


# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DIPUTACIÓ DE CASTELLÓ




DIPUTACIÓ  
D E  
CASTELLÓ


 <b>DIPUTACIÓN D E CASTELLÓN</b>	Política de Seguridad		<b>DOC-ENS-010</b>
	ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN		
	Nº edición: 01	Nº revisión: 06	Página 2 de 34

## ÍNDICE

<b>1. INTRODUCCIÓN.....</b>	<b>4</b>
<b>1.1. JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.....</b>	<b>4</b>
<b>1.2. MISIÓN Y SERVICIOS PRESTADOS.....</b>	<b>4</b>
<b>2. MARCO NORMATIVO.....</b>	<b>6</b>
<b>3. ORGANIZACIÓN DE LA SEGURIDAD.....</b>	<b>7</b>
<b>3.1. definición de Roles.....</b>	<b>7</b>
<b>A. Responsable de la Información.....</b>	<b>7</b>
<b>B. Responsable del Servicio.....</b>	<b>7</b>
<b>C. Responsable de Seguridad de la Información.....</b>	<b>8</b>
<b>D. Responsable del Sistema.....</b>	<b>9</b>
<b>E. Administrador de la Seguridad del Sistema.....</b>	<b>9</b>
<b>F. Responsable de Seguridad Física.....</b>	<b>10</b>
<b>G. Responsable de Gestión de Personal.....</b>	<b>10</b>
<b>H. Responsable Técnico.....</b>	<b>10</b>
<b>3.2. roles relacionados con continuidad del servicio.....</b>	<b>11</b>
<b>3.2.1 Comité de Crisis.....</b>	<b>11</b>
<b>3.2.2. Equipo de recuperación.....</b>	<b>11</b>
<b>3.3. Comité de Seguridad de la información.....</b>	<b>12</b>
<b>3.4. jerarquía en el proceso de decisiones y mecanismos de coordinación.....</b>	<b>14</b>
<b>3.5. procedimientos de designación de personas.....</b>	<b>15</b>
<b>4. FIGURAS VINCULADAS A PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL</b>	<b>16</b>
<b>4.1. INTRODUCCIÓN.....</b>	<b>16</b>
<b>4.2. FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO.....</b>	<b>16</b>
<b>4.3. FUNCIONES Y OBLIGACIONES DEL DELEGADO DE PROTECCIÓN DE DATOS</b>	<b>17</b>
<b>4.4. FUNCIONES Y OBLIGACIONES DE USUARIOS CON ACCESO A DATOS.....</b>	<b>20</b>
<b>4.5. FUNCIONES Y OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO.....</b>	<b>21</b>
<b>5. GESTIÓN DE RIESGOS.....</b>	<b>23</b>
<b>5.1. justificación.....</b>	<b>23</b>
<b>5.2. criterios de evaluación de riesgos.....</b>	<b>23</b>
<b>5.3. directrices de tratamiento.....</b>	<b>23</b>

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 3 de 34

<b>5.4.</b>	<b>proceso de aceptación del riesgo residual.....</b>	<b>23</b>
<b>5.5.</b>	<b>necesidad de realizar o actualizar las evaluaciones de riesgos.....</b>	<b>24</b>
<b>5.6.</b>	<b>EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE LOS DATOS SUJETAS AL RGPD.....</b>	<b>24</b>
<b>6.</b>	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD.....</b>	<b>26</b>
<b>6.1.</b>	<b>Prevención de incidentes.....</b>	<b>26</b>
<b>6.2.</b>	<b>monitorización y detección de incidentes.....</b>	<b>26</b>
<b>6.3.</b>	<b>respuesta ante incidentes.....</b>	<b>27</b>
<b>6.4.</b>	<b>recuperación ante incidentes y planes de continuidad.....</b>	<b>27</b>
<b>6.5.</b>	<b>VIOLACIÓN DE LA SEGURIDAD DE DATOS PERSONALES.....</b>	<b>27</b>
<b>7.</b>	<b>OBLIGACIONES DEL PERSONAL.....</b>	<b>29</b>
<b>8.</b>	<b>TERCERAS PARTES.....</b>	<b>30</b>
<b>9.</b>	<b>REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD.....</b>	<b>31</b>
<b>10.</b>	<b>DOCUMENTACIÓN COMPLEMENTARIA.....</b>	<b>32</b>
	<b>anexo. glosario de términos.....</b>	<b>33</b>

 <b>DIPUTACIÓN D CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 4 de 34

## 1. INTRODUCCIÓN

### 1.1. JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Diputación de Castellón depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o 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, 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. Es por ello que el Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de Enero, ENS en adelante), 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”.


Esto implica que las diferentes áreas de la Diputación deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.

Todas las áreas 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 al Artículo 7 del ENS.

En este sentido, también se ha tenido en cuenta la normativa en materia de protección de datos: Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, con objeto de llevar a cabo una integración ente la organización en materia de seguridad y en materia de protección de datos, como parte del compromiso de la Diputación de Castellón con la Seguridad de la Información y con la Privacidad.

### 1.2. MISIÓN Y SERVICIOS PRESTADOS


La Diputación de Castellón, para la gestión de sus intereses, y en el ámbito de sus competencias y como Administración pública, sirve con objetividad los intereses generales y actúa de acuerdo a los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 5 de 34

actividades y presta los servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de los habitantes de la provincia.

La presente Política de Seguridad aplica a las diferentes actividades en las que participa la Diputación de Castellón a través de medios electrónicos, en concreto:


- a. Las relaciones de carácter jurídico-económico entre los ciudadanos y la Diputación.
- b. La consulta por parte de los ciudadanos de la información pública administrativa y de los datos administrativos que estén en poder de la Diputación.
- c. La realización de los trámites y procedimientos administrativos incorporados para su tramitación en la Sede Electrónica de la Diputación.
- d. El tratamiento de la información obtenida por la Diputación en el ejercicio de sus potestades.

 <b>DIPUTACIÓN D CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 6 de 34

## 2. MARCO NORMATIVO

Como base normativa para realizar la presente guía de seguridad, se ha analizado la legislación vigente, que afecta al desarrollo de las actividades de la Administración en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información. El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- 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, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de Enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunde en beneficio de la eficacia y la eficiencia.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

 <b>DIPUTACIÓN D CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 7 de 34

### 3. ORGANIZACIÓN DE LA SEGURIDAD

#### 3.1. Definición de Roles

Tal como indica el artículo 12 del ENS, La seguridad deberá comprometer a todos los miembros de la organización. La Política de Seguridad, según detalla 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 por tanto los siguientes roles en la organización relacionados con la Seguridad de la Información:

##### A. Responsable de la Información


Se ha designado responsable de la Información al Presidente de la Diputación, u órgano en quien delegue, a quien le corresponden las siguientes funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- El Responsable de la Información 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 Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

##### B. Responsable del Servicio

Se ha designado responsable del Servicio a cada uno de los responsables de unidades funcionales afectadas por el ENS en los términos en los que lo establece el decreto que lo regula, a quienes les corresponden las siguientes funciones:

- Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio,

 <b>DIPUTACIÓN D CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 8 de 34

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 pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

### C. Responsable de Seguridad de la Información

Se ha designado como responsable de Seguridad de la Información al Jefe del servicio de Informática, a quien le corresponderán las siguientes funciones:

- Reportará directamente al Comité de Seguridad de la Información.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- 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.



 <b>DIPUTACIÓN D CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 9 de 34

## D. Responsable del Sistema


Se ha designado como responsable del Sistema al jefe de sección de Sistemas, al que le corresponden las siguientes funciones:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de 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.

## E. Administrador de la Seguridad del Sistema

Se ha designado como Administrador de la Seguridad del Sistema al técnico de Sistemas, al que como tal, le corresponden las siguientes funciones:

- 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

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 10 de 34

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 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 reflejadas en un procedimiento documentado 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 reflejadas en un procedimiento documentado 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.

## F. Responsable de Seguridad Física


Se ha designado como responsable de Seguridad Física al jefe del servicio de ingeniería interna, al que le corresponderá implantar las medidas de seguridad que le competan dentro de las determinadas por el responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

## G. Responsable de Gestión de Personal

Se ha designado como responsable de Gestión de Personal a la jefe del servicio de Recursos Humanos, al que le corresponde implantar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

## H. Responsable Técnico

El Responsable Técnico, implantará las medidas necesarias para mantener, controlar y agilizar las tareas derivadas del cumplimiento del ENS y RGPD. Además, será el encargado de gestionar las herramientas de gestión normativa implantadas en la Diputación de Castellón (Sandas GRC), con el fin de mantener la gestión diaria actualizada e informada a los diferentes responsables.

 <b>DIPUTACIÓN D CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 11 de 34

La designación nominativa de las personas que ocupan los roles anteriormente referidos se relacionan en el anexo del decreto que regula la designación de responsables del servicio.

## **3.2. Roles relacionados con continuidad del servicio**

### **3.2.1. Comité de Crisis**


El comité de Crisis está compuesto por personas con responsabilidad administrativa y/o tecnológica dentro de la Diputación.

Las principales funciones del Comité de Crisis son las siguientes:

- Coordinar la respuesta ante las incidencias graves o catastróficas determinando, en caso de considerarlo necesario, el traslado de las operaciones a las ubicaciones de contingencia, y garantizando la reanudación de las mismas en el marco temporal establecido para ello.

Las responsabilidades del Comité de crisis son:

- Prestar un apoyo visible por parte de la Dirección al PCN.
- Garantizar que la Diputación dispone de un PCN acorde a las necesidades de negocio.
- Desarrollar programas de concienciación y formación sobre el PCN para el personal de la Diputación.
- Supervisar la realización de pruebas y el mantenimiento y actualización del PCN.
- Aprobar los cambios del PCN.
- Activar el/los Plan/es de Emergencia y/o Plan/es de Evacuación en el supuesto de que se dieran las condiciones que obliguen a la evacuación de las personas de las instalaciones de la Diputación.
- Activar el PCN en cualquiera de los escenarios de contingencia o de desastre previamente establecidos.
- Gestionar las reclamaciones de cobertura de las pólizas de seguros contratadas por la Diputación.
- Asegurarse de contar con los recursos económicos necesarios para afrontar las partidas de gastos extraordinarios en los que sea necesario incurrir durante el estado de contingencia o desastre y autorizar la ejecución de los mismos.
- Mantener informada a la opinión pública, accionistas y proveedores acerca de la situación de la Diputación tras la contingencia o el desastre.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 12 de 34

- Proveerse de centros alternativos de operación en el supuesto de que resulte necesario, así como autorizar y coordinar el traslado de las operaciones de negocio a los lugares seleccionados.

### 3.2.2. Equipo de recuperación


El Equipo de Recuperación está constituido por los responsables de departamentos o actividades de la Diputación que, no formando parte del Comité de Crisis, deban participar en las actividades de evaluación y recuperación de los procesos de negocio, realizando una evaluación de daños ocasionados por la incidencia en sus respectivas áreas de responsabilidad y adoptando todas aquellas medidas que resulten necesarias para la resolución de la incidencia y el restablecimiento de los procesos de negocio.

En la gestión de la continuidad del negocio el equipo de recuperación deberá:

- Evaluar la repercusión y efectos de la incidencia sobre los recursos de su área de responsabilidad, determinando la posibilidad de recuperación de los mismos.
- Iniciar los procedimientos de recuperación de los procesos de negocio de los que son responsables.
- Contactar tan pronto como sea posible con las personas que de ellos dependen y coordinar sus acciones para la recuperación de los procesos de negocio que caen bajo su responsabilidad.
- Establecer contacto con los terceros (proveedores, socios, ...) con los que habitualmente mantienen relaciones a fin de coordinarse con ellos en la medida en que sea necesario.
- Supervisar y coordinar la recuperación de los recursos (infraestructura, hardware, software, información, ...) que hubieran resultado afectados por la incidencia en las Oficinas Centrales.
- Adoptar todas aquellas medidas adicionales que resulten necesarias para la reanudación de los procesos críticos de negocio, ya sea en las propias oficinas o en las oficinas de contingencia que les fuera comunicado.
- Gestionar y coordinar, si procede, el traslado a los centros de contingencia de las personas y los activos de información que fueran necesarios.

### 3.3. Comité de Seguridad de la información

Se ha creado el Comité de Seguridad de la Información que estará compuesto por los siguientes miembros:

 <b>DIPUTACIÓN D CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 13 de 34

Responsable de modernización, Responsable de Seguridad de la Información, Secretaría General, Archivo y publicaciones, junto con Área Técnica y el Responsable Técnico.

A requerimiento del Comité se convocará cualesquiera otros Jefes de Servicio o Área y responsables, cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad y por la RGPD.


Corresponde al Secretario/a del Comité de Seguridad de la Información:

- Convocar las reuniones del Comité de Seguridad de la información
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Todos miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos/áreas.
- 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 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 Diputación 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 Diputación de Castellón. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Velar para que 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.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 14 de 34

- 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.
- Recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.
- Se asesorará de los temas 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 interna y/o externa.
  - Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.
- Aprobará el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente, en caso de ocurrencia de incidentes de seguridad de la información.

### **3.4. 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 Responsable del Sistema:

1. Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
2. Informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
3. Da cuenta 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:

1. 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.
2. 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.
3. Da cuenta al Comité de Seguridad de la Información:
  - Resumen consolidado de actuaciones en materia de seguridad.
  - Resumen consolidado de incidentes relativos a la seguridad de la información.


 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 15 de 34

- Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.
1. Da cuenta a la Alta Dirección de la Diputación de Castellón, según lo acordado en el Comité de Seguridad de la Información.
    - 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.

### **3.5. Procedimientos de designación de personas**

La Dirección de la Organización nombrará formalmente mediante su publicación en el Boletín Oficial correspondiente:

- Al Responsable de la Información.
- A los Responsables del Servicio.
- Al Responsable de la Seguridad.
- Al Responsable del Sistema, que debe reportar directamente al Comité de Seguridad de la Información.
- Al Administrador de Seguridad del Sistema, a propuesta del Responsable de Seguridad de la Información.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	Política de Seguridad		<b>DOC-ENS-010</b>
	ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN		
	Nº edición: 01	Nº revisión: 06	Página 16 de 34

#### 4. FIGURAS VINCULADAS A PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

##### 4.1. INTRODUCCIÓN

De conformidad con lo establecido en la normativa europea y estatal en materia de protección de datos (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos; y, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales) la Diputación de Castellón debe designar, en línea con sus necesidades organizativas y con el objetivo de garantizar las exigencias de la regulación aplicable, una serie de figuras que a continuación se exponen.

##### 4.2. FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

El Responsable del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento.


A efectos de la **Diputación de Castellón** se ha atribuido la condición de Responsable de Tratamiento a la persona jurídico-pública, es decir, la propia Diputación. De manera que, se ha entendido que la Diputación es Responsable del Tratamiento de los datos de carácter personal, que obran en sus sistemas de información, y que derivan de la prestación de los servicios públicos atribuidos a nivel de competencias.

A su vez, cabe decir que la consideración de Responsable de Tratamiento **no** debe ser asociada a persona física representante de la Diputación, en calidad del cargo o puesto (como por ejemplo, el Presidente o Secretario).

Las funciones del Responsable del tratamiento son:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
- Deberá informar a los titulares de los datos los derechos que les asisten y en los términos en los que pueden ejercerlos.
- Deberá excluir del tratamiento los datos relativos al afectado que se oponga al tratamiento de los mismos.
- Deberá cesar en la utilización o cesión ilícita de los datos cuando así lo requiera el interesado.
- Obligación de hacer efectivo el derecho de rectificación o supresión del interesado en el plazo máximo de 1 mes.



 <b>DIPUTACIÓN D E CASTELLÓN</b>	Política de Seguridad		<b>DOC-ENS-010</b>
	ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN		
	Nº edición: 01	Nº revisión: 06	Página 17 de 34

- Notificar las rectificaciones o cancelaciones efectuadas en los datos personales a quien se haya comunicado dichos datos, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.


### 4.3. FUNCIONES Y OBLIGACIONES DEL DELEGADO DE PROTECCIÓN DE DATOS

Mediante Decreto del Presidente número 1900 de fecha 24 de mayo de 2018 de la Diputación de Castellón se creó la **Oficina Provincial de Protección de Datos y Seguridad** con el objeto de desarrollar las funciones previstas tanto en la normativa nacional como comunitaria relativas al Delegado de Protección de Datos así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad, tanto para la Diputación de Castellón, las entidades del sector público dependientes de la misma, como para los municipios de la provincia que se sitúan por debajo del umbral de los 20.000 habitantes que así lo soliciten.

En este último término, el Reglamento General de Protección de Datos establece en su artículo 37.3 *Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.*

La Oficina Provincial de Protección de Datos y Seguridad está compuesta por los empleados públicos que se relacionan a continuación:

<b>Jefe del Servicio de Administración e Innovación Pública</b>	<b>Representante de la Oficina ante la Agencia Española de Protección de Datos, así como ante los interesados y/o afectados que así lo requieran.</b>
<b>Secretario General de la Diputación</b>	
<b>Jefe del Servicio de Informática</b>	Responsable de la seguridad para la Diputación de Castellón en los términos establecidos en el Esquema Nacional de Seguridad, debiendo abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.
<b>Jefe de Sección de Informática Municipal</b>	
<b>Jefa del Servicio de Recursos Humanos</b>	
<b>Asesora Jurídica adscrita al Servicio de Gestión, Inspección y Recaudación</b>	
<b>Auxiliar Administrativa de Actas y Decretos</b>	Funciones administrativas de secretaría de la Oficina

 <b>DIPUTACIÓN D E CASTELLÓN</b>	Política de Seguridad		<b>DOC-ENS-010</b>
	ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN		
	Nº edición: 01	Nº revisión: 06	Página 18 de 34

El DPO es un órgano colegiado cuyas funciones se señalan en el artículo **39 del Reglamento (UE) 679/2016**, así como los **artículos 36 y 37 de la Ley Orgánica 3/2018**, y se ocupa de la aplicación de la legislación sobre privacidad y protección de datos en la entidad en la que desarrolla sus funciones.


El delegado de protección de datos tendrá como mínimo las siguientes **funciones**:

- a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
- d) cooperar con la autoridad de control;
- e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Para ello deberá **ser capaz de**:

- a) Recabar información para determinar las actividades de tratamiento,
- b) analizar y comprobar la conformidad de las actividades de tratamiento, e
- c) informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- d) Recabar información para supervisar el registro de las operaciones de tratamiento.
- e) Asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
- f) Asesorar sobre:
  - Si se debe llevar a cabo o no una evaluación de impacto de la protección de datos
  - Qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos.


 <b>DIPUTACIÓN D CASTELLÓN</b>	Política de Seguridad		<b>DOC-ENS-010</b>
	ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN		
	Nº edición: 01	Nº revisión: 06	Página 19 de 34

- Si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
  - Qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos de intereses de los afectados.
  - Si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y
  - si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes al Reglamento.
- g) Priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.
- h) Asesorar al responsable del tratamiento sobre:
- Qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos,
  - qué áreas deben someterse a auditoría de protección de datos interna o externa,
  - qué actividades de formación internas proporcionar al personal o a los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

El DPO deberá reunir conocimientos especializados del Derecho y la práctica en materia de protección de datos. Se han identificado, en consecuencia, aquellos **conocimientos, habilidades o destrezas necesarias** que tiene que saber o poseer el Delegado de Protección de Datos para llevar a cabo una de las funciones propias de su puesto.

Estas funciones genéricas del DPO se pueden concretar en tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
2. Identificación de las bases jurídicas de los tratamientos.
3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
4. Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
5. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
6. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.


 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 20 de 34

7. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
8. Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
9. Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
10. Diseño e implantación de políticas de protección de datos.
11. Auditoría de protección de datos.
12. Establecimiento y gestión de los registros de actividades de tratamiento.
13. Análisis de riesgos de los tratamientos realizados.
14. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
16. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
18. Realización de evaluaciones de impacto sobre la protección de datos
19. Relaciones con las autoridades de supervisión
20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

#### **4.4. FUNCIONES Y OBLIGACIONES DE USUARIOS CON ACCESO A DATOS**

Todos los empleados de la entidad están sujetos a funciones y obligaciones. Todo el personal de la entidad que disponga de acceso a los datos de carácter personal debe cumplir con las siguientes obligaciones:

- No se permite la difusión de datos de carácter personal ni confidencial perteneciente a la entidad. Estando obligado a guardar secreto de la información incluso terminada la relación laboral.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	Política de Seguridad		<b>DOC-ENS-010</b>
	ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN		
	Nº edición: 01	Nº revisión: 06	Página 21 de 34

- El usuario se responsabilizará de notificar toda incidencia según el procedimiento de gestión de incidencias, no notificar una incidencia será considerada una omisión del deber del trabajador.
- El usuario se responsabilizará de todos los accesos que se realicen bajo su identificador y contraseña, por tanto, no deberá revelar la contraseña.
- El usuario se responsabilizará siempre que abandone el puesto de trabajo de cerrar su sesión o bloquear el equipo con contraseña.
- No se podrán instalar aplicaciones en los sistemas de la entidad sin el consentimiento del delegado de protección de datos.
- No se permite la copia de datos de carácter personal, en soportes, sin la autorización expresa del delegado de protección de datos.
- El usuario se responsabilizará de guardar copias de todos los correos que incluyan anexos con datos personales vinculados a la entidad.

#### 4.5. FUNCIONES Y OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

Los encargados del tratamiento tienen como misión realizar las tareas ordinarias para el desarrollo efectivo de las funciones para las que ha sido creado el tratamiento por cuenta del Responsable del tratamiento.


En este sentido, el **apartado 8 del artículo 4 del RGPD** define al Encargado de Tratamiento como <<la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento>>.

El Encargado del Tratamiento deberá aplicar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado


Igualmente deberá implementar las medidas de seguridad a que se refiere el párrafo anterior y que aparecerán estipuladas en el contrato con el Responsable del Tratamiento.

En concreto, sus funciones son las de:

- Tratar los datos del tratamiento.
- Realizar el control de tratamiento, calidad y seguridad de los datos.
- Controlar la forma y requisitos para proceder a las adiciones y cancelaciones.
- Controlar los soportes de seguridad.
- Control y acceso de contraseñas.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 22 de 34

- Mantenimiento del registro de incidencias.
- Crear una lista para las situaciones en la que un afectado no desee que sus datos personales se almacenen en el tratamiento.
- Dar traslado al responsable del tratamiento de aquellas solicitudes de ejercicio de derecho que se reciban por parte de los interesados.

 <b>DIPUTACIÓN D CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 23 de 34

## 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 Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

Así mismo, de acuerdo con el principio de responsabilidad proactiva establecido en el RGPD, debe tenerse en cuenta la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado, determinándose con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto. Como punto de partida, de igual modo que en una Evaluación de Impacto en Protección de Datos (EIPD), se deben describir adecuadamente las actividades de tratamiento, proceso que facilitará la documentación del registro de actividades de tratamiento.

### 5.2. criterios de evaluación de riesgos

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información 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.

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 de la Información 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.

 <b>DIPUTACIÓN D CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 24 de 34

Los niveles de Riesgo residuales esperados sobre cada Información 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 su Responsable de esa Información.

Los niveles de Riesgo residuales esperados sobre cada 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 su Responsable de ese Servicio.

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.

### **5.6. EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE LOS DATOS SUJETAS AL RGPD**

El continuo avance de la tecnología y la evolución de los tratamientos propician la aparición continua de nuevos riesgos que deben ser gestionados. En este contexto, el RGPD exige que los responsables del tratamiento implementen medidas de control adecuadas para demostrar que se garantizan los derechos y libertades de las personas y la seguridad de los datos, teniendo en cuenta entre otros, los “riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas” (artículo 24.1 del RGPD) y aplicando las medidas oportunas. Para ello, la Diputación de Castellón debe considerar desde el inicio, en la fase de diseño, las acciones preventivas suficientes para poder identificar, evaluar y tratar los riesgos asociados al tratamiento de datos personales, y así, poder asegurar los principios de protección de los datos garantizando los derechos y libertades de los interesados

La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento,




 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 25 de 34

con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

El resultado de la EIPD se debe tener en cuenta, necesariamente, a la hora de tomar las decisiones relacionadas con el cumplimiento de lo previsto en el RGPD y la toma de decisión de la viabilidad o no de llevar a cabo el tratamiento de los datos.

A la hora de realizar una EIPD, se debe disponer de una metodología que considere los requerimientos exigidos por el RGPD en su artículo 35.7, donde se establece que la EIPD deberá incluir como mínimo:

- Una descripción sistemática de la actividad de tratamiento previstas.
- Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad.
- Una evaluación de los riesgos.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 26 de 34

## 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. El ENS a través de su artículo 19 establece la que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. De igual forma, el artículo 17 del citado ENS define que los sistemas de instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

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:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- 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.

### 6.2. Monitorización y detección de incidentes


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 cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la Organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	Política de Seguridad		<b>DOC-ENS-010</b>
	ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN		
	Nº edición: 01	Nº revisión: 06	Página 27 de 34

### 6.3. Respuesta ante incidentes

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto 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.

### 6.5. VIOLACIÓN DE LA SEGURIDAD DE DATOS PERSONALES

Con el objetivo de identificar de un evento de privacidad, catalogar, resolver y/o escalar todas aquellas entradas relacionadas con eventos en los que se vean implicados “datos personales”, se debe desarrollar un procedimiento operativo por parte de la Diputación de Castellón en relación a la gestión y notificación de todos aquellos eventos relacionados con privacidad.


En el contexto del Reglamento General de Protección de Datos, se entiende **por violación de datos de carácter personal** lo establecido como definición en el Art.3 del citado reglamento y que indica lo siguiente:

*“Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.”*

En este sentido, y dadas las definiciones, cualquier entrada que afecte o impacte en las dimensiones de la seguridad (Confidencialidad, Integridad o Disponibilidad) debe ser considerado al menos como **un evento de privacidad** siempre que afecte a un sistema de información que contenga datos de carácter personal.

De acuerdo con la normativa, el tiempo máximo de comunicación a la autoridad de control (Agencia Española de Protección de Datos) de una violación de privacidad no debe de superar las **72 horas** desde el momento en el que se identifica la violación de privacidad.


Dicha notificación, la debe llevar a cabo, el Delegado de Protección de Datos nombrado en la Diputación de Castellón.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 28 de 34

En la notificación se deberá de incluir al menos la siguiente información:

- Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
- Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales;
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

En caso de que no fuese posible facilitar toda la información en un primer reporte, podrán realizarse notificaciones graduales que incorporen la información requerida según se disponga de ella.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 29 de 34


## 7. OBLIGACIONES DEL PERSONAL

Los miembros de la organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de la organización atenderán 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 los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten 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 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.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 30 de 34

## 8. TERCERAS PARTES


Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha 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, 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.


 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 31 de 34

### 9. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

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.

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 32 de 34

## 10. 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.
- Guías de seguridad.
- Procedimientos de seguridad.

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. 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.



 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 33 de 34

## anexo. glosario de términos

### **Análisis de riesgos**

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

### **Datos de carácter personal**

Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

### **Tratamiento**

Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

### **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.

### **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 consideran 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**

 <b>DIPUTACIÓN D E CASTELLÓN</b>	<b>Política de Seguridad</b>		<b>DOC-ENS-010</b>
	<b>ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN</b>		
	Nº edición: 01	Nº revisión: 06	Página 34 de 34

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.

### **Responsable del tratamiento**

La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

### **Encargado del tratamiento**

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

### **Tercero**

Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

### **Violación de la seguridad de los datos personales**

Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.