos de coordinación.

Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el Comité de Seguridad de la Información da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la Política de Seguridad aprobada para la Organización.

El Administrador de Seguridad reporta al Responsable del

Sistema:

- *Incidentes relativos a la seguridad del sistema.*
- *Acciones de configuración, actualización o corrección.*

El Responsable del Sistema informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.

El Responsable del Sistema informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

El Responsable del Sistema reporta al Responsable de la Seguridad:

- *Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.*
- *Resumen consolidado de los incidentes de seguridad.*
- *Medidas de la eficacia de las medidas de protección que se deben implantar.*

El Responsable de la Seguridad informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

El Responsable de la Seguridad informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

Cuando exista un Comité de Seguridad de la Información, el Responsable de la Seguridad reporta a dicho Comité como secretario:

- *Resumen consolidado de actuaciones en materia de seguridad*
- *Resumen consolidado de incidentes relativos a la seguridad de la información*
- *Estado de la seguridad del sistema, en particular del*

riesgo residual al que el sistema está expuesto

Cuando no exista un Comité de Seguridad de la Información, el Responsable de la Seguridad reporta directamente a la Dirección de la Organización:

- *Resumen consolidado de actuaciones en materia de seguridad.*
- *Resumen consolidado de incidentes relativos a la seguridad de la información.*
- *Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.*

4.4. Procedimientos de designación de personas.

La Presidencia de la Diputación de Alicante designará formalmente mediante su publicación en el Boletín Oficial correspondiente:

- *Al Responsable de la Información, en caso de no asumir directamente este rol.*
- *Al Responsable del Servicio, en caso de no asumir directamente este rol.*
- *Al Responsable de la Seguridad, que debe reportar directamente a la Dirección o, cuando existan, a los Comités de Seguridad de la Información y Seguridad Corporativa.*
- *Al Responsable del Sistema, que debe reportar directamente a la Dirección o, cuando existan, a los Comités de Seguridad de la Información y Seguridad Corporativa.*

La Presidencia de la Diputación de Alicante designará a la persona Responsable del Sistema:

- *A propuesta del Responsable de la Información tratada, cuando el Sistema de información trate una única información.*
- *A propuesta del Responsable del Servicio prestado, cuando el Sistema de información preste un único servicio.*
- *Directamente, cuando el Sistema de información trata diferentes informaciones o presta diferentes servicios, oídos los responsables de las informaciones y los servicios afectados.*

La Presidencia de la Diputación de Alicante designará al Administrador de Seguridad del Sistema a propuesta del Responsable del Sistema.

4.5. Relación con el documento de seguridad y protección de datos personales.

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. El Documento de Seguridad de la Diputación de Alicante detalla los ficheros afectados y los responsables correspondientes, así como las medidas adoptadas en el marco del Real Decreto 1720/2007 y normativa complementaria. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

5. GESTIÓN DE RIESGOS.

5.1. Justificación.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el ENS, según lo previsto en el artículo 6 del mismo.

5.2. Criterios de evaluación de riesgos.

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.

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas. En concreto, la Diputación efectuará un análisis y evaluación de riesgos basándose en la metodología MAGERIT V.2 elaborado por el Ministerio de Política Territorial y

Administración Pública.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

5.3. Directrices de tratamiento.

El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

5.4. Proceso de aceptación del riesgo residual.

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.

Los niveles de Riesgo residuales esperados sobre cada Información o Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por los responsables correspondientes.

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

5.5. Necesidad de realizar o actualizar las evaluaciones de riesgos.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el artículo 9 del ENS. Este análisis se repetirá:

- *Regularmente, al menos una vez al año.*
- *Cuando se produzcan cambios significativos en la*

información manejada.

- *Cuando se produzcan cambios significativos en los servicios prestados.*
- *Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.*
- *Cuando ocurra un incidente grave de seguridad.*
- *Cuando se reporten vulnerabilidades graves.*

6. GESTIÓN DE INCIDENTES DE SEGURIDAD.

6.1. Prevención de incidentes.

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 una 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 Política, los departamentos deben:

- *Autorizar los sistemas antes de entrar en operación.*
- *Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.*

6.2. Monitorización y detección de incidentes.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una disminución hasta el cese del nivel de prestación, 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 puedan informar a los responsables tanto regularmente como cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

6.3. Respuesta ante incidentes.

Las distintas Áreas de esta Diputación deben:

- *Establecer mecanismos para responder eficazmente a los incidentes de seguridad.*
- *Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.*
- *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).*

6.4. Recuperación ante incidentes y planes de continuidad.

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

7. OBLIGACIONES DEL PERSONAL.

Todo el personal de la Diputación de Alicante, tanto empleados públicos como políticos, tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los mismos.

Todo el personal de la Diputación de Alicante atenderá a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

El personal con responsabilidad en el uso, operación o administración de sistemas TIC recibirá formación para el manejo seguro de los sistemas 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 como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

8. TERCERAS PARTES.

Cuando la Diputación de Alicante preste servicios o maneje información de otras entidades, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios externos o se ceda información a entidades o empresas, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta 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 ajeno a esta Diputación de Alicante que vaya a manejar la información está adecuadamente concienciado en materia de seguridad, 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 requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

9. DOCUMENTACIÓN COMPLEMENTARIA.

La Política de Seguridad de la Información se cumplimentará con documentos más precisos que ayudan a llevar a cabo lo propuesto. Para ello se utilizarán:

- *Normas de seguridad (*security standards*).*
- *Guías de seguridad (*security guides*).*
- *Procedimientos de seguridad (*security procedures*).*

Las normas *uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.*

Las guías *tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. De igual manera, las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.*

Los procedimientos [operativos] de seguridad *afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.*

10. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 11 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

11. POLÍTICAS RELACIONADAS.

Esta Política de Seguridad de la Información complementa las Políticas de Seguridad corporativas, detallando las medidas a adoptar sobre Sistemas de Información.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

ANEXO A. GLOSARIO DE TÉRMINOS.

Análisis de riesgos

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

Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Gestión de incidentes

Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del Sistema de Información.

Información

Es cualquier conjunto de datos que tienen significado. El Esquema Nacional de Seguridad se limita a valorar aquellos tipos de información que son relevantes para el proceso administrativo y pueden ser tratados en algún servicio afecto a la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos. Por ejemplo, datos médicos, fiscales, administrativos, contrataciones, resoluciones, notificaciones, etc. En general, cabe esperar que estos tipos de información estén identificados en algún tipo de ordenamiento general o particular del organismo, lo que les confiere entidad propia e implica unos deberes de la administración respecto del tratamiento de dicho tipo de información.

Política de seguridad

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Principios básicos de seguridad

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que se encarga de la explotación del sistema de información.

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

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.

ANEXO B. GLOSARIO DE ABREVIATURAS.

ENS *Esquema Nacional de Seguridad*

TIC *Tecnologías de la Información y las Comunicaciones*

ANEXO C. REFERENCIAS

CCN-STIC-402
Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.

CCN-STIC-801
ENS - Responsables y Funciones. 2010.

Ley 11/2007
Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE de 23 de junio de 2007.

Ley 15/1999
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 14 de diciembre de 1999.

RD 1720/2007
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. BOE de 19 de enero de 2008.

RD 3/2010
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. BOE de 29 de enero de 2010.