FUNCIONES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El marco organizativo para la gestión de la política de seguridad de la información de la Diputación Provincial de Valladolid y Organismos Dependientes estará constituido por:

a. El Comité de Seguridad de la Información.
b. El Responsable y Administrador de Sistemas, y los Responsables de Seguridad, Servicios e Información, roles con funciones asociadas a la implantación del Esquema Nacional de Seguridad (ENS), y la adecuación a la legalidad vigente en materia de privacidad y protección de datos (RGPD y LOPD).
c. El Delegado de Protección de Datos, al tratarse de una figura que se encarga de asesorar y supervisar el cumplimiento del RGPD y una de las vertientes de la protección de la privacidad es la seguridad de los datos personales, se integra esta figura en el marco organizativo de la presente política.

Las Áreas de la Diputación y los Organismos Dependientes de ella, realizarán un seguimiento continuado de los niveles de prestación de servicio, calidad y seguridad de la información existiendo uno o varios responsables de los servicios y tratamientos de la información, según proceda.

Una única persona podrá desempeñar las funciones de responsable del servicio y tratamiento de la información cuando:

a. Los servicios prestados contengan datos de carácter personal.
b. La prestación del servicio dependa de la misma unidad u órgano administrativo que es responsable de la información.
c. La información utilizada para la prestación del servicio proceda de la misma unidad u órgano administrativo que lo presta.

1. Comité de Seguridad de la Información

1. Es el órgano de seguimiento de esta materia y estará formado:

a. Diputado/a Delegado/a del Área con competencias en Nuevas Tecnologías, que actuará como presidente.
b. Jefe/a del Servicio con competencias en Nuevas Tecnologías, que actuará como ponente.
c. Los responsables de las Áreas de la Diputación, o personas en quienes deleguen.
d. Los gerentes responsables de los Organismos Dependientes de la Diputación, o personas en quienes deleguen.
e. Un técnico del Área o del Servicio con competencias en Nuevas Tecnologías, que actuará como asesor del Comité, con voz, pero sin voto.
f. Un técnico de perfil jurídico del Área con competencia en Nuevas Tecnologías, responsable jurídico relacionado con privacidad y protección de datos, que actuara como secretario/a, con voz pero sin voto.

2. Serán funciones del Comité de Seguridad de la Información:
   a. Coordinar e impulsar las funciones de seguridad de la Diputación, así como velar por la mejora continua del sistema de gestión de la seguridad de la información.
   b. Elaborar la estrategia de evolución de la Diputación de Valladolid en lo que respecta a seguridad de la información.
   c. 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.
   d. Proponer y revisar regularmente las directrices de la Política de Seguridad de la información para que sea aprobada por el órgano competente.
   e. Velar por el cumplimiento de la normativa de aplicación en materia de seguridad de la información.
   f. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

3. A las reuniones del Comité Operativo de Seguridad de la Información, podrá asistir personal técnico si el presidente lo considerase oportuno a petición de cualquier miembro.

4. Este Comité se reunirá, al menos, una vez al semestre.

2. Responsabilidades asociadas al ENS y al RGPD/LOPD

En los sistemas de información se diferencia el responsable de la información, el responsable del servicio y el responsable de la seguridad. La responsabilidad de la seguridad de los sistemas de información está diferenciada de la responsabilidad sobre la prestación de los servicios.

1. Delegado de Protección de Datos **(DPD).** Persona física o jurídica, con máxima autoridad e independencia dentro de la Organización, responsable de liderar la adecuación a la legalidad vigente en materia de privacidad y protección de datos personales.

   Sus funciones, establecidas en el artículo 39 del RGPD, serán las siguientes:
   a. Asegurar el cumplimiento del RGPD, mediante la recolección de información, su análisis y revisión del cumplimiento en relación con los tratamientos de datos llevados a cabo en el seno de la organización realizando cuantas recomendaciones fuesen necesarias para garantizar el cumplimiento.
   b. Informar y asesorar al órgano decisorio de la empresa y a los propios empleados que se ocupen del tratamiento, sobre las obligaciones que les incumben, en relación con el RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados Miembros.
   c. Supervisar el cumplimiento de lo dispuesto en el RGPD, en otras disposiciones de protección de datos de la Unión o de los Estados miembros y en las políticas internas de la compañía 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.
   d. Cooperar con la autoridad de control, actuando como punto de contacto entre ésta y los interesados para cuestiones relativas al tratamiento de los datos personales en el seno de la organización.
   e. Participar en el desarrollo y ejecución de las evaluaciones de impacto (PIAs), asesorando sobre las cuestiones principales que podrán suscitarse de la ejecución de las mismas.
   f. Gestionar un registro actualizado de los tratamientos llevados a cabo en el seno de la compañía.

g. Comunicar la existencia de una vulneración relevante en materia de protección de datos a los órganos de administración y dirección de la entidad, proponiendo las medidas necesarias para evitar la persistencia en esa conducta.

2. *Responsable de la información (RINFO).* El responsable de establecer los requisitos de la información en materia de seguridad será el titular de cada área de la Diputación y de los Organismos Asociados, o persona en quien delegue, con competencia para decidir sobre la finalidad, contenido y tratamiento de dicha información, a cuyo efecto determinará los requisitos en materia de seguridad de la información que se maneja.

   Asimismo, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, establecerá los niveles de seguridad requeridos para la información, efectuando para ello las valoraciones del impacto que tendría un incidente que afectará a dicha información.

   Sus funciones serán las siguientes:

   a. Velar por el buen uso de la información y, por tanto, de su protección.
   b. Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
   c. Establecer los requisitos de la información tratada en materia de seguridad. Determinar los niveles de seguridad de la información, y aceptar los riesgos residuales calculados en el análisis, realizando su seguimiento y control.
   d. Promover la formación y concienciación en materia de seguridad de la información, en su ámbito de responsabilidad, siguiendo las directrices marcadas por el Comité de Seguridad.

3. *Responsable del servicio y tratamiento (RSERV).* Serán nombrados por los responsables de la información. Sus funciones serán las siguientes:

   a. Aplicar las medidas de seguridad determinadas por el Responsable de Seguridad sobre los servicios/sistemas de información de los que son responsables.
   b. Informar al Delegado de Protección de Datos de cualquier actividad que pueda suponer cambios en el registro de actividades de tratamiento.
   c. Aplicar los plazos de supresión asociados a los tratamientos con datos personales correspondientes.
   d. Aplicar las solicitudes de ejercicio de derechos ARCOP sobre las actividades de tratamiento de las que son responsables.
   e. Informar correctamente al ciudadano, a instancias de las indicaciones dadas por el Delegado de Protección de Datos, facilitando toda la información necesaria en las diferentes fuentes de recogida de datos personales (formularios en papel, aplicaciones informáticas, páginas web, etc…), y en los casos requeridos, solicitar previamente el consentimiento explícito previo.
   f. A instancia del Responsable de Seguridad y/o el Delegado de Protección de Datos, solicitar en los correspondientes pliegos/contratos con empresas externas que tengan rol de 'Encargado de Tratamiento' y/o 'Prestador de Servicios TI', la certificación de conformidad con el ENS.

4. *Responsable de Seguridad (RSEG).* Es la persona física o jurídica, u órgano colegiado, designado por el titular del Área con competencias en Nuevas Tecnologías. Sus funciones serán:

a. Determinar las decisiones para satisfacer y mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, mediante planes, procedimientos e instrucciones técnicas de seguridad, coordinando el proceso de gestión de la seguridad.
b. Mantener actualizada y disponible dicha documentación y diseñar las actividades de concienciación y formación en materia de seguridad, siguiendo las directrices marcadas por el Comité de Seguridad.
c. Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
d. Asesorar en la definición de requisitos, y validar la implantación de los mismos respecto al diseño e implantación de las aplicaciones informáticas.
e. Definir la tipología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
f. Elaborar informes periódicos de seguridad, conforme a la normativa vigente, para el Comité de Seguridad que incluyan los incidentes más relevantes de cada período, así como cualquier otra documentación de apoyo que el Comité necesite recabar dentro del ámbito de actuación del responsable de seguridad.
g. Supervisar el cumplimiento de la legislación vigente, normas, estándares y buenas prácticas aplicables en materia de seguridad de la información.
h. Promover y proponer auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a los responsables del servicio o tratamiento y a los responsables de la información y del fichero para que adopten las medidas correctoras adecuadas.
i. Realizar la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad, y en particular, asesorar, en colaboración con el responsable del sistema, a los responsables de la información y a los responsables del servicio en la realización de los preceptivos análisis de riesgos, y revisar el proceso de gestión del riesgo, elevando un informe anual al Comité de Seguridad de la Información.

5. *Responsable de los Sistemas (RSIS).* Será designado por el titular del Área con competencias en Nuevas Tecnologías. Sus funciones serán:

a. Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento, implantando las medidas seguridad que requieren los servicios, siguiendo las indicaciones del responsable de seguridad. Para ello, deberán aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema y asesorar a los responsables de la información y a los responsables del servicio en la realización de los análisis de riesgos.
b. Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
d. Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el responsable de dicha información o servicio, según proceda, y con el responsable de seguridad.

6. Administrador de la Seguridad del Sistema (*ASS*). Será designado por el titular del Área con competencias en Nuevas Tecnologías. Sus funciones serán:

a. Implementar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.

b. Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
c. Gestionar las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
d. Aplicar los Procedimientos Operativos de Seguridad.
e. Aprobar los cambios en la configuración vigente del Sistema de Información.
f. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
g. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
h. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
i. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
j. Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
k. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

En la siguiente tabla se relacionan las diferentes tareas de seguridad para cada uno de los roles el ENS:

Tarea	Responsable
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o el Comité de Seguridad de la Información
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	Elabora RSEG aplica ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: comité se seguridad // aprueba: Presidencia
Normativa de seguridad	elabora RSEG; aprueba: comité de seguridad de la información
Procedimientos operativos de seguridad	Elabora RSIS; aprueba RSEG, aplica ASS
Estado de la seguridad del sistema	Monitoriza ASS reporta: RSEG

Planes de mejora de la seguridad	elaboran: RSIS + RSEG // aprueba: comité de seguridad de la información
Planes de concienciación y formación	elabora: RSEG // aprueba: comité de seguridad, promueven: RINFO
Planes de continuidad	elabora: RSIS // valida: RSEG // coordina y aprueba: comité de seguridad; ejercicios: RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS // aprueba: RSEG

En la siguiente tabla se muestra la relación de acciones para respuesta a incidentes de seguridad y su responsable

Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los sistemas bajo su responsabilidad.	ASS
Comunicar el incidente a la AEPD en caso de que estén involucrados datos de carácter personal	DPD
Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo	ASS
Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).	ASS
Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).	ASS
Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados	ASS
Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.	RSEG
Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro	RSEG
Planificar la implantación de las salvaguardas en el sistema.	RSIS
Ejecutar el plan de seguridad aprobado.	RSIS
Aprobar el plan de mejora de la seguridad, con su dotación presupuestaria correspondiente.	Comité de Seguridad de la Información

La tabla siguiente muestra la matriz de Responsabilidades de los distintos actores en relación con la seguridad de la información:

R. - Es responsable de la realización de la tarea señalada.
A. - Es responsable de aprobar la tarea a realizar, haciéndose responsable de ella una vez aprobada.
C. - Es consultado y se le informa del trabajo hecho.
I. - Es informado sobre el proceso y sus resultados.

Tarea	Dirección	DPD	RINF	RSER	RSEG	RSIS	ASS
Niveles de seguridad requeridos por la información		I	A	I	R	C	
Niveles de seguridad requeridos por el servicio		I	I	A	R	C	
Determinación de la categoría del sistema		C	I	I	A/R	I	
Análisis de riesgos		C	I	I	A/R	C	
Declaración de aplicabilidad		I	I	I	A/R	C	
Medidas de seguridad adicionales					A/R	C	
Configuración de seguridad			I	I	A	C	R
Aceptación del riesgo residual		C	A	A	R	I	
Documentación de seguridad		I			A/R	C	I
Política de seguridad	A	I			R	C	I
Normativa de seguridad	A	I			A/R	C	I
Procedimientos de seguridad		I			C	A	I
Implantación de las medidas de seguridad		I	I	I	C	A	R
Supervisión de las medidas de seguridad		I			A	C	R
Estado de seguridad del sistema	I	I	I	I	A	I	R
Planes de mejora de la seguridad		I			A	C	
Planes de concienciación y formación		C			A	C	
Planes de continuidad					C	A	
Suspensión temporal del servicio	A	I	C	C	C	R	
Seguridad en el ciclo de vida					C	A	

3. Resolución de conflictos.

1. En caso de conflicto entre los diferentes responsables que componen la estructura organizativa para la gestión de la seguridad de la información, éste será resuelto por su superior jerárquico común. Si no existiera, deberá resolver el Comité de Seguridad de la Información.

2. En caso de conflictos entre los responsables que componen la estructura organizativa de la política de seguridad de la información, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

ANEXO 1

RESPONSABLES ASOCIADOS AL ENS y RGPD/LOPD

1. *Responsables de la información*. Son los titulares de cada área de la Diputación y de los Organismos Asociados, o persona en quien delegue.

2. *Delegado de Protección de Datos*. Es la persona física u órgano colegiado designado por el titular del Área con competencias en Nuevas Tecnologías, o persona jurídica contratada al amparo 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

3. *Responsables del servicio y tratamiento.* Son los responsables asignados a cada actividad de tratamiento de las existentes en el registro de actividades de tratamiento de la Diputación Provincial y Organismos asociados. Serán nombrados por los responsables de la información dentro de cada área de la Diputación y de los Organismos Asociados.

4. *Responsable de Seguridad.* Es la persona física u órgano colegiado designado por el titular del Área con competencias en Nuevas Tecnologías, o persona jurídica contratada al amparo del Real Decreto 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

5. *Responsable de los Sistemas.* Es el responsable del Servicio de Nuevas Tecnologías o persona en quien delegue.

6. Administrador de la Seguridad del Sistema (*ASS*). Es personal técnico cualificado del Servicio de Nuevas Tecnologías con experiencia en telecomunicaciones y sistemas. Será designado por el titular del Área con competencias en Nuevas Tecnologías, a propuesta del Jefe del Servicio de Nuevas Tecnologías.