FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO

EXCMA. DIPUTACIÓN PROVINCIAL DE CASTELLÓN

HOJA DE ESTADO DEL DOCUMENTO

Versión	Fecha	Cambios	Revisado	Aprobado
1.0	25/11/2021	v.1	AYZ	
2.0	01/12/2021	v.2	MBB	
3.0	18/01/2022	v.3	MBB	
4.0	19/02/2024	V.4	ASS	
5.0	29/07/2024	V.5	ASS	
6.0	17/09/2024	V.6	ASS	Acuerdo JGL 17/9/2024

ÍNDICE DE CONTENIDOS

1 OBJETO

El objeto del presente documento es la definición de una propuesta de funciones y obligaciones en materia de privacidad y seguridad de la información que incluir en detalle en la relación de puestos de trabajo (en adelante, RPT) de la Excma. Diputación Provincial de Castellón (en adelante, Diputación o Dipcas). En este sentido, se busca proponer un marco de referencia que establezca las responsabilidades generales en la gestión de la privacidad y seguridad de los sistemas de información de la propia Diputación del ámbito subjetivo de aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), así como del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de seguridad (ENS), desarrollando las figuras o roles más significativos que asuman dichas responsabilidades.

Con la implantación del presente documento se atiende a lo establecido en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos):

> ***Artículo 32. Seguridad del tratamiento***
>
> *1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> *a) la seudonimización y el cifrado de datos personales;*
>
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
>
> *c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
>
> *d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. […]*

Así como, con el cumplimiento de lo establecido en la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

> ***Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.***
>
> *1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado,*

adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

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

Asimismo, para la elaboración del presente documento se han tomado como base las directrices señaladas en la normativa anteriormente mencionada, la *Guía de Seguridad de las TIC CCN-STIC 801: Esquema Nacional de Seguridad, Responsabilidades y funciones*, y otras Guías publicadas por la Agencia Española de Protección de Datos u otras autoridades europeas en materia de privacidad.

A este respecto, la Diputación ha establecido y aprobado su propia Organización de Seguridad, de acuerdo con su naturaleza, estructura, dimensión y recursos disponibles, que está recogida en la Política de Seguridad de la Información y, en la normativa interna sobre Protección de Datos. Es por ello que, derivado de esta Organización de Seguridad resulta necesario regular las funciones y obligaciones que deben asumir distintos empleados de la organización en el desarrollo de sus roles y responsabilidades. Estas funciones y obligaciones vienen reguladas a continuación.

2 ÁMBITO DE APLICACIÓN

Esta normativa es de aplicación a todo al ámbito de gestión de la seguridad de los sistemas de información de la Diputación. Concretamente, resulta aplicable a la redacción y elaboración de la Relación de Puestos de Trabajo (RPT). Bien es conocido por todos, que la RPT es el instrumento técnico sobre el que las Administraciones Públicas diseñan su estructura de personal para adecuarla a las necesidades del servicio público (tanto internamente como hacia la ciudadanía). Es por tanto el eje sobre el que pivota la gestión de recursos humanos. La eficacia y gran diferencia de la RPT respecto a un organigrama radica en su objetividad: no tiene en consideración a la persona que ocupa el puesto de trabajo sino al puesto en sí.

Atendiendo estos aspectos, y de acuerdo con lo comentado anteriormente, a través del presente documento se establecen aquellas funciones y obligaciones a incluir en el RPT de determinados roles establecidos por la normativa de seguridad y privacidad que, obligatoriamente deben estar designados en la propia Diputación.

3 VIGENCIA

La presente normativa entrará en vigor a partir de su aprobación inicial por la Oficina Provincial de Protección de Datos y Seguridad de la Diputación de Castellón y estará vigente hasta su sustitución por otra normativa del mismo alcance o similar.

4 MARCO NORMATIVO Y ACRÓNIMOS

Acrónimo	Concepto
RGPD	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).
LOPD-GDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales
LBRL	Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
ET	Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
EBEP	Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
ENS	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
TC	Tribunal Constitucional.
TS	Tribunal Supremo.
SAN	Sentencia de la Audiencia Nacional.
RPT	Relación de Puestos de Trabajo

1.

5 ACTORES Y RESPONSABLES

La gestión de la seguridad de los sistemas de información en las organizaciones *-definición, implantación y mantenimiento-* exige establecer una Organización de la Seguridad. En este caso, la Diputación ha determinado con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.

Si bien en la anterior regulación , en el artículo 10 del ENS se definían las funciones (las negritas son nuestras):

Artículo 10. La seguridad como función diferenciada

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

*El **responsable de la información** determinará los requisitos de la información tratada; el **responsable del servicio** determinará los requisitos de los servicios prestados; y el **responsable de seguridad** determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.*

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

Imagen 1. Guía de Seguridad de las TIC CCN-STIC 801: Esquema Nacional de Seguridad, Responsabilidades y funciones.

En fecha 3 de mayo de 2022, se aprobó la nueva regulación del ENS, mediante la promulgación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, publicado en el BOE número 106, de fecha 4 de mayo de 2022. Estableciéndose una nueva diferenciación de responsabilidades en materia de seguridad, ampliando a cuatro a las figuras que deben designarse en la organización frente a las tres anteriores.

Es en el actual artículo 11 del ENS, en el que se definen las distintas responsabilidades (las negritas son nuestras):

"Artículo 11. Diferenciación de responsabilidades.

*1. En los sistemas de información se diferenciará el **responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema**.*

2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos."

Además de las tres figuras mencionadas en el art. 10 del anterior ENS -Responsable de la Información, Responsable del Servicio y Responsable de la Seguridad-, cuyas competencias y responsabilidades

pueden ser indelegables[1], las organizaciones suelen disponer también del denominado Responsable del Sistema (de información[2]), y cuya responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata[3] (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados[4].

La nueva regulación del ENS (Real Decreto 311/2021), ya establece la obligatoriedad de contar con cuatro figuras diferencias:

1. Responsable de la información
2. Responsable del servicios
3. Responsable de la seguridad
4. Responsable del sistema

Por otro lado, cuando la entidad está tratando datos de carácter personal, se hace necesario contemplar las figuras de Responsable del Tratamiento, Delegado de Protección de Datos y, en su caso, Encargado del Tratamiento, con las funciones definidas en el RGPD y en la LOPDGDD.

El cuadro[5] siguiente muestra las peculiaridades de las figuras más significativas en materia de seguridad de la información y privacidad, atendiendo a la norma legal de la que traen causa:

Entidad	Ubicación legal	Funciones, Características o Referencias
Dirección de la Entidad del Sector Público	La derivada de la aplicación de la Ley 40/2015	Entidades del Sector Público del ámbito de aplicación del ENS, cuyo titular ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad, incluyendo las de seguridad de la información, de conformidad con lo dispuesto en la Ley 40/2015 y en el resto del ordenamiento jurídico. Es el máximo responsable de la implantación del ENS.
Responsable de la Información	ENS, art. 11 y 13	Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de la información constituye asimismo una actividad indelegable.
	ENS, art. 40	La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su

[1] Parece claro que, mientras que las responsabilidades del Responsable de la Información y Responsable del Servicio son siempre indelegables, no ocurre lo mismo con las correspondientes al Responsable de la Seguridad, que podrían ser asumidas, como competencias propias, por las Diputaciones Provinciales, en el caso de las entidades locales. Por tanto, habrá que sostener, con carácter general, que todas las responsabilidades mencionadas son indelegables en tanto no exista una habilitación legal que permita la delegación.

[2] El ENS define "sistema de información" como: "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 IV. Glosario).

[3] Es "autor mediato" quien causa un resultado sirviéndose de otra persona como medio o instrumento para realizar la ejecución. El autor no realiza directa y personalmente el delito, se sirve de otra persona consciente de la trascendencia penal que tiene su acto.

[4] Cuando se utilizan servicios externalizados (mediante contrato, convenio, encomienda, etc.), es frecuente que la entidad prestadora (pública o privada) cuente asimismo con un Responsable de la Seguridad al que será exigible el mantenimiento de la seguridad de los sistemas de información concernidos, sin que ello suponga merma de la responsabilidad exigible al Responsable de la Seguridad de la entidad pública destinataria de los servicios.

[5] Cuadro extraído de la *Guía de Seguridad de las TIC CCN-STIC 801: Esquema Nacional de Seguridad, Responsabilidades y funciones*

Entidad	Ubicación legal	Funciones, Características o Referencias
		repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
Responsable del Servicio	ENS, art. 11 y 13	Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de los servicios constituye asimismo una actividad indelegable.
	ENS, art. 36	Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
	ENS, art. 40	Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
Responsable de la Seguridad	ENS, art. 11 y 13	Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobres estas cuestiones. Nota: En caso de servicios externalizados, la responsabilidad última la tiene siempre la entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio.
	ENS, art. 16.3	Las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
	ENS, art 19	En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de la Seguridad.
	ENS, arts. 28	Las medidas del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del Responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos. La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el Responsable de la Seguridad. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los

Entidad	Ubicación legal	Funciones, Características o Referencias
		requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de la seguridad.
	ENS, art. 29	La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el ENS en condiciones de mejor eficiencia. Los supuestos concretos de utilización de estas infraestructuras y servicios comunes serán determinados por cada Administración.
	ENS, art. 31 y Anexo III	Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
Entidad Responsable de la Seguridad de la Información	Propuesta de Reglamento de Desarrollo del RD-l 12/2018[6]	El Responsable de la Seguridad (de la información) es la persona designada por la Dirección de la entidad, según el procedimiento descrito en su Política de Seguridad de la Información. El ENS señala que el Responsable de la Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Además de ello, como hemos visto con anterioridad, en caso de servicios externalizados, la responsabilidad última la tiene siempre la Entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio (lo que sucede, por ejemplo, en la utilización de servicios en la nube).
Responsable del Sistema (de información)		
	ENS, artículo 11 y 13	Se encarga por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
	La derivada de la aplicación de la Ley 40/2015	Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.
	ENS, art. 31	Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.
Responsable del	RGPD, art. 4.7) y	La persona física o jurídica, autoridad pública, servicio u otro

[6] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. En el momento de redactar estas líneas, este RD-l está siendo tramitado como Proyecto de Ley, al tiempo que se está redactando su Reglamento de Desarrollo, que recogerá definitivamente las funciones y competencias de esta Entidad Responsable de la Seguridad de la Información. Por tanto, la lista de funciones indicada no debe considerarse definitiva.

Entidad	Ubicación legal	Funciones, Características o Referencias
Tratamiento (Protección de Datos)	LOPDGDD, Título V	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 (Protección de Datos)	RGPD, art. 4.8) y LOPDGDD, Título V	La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable del Tratamiento.
Delegado de Protección de Datos	RGPD, art. 39 y LOPDGDD, arts. 34 a 37	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.

6 PROPUESTA DE ELEMENTOS BÁSICOS DE LAS FUNCIONES Y OBLIGACIONES QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO

A continuación, se detalla una propuesta de elementos básicos de las funciones y obligaciones que anunciar en detalle en la RPT de la Diputación. Se ha elaborado esta propuesta de funciones y obligaciones atendiendo a los distintos puestos de trabajo de la organización que tiene asignado un rol o responsabilidad con relevancia en materia de privacidad y seguridad. Son los siguientes:

6.1 Puesto 1245 – Jefe/a del Servicio de Informática:

De forma general, el Jefe/a del Servicio de Informática por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

En tanto **Responsable de Seguridad**, le corresponden 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.

- Asimismo, cumplirá con las funciones y responsabilidad que establece internamente el Plan de Continuidad de Negocio en caso de incidencias y para la ejecución de las actividades de recuperación, informando al Comité de Crisis existente a tales efectos.

Como **miembro del Comité de Seguridad de la Información**, le corresponden las siguientes funciones:

- 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 por 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.
- 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.

Como **miembro de la Oficina Provincial de Protección de Datos y Seguridad**, debe tenerse en cuenta que, como Jefe/a del Servicio de Informática, que se integra en la misma como responsable de la seguridad para la Diputación de Castellón en los términos establecidos en el Esquema Nacional de Seguridad, deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades. A este respecto, siempre que no se aprecie conflicto de intereses en el ejercicio del resto de funciones asignadas, le corresponden las siguientes funciones:

- Ser el representante de la Oficina ante la Agencia Española de Protección de Datos, así como ante los interesados y/o afectados que así lo requieran.
- 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. Concretamente:
    - 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;
    - 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;
    - 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;
    - Cooperar con la autoridad de control;
    - 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.

En tanto **Responsable del Servicio y de la información** le corresponden las siguientes funciones, contando con los criterios del Responsable de Seguridad y del Responsable del Sistema:

- Establecer 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.
- Determinar los requisitos de los servicios prestados y adoptará las medidas de índole técnicas y organizativas necesarias que sean posibles para garantizar la seguridad en el ciclo de vida de los servicios y sistemas.
- 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, 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.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Como **miembro del Comité de Crisis**, le corresponden las siguientes funciones:

- Coordinar la respuesta ante los 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.
- Concretamente:
    - 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.
- 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.

Como **miembro del Equipo de recuperación**, le corresponden las siguientes funciones:

- 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.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón y en Seguridad de las tecnologías de la información y comunicaciones, según programa Angeles CCN-CERT.

6.2 Puesto 1368 – Jefe/a Sección de Sistemas:

De forma general, el Jefe/a de Sección de Sistemas por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

En tanto **Responsable de Sistemas**, 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.
- Particularmente, integrará el Comité de Operaciones con las funciones que le son propias.
- Asimismo, cumplirá con las funciones y responsabilidad que establece internamente el Plan de Continuidad de Negocio en caso de incidencias y daños sobre los sistemas de información.

Como **miembro del Comité de Crisis**, le corresponden las siguientes funciones:

- Coordinar la respuesta ante los 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.

- Concretamente:

    - 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.

    - 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.

Como **miembro del Equipo de recuperación**, le corresponden las siguientes funciones:

- 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.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón y en esquema nacional de seguridad (aproximación practica) según programa Angeles CCN-CERT.

6.3 Cada uno de los responsables de unidades funcionales siguientes afectadas por el ENS en los términos en los que lo establece el decreto que lo regula:

1382	Jefe/a del Servicio de Acción Social
112	Interventor/a
930	Jefe/a del Servicio Jurídico
1544	Responsable de Formación
785	Jefe/a Servicio Carreteras y Obras
78	Jefe/a Oficina Técnica
1044	Jefe/a Servicio Ingeniería Interna
1309	Regente Personal Subalterno
1337	Jefe/a Servicio Cooperación Municipal
931	Jefe/a Servicio Gestión, inspección y recaudación
1307	Jefe/a Servicio Contratación y Central de Compras
1434	Técnico medio de archivo
1445	Jefe/a Servicio Patrimonio y Expropiaciones
125	Tesorero/a
1176	Jefe/a Servicio Promoción Económica RI
1312	Jefe/a Servicio Cultura, Restauración, Deportes y Juventud
1442	Responsable Imprenta
483	Director/a Complejo Penyeta Roja

En tanto **Responsable del Servicio y de la información** le corresponden las siguientes funciones, contando con los criterios del Responsable de Seguridad y del Responsable del Sistema:

- Establecer 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.
- Determinar los requisitos de los servicios prestados y adoptará las medidas de índole técnicas y organizativas necesarias que sean posibles para garantizar la seguridad en el ciclo de vida de los servicios y sistemas.
- 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, 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.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.4 Puesto 1044 – Jefe/a Servicio Ingeniería Interna

De forma general, el Jefe/a del Servicio de Ingeniería Interna por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

En tanto **Responsable de Seguridad Física**, le corresponden las siguientes funciones:

- Implantar las medidas de seguridad que le competan dentro de las determinadas por el responsable de la Seguridad de la Información.
- Informar a éste de su grado de implantación, eficacia e incidentes.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Como **miembro del Equipo de recuperación**, le corresponden las siguientes funciones:

- 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.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.5 Puestos actuales: 985, 1065, 1340, 1399, 1438, 1460 [Todos los Técnicos de Sistemas] – Coordinador de técnicos de sistemas:

En tanto **Administrador de Sistemas**, 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 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.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

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.

Debe estar formado en formación avanzada de gestión de incidentes de ciberseguridad según programa Angeles CCN-CERT.

6.6 Puesto 1323 – Jefe/a del Servicio Recursos Humanos:

De forma general, el Jefe/a del Servicio de Recursos Humanos por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

En tanto **Responsable de Gestión de Personal**, le corresponden las siguientes funciones:

- Implantar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad de la Información.
- Informar a éste de su grado de implantación, eficacia e incidentes.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Como **miembro de la Oficina Provincial de Protección de Datos y Seguridad**, le corresponden las siguientes funciones:

- 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. Concretamente:

    - 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;

    - 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;

    - 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;

    - Cooperar con la autoridad de control;

    - 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.

En tanto **Responsable del Servicio y de la información** le corresponden las siguientes funciones, contando con los criterios del Responsable de Seguridad y del Responsable del Sistema:

- Establecer 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.
- Determinar los requisitos de los servicios prestados y adoptará las medidas de índole técnicas y organizativas necesarias que sean posibles para garantizar la seguridad en el ciclo de vida de los servicios y sistemas.
- 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, 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.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Como **miembro del Comité de Crisis**, le corresponden las siguientes funciones:

- Coordinar la respuesta ante los 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.
- Concretamente:
    - 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.

- 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.

Como **miembro del Equipo de recuperación**, le corresponden las siguientes funciones:

- 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.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.7 Puesto 1 – Secretaría General:

De forma general, la Secretaría General por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

Como **miembro del Comité de Seguridad de la Información**, le corresponden las siguientes funciones:

- 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 por 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.
- 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.

Como **miembro de la Oficina Provincial de Protección de Datos y Seguridad**, le corresponden las siguientes funciones:

- 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. Concretamente:

    - 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;

    - 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;

    - 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;

    - Cooperar con la autoridad de control;

    - 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.

En tanto **Responsable del Servicio y de la información** le corresponden las siguientes funciones, contando con los criterios del Responsable de Seguridad y del Responsable del Sistema:

- Establecer 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.
- Determinar los requisitos de los servicios prestados y adoptará las medidas de índole técnicas y organizativas necesarias que sean posibles para garantizar la seguridad en el ciclo de vida de los servicios y sistemas.
- 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, 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.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Como **miembro del Comité de Crisis**, le corresponden las siguientes funciones:

- Coordinar la respuesta ante los 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.
- Concretamente:
    - 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.

- 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.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.8 Puesto 1434 – Técnico medio archivo:

De forma general, el Jefe/a del Servicio Archivo, Gestión Documental y Publicaciones por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

Como **miembro del Comité de Seguridad de la Información**, le corresponden las siguientes funciones:

- 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 por 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.
- 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.

En tanto **Responsable del Servicio y de la información** le corresponden las siguientes funciones, contando con los criterios del Responsable de Seguridad y del Responsable del Sistema:

- Establecer 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.
- Determinar los requisitos de los servicios prestados y adoptará las medidas de índole técnicas y organizativas necesarias que sean posibles para garantizar la seguridad en el ciclo de vida de los servicios y sistemas.
- 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, 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.

- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.9 Puesto 1043 – Jefe/a del Área técnica:

De forma general, el Jefe/a del Área Técnica por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

Como **miembro del Comité de Seguridad de la Información**, le corresponden las siguientes funciones:

- 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 por 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.
- 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.

En tanto **Responsable del Servicio y de la información** le corresponden las siguientes funciones, contando con los criterios del Responsable de Seguridad y del Responsable del Sistema:

- Establecer 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.
- Determinar los requisitos de los servicios prestados y adoptará las medidas de índole técnicas y organizativas necesarias que sean posibles para garantizar la seguridad en el ciclo de vida de los servicios y sistemas.
- 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, 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.

- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.10 Puesto 1308 - Jefe/a del Servicio de Administración e Innovación Pública

De forma general, el Jefe/a del Servicio de Administración e Innovación Pública por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

Como **miembro del Comité de Seguridad de la Información**, le corresponden las siguientes funciones

- 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 por 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.

- 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.

Como **miembro de la Oficina Provincial de Protección de Datos y Seguridad**, le corresponden las siguientes funciones:

- 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. Concretamente:
  - 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;
  - 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;
  - 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;
  - Cooperar con la autoridad de control;

- 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.

En tanto **Responsable del Servicio y de la información** le corresponden las siguientes funciones, contando con los criterios del Responsable de Seguridad y del Responsable del Sistema:

- Establecer 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.
- Determinar los requisitos de los servicios prestados y adoptará las medidas de índole técnicas y organizativas necesarias que sean posibles para garantizar la seguridad en el ciclo de vida de los servicios y sistemas.
- 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, 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.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Como **miembro del Comité de Crisis**, le corresponden las siguientes funciones:

- Coordinar la respuesta ante los 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.
- Concretamente:
  - 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.
- 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.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.11 Puesto 1060 – Jefe/a de Sección de Informática Municipal

De forma general, el Jefe/a de Sección de Informática Municipal por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

Como **miembro de la Oficina Provincial de Protección de Datos y Seguridad**, le corresponden las siguientes funciones:

- 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. Concretamente:
  - 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;

- 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;

- 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;

- Cooperar con la autoridad de control;

- 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.

En tanto **Responsable del Servicio y de la información** le corresponden las siguientes funciones, contando con los criterios del Responsable de Seguridad y del Responsable del Sistema:

- Establecer 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.
- Determinar los requisitos de los servicios prestados y adoptará las medidas de índole técnicas y organizativas necesarias que sean posibles para garantizar la seguridad en el ciclo de vida de los servicios y sistemas.
- 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, 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.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.12 Miembros del Comité de Crisis: Presidente y Diputado Informática (sin RPT), puestos de trabajo 1, 1308,1245, 1323, 1368

Como **miembro del Comité de Crisis**, le corresponden las siguientes funciones:

- Coordinar la respuesta ante los 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.
- Concretamente:
    - 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.
    - 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.

Debe estar formado en Ciberseguridad según programa propio de la diputación de Castellón.

6.13 Equipo de recuperación: Puestos de trabajo: 1044, 1245, 1368, 1323, y 930

Como **miembro del Equipo de recuperación**, le corresponden las siguientes funciones:

- 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.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.14 Resto del personal:

Al resto del personal de la Diputación que no tenga encomendada alguna de las funciones anteriormente descritas, le corresponden las siguientes funciones:

- 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.

- 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.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan de Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Debe estar formado en Ciberseguridad según programa propio de la diputación de Castellón.

7 ANEXO “A”: RELACIÓN DE RESPONSABLES DE SERVICIO

1245	Jefe/a del Servicio de Informática
1382	Jefe/a del Servicio de Acción Social
1	Secretaría General
112	Interventor/a
930	Jefe/a del Servicio Jurídico
1308	Jefe/a del Servicio de Administración e Innovación Pública
785	Jefe/a Servicio Carreteras y Obras
1043	Jefe/a Área Técnica
78	Jefe/a Oficina Técnica
1044	Jefe/a Servicio Ingeniería Interna
1309	Regente Personal Subalterno
1337	Jefe/a Servicio Cooperación Municipal
931	Jefe/a servicio Servicio Gestión, Inspección y Recaudación
1307	Jefe/a Servicio Contratación y Central de Compras
1323	Jefe/a Servicio RRHH
1434	Técnico medio archivo
1445	Jefe/a Servicio Patrimonio y Expropiaciones
125	Tesorero/a
1176	Jefe/a Servicio Promoción Económica RI
1312	Jefe/a Servicio Cultura, Restauración, Deportes y Juventud
1442	Responsable Imprenta Provincial
483	Director/a Complejo Penyeta Roja