ADMINISTRACIÓN LOCAL

DIPUTACIÓN PROVINCIAL DE HUESCA

NUEVAS TECNOLOGÍAS

5279

ANUNCIO

APROBACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA DIPUTACIÓN PROVINCIAL DE HUESCA

Por Decreto n.º 3383, de 21 de octubre de 2024, el Presidente de la Diputación Provincial de Huesca ha aprobado la Política de Seguridad de la Información de la Diputación de conformidad con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, cuyo texto íntegro consta en el expediente, adjuntando a este anuncio el texto a efectos de publicación para general conocimiento.

Huesca, 22 de octubre de 2024. El Presidente, Isaac Claver Ortigosa.

Seguridad de la Información

DIPUTACIÓN HUESCA

Política de Seguridad de la Información

ENS
Real Decreto 311/2022

ÍNDICE

1 INFORMACIÓN DEL DOCUMENTO

Control de versiones de la Política de Seguridad de la Información

FECHA	VERSIÓN	DESCRIPCIÓN DE CAMBIOS
15/11/21	1	Versión inicial del documento
21/04/22	2	Actualización de los miembros del Comité
17/10/24	3	Adecuación al Real Decreto 311/2022

Listado de distribución de la Política de Seguridad de la Información

	PUESTO	CORREO ELECTRÓNICO
Propuesta Comité de Seguridad y Protección de Datos, de acuerdo con el Decreto n.º 995 de 21/04/2022 de Diputación Provincial de Huesca	Comité de Protección de Datos y Seguridad de la Información	Secretaria
Propuesta Comité de Seguridad y Protección de Datos, de acuerdo con el Decreto n.º 2333 de fecha 25/07/2023 de Diputación Provincial de Huesca	Comité de Protección de Datos y Seguridad de la Información	Secretaria

Estado del Procedimiento de la Política de Seguridad de la Información

VERSIÓN	ESTADO	ELABORADO	REVISADO	APROBADO
2		Fecha: 21/04/23 Jefe de los Servicios Informáticos y Responsable de Seguridad de la Información.	Fecha: 25/04/23 Jefe de los Servicios Informáticos y Responsable de Seguridad de la Información.	Fecha: 9/05/23 Presidente de la Diputación Provincial de Huesca
3		Fecha: 30/09/24 Jefe de los Servicios Informáticos y Responsable de Seguridad de la Información.	Fecha: 30/09/24 Jefe de los Servicios Informáticos y Responsable de Seguridad de la Información.	Fecha: 21/10/24 Presidente de la Diputación Provincial de Huesca

2 APROBACIÓN Y ENTRADA EN VIGOR

Texto revisado por el Comité de Protección de Datos y Seguridad de la Información y aprobado el día 21 de octubre de 2024 por el Presidente de la Diputación Provincial de Huesca.

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde la fecha de aprobación por el Presidente de la Diputación y hasta que sea reemplazada por una nueva Política.

3 INTRODUCCIÓN

El desarrollo de la Administración Electrónica implica el tratamiento de gran cantidad de información por parte de los sistemas de tecnologías de la información y de las comunicaciones. La información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. El Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Al objeto de dar cumplimiento al ENS, la Diputación Provincial de Huesca, conocedora de los riesgos que pueden afectar a los sistemas de información, que soportan los trámites electrónicos puestos a disposición a la ciudadanía, y teniendo en cuenta que ésta pone a su disposición su activo más valioso "su propia Información" es consciente de que éstos deben ser administrados con la suficiente diligencia, y que se deben de tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

De este modo, todos los departamentos y/o áreas de la Diputación Provincial de Huesca, que se encuentran dentro del ámbito del ENS, tienen presente que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, Para la Diputación Provincial de Huesca, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el Artículo 7 del ENS.

3.1 Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Diputación Provincial de Huesca implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la Diputación Provincial de Huesca:

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

- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.2 Detección

La Diputación Provincial de Huesca establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS (Vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS. Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

3.3 Respuesta

La Diputación Provincial de Huesca establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

3.4 Recuperación

Para garantizar la disponibilidad de los servicios, la Diputación Provincial de Huesca dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

4 MISIÓN DE LA DIPUTACIÓN PROVINCIAL DE HUESCA

La Diputación Provincial de Huesca pone a disposición de la ciudadanía la realización de trámites online con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la eficacia de la acción pública.

Potenciando por otro lado también, el uso de las nuevas tecnologías en la Diputación y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con la Diputación, reduciendo así los tiempos de espera y de resolución de trámites solicitados por éstos.

Establece igualmente vías de comunicación con la ciudadanía través de su página web, publicando comunicados, subvenciones, becas y otra información de interés

5 ALCANCE

Esta Política se aplicará a los siguientes sistemas:

1) los sistemas de información del portal de la Diputación Provincial de Huesca y el Instituto de Estudios Altoaragoneses.
2) los portales de todo ayuntamiento, entidad local y comarca de la provincia de Huesca que estén alojados en los sistemas de Diputación Provincial de Huesca

Y que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

En relación con los portales,

- se incluyen todos aquellos servicios e información directamente ofrecidos por el portal
- no se incluyen aquellos servicios e información alojados en otros dominios, para los cuales el portal sólo ofrece servicio de reenvío.

Todos los miembros de la Diputación Provincial de Huesca, afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad, siendo responsabilidad del Comité de Protección de Datos y Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

La presente Política de Seguridad será de aplicación para todos los sistemas de información y usuarios de la Diputación Provincial que no dispongan de políticas específicas vigentes.

6 MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades de la Diputación Provincial de Huesca, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía está integrado por las siguientes normas:

a) 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.
b) Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
c) Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
d) Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
e) Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
f) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
g) 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).
h) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
i) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
j) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
k) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
l) Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local
m) Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.

n) 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.

o) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

p) Reglamento de Administración Electrónica de la Diputación Provincial de Huesca, publicado en el BOPH n.º 138, de fecha 21 de julio de 2020, modificado según publicación en el BOPH n.º 83, de fecha 2 de mayo de 2024).

q) Reglamento de asistencia jurídica, tributaria, económico-financiera y técnica de la Diputación provincial de Huesca a las Entidades Locales Altoaragonesas, publicado en el BOPH n.º 14, de fecha 24 de enero de 2023.

r) Decreto 2997 de noviembre de 2013, publicado en BOPH de fecha 15 de enero de 2014, por el que se constituye el Comité de Seguridad y de las distintas responsabilidades.

s) Decreto nº 3288 de fecha 10 de diciembre de 2020, que designa al Comité como Responsable del servicio (ENS) y Responsable de la información (ENS), con las funciones que en el mismo se detallan.

t) Decreto nº 363 de 8 de febrero de 2021, donde se actualiza la composición y funciones del Comité de Protección de Datos y Seguridad de la Información,

u) Decreto n.º 995 de 21 de abril de 2022, donde se actualiza la composición y funciones del Comité de Protección de Datos y Seguridad de la Información.

v) Decreto n.º 2333 de 25 de julio de 2023, donde se actualiza la composición del Comité de protección de Datos y Seguridad de la Información.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la Diputación Provincial de Huesca derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política.

7 ORGANIZACIÓN DE LA SEGURIDAD

7.1 Seguridad como un proceso integral

La Diputación de Huesca para lograr el cumplimiento de los artículos del 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, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral (artículo 6) y mínimo privilegio (artículo 20)

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

7.2 Reevaluación periódica (artículo 10) e integridad y actualización del sistema (artículo 21)

La Diputación de Huesca ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal. Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

7.3 Gestión de la seguridad basada en los riesgos (artículo 7) y análisis y gestión de riesgos (artículo 14)

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y /o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Protección de Datos y Seguridad de la Información. El Comité dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.

El Comité de Protección de Datos y Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas. Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional. En particular, para realizar el análisis de riesgos se utiliza la metodología MAGERIT metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

7.4 Incidentes de seguridad (artículo 25), prevención, reacción y recuperación (artículo 8)

La Diputación de Huesca ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la

Diputación de Huesca implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

Diputación de Huesca establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Para garantizar la disponibilidad de los servicios, Diputación de Huesca dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

7.5 Líneas de defensa (artículo 9) y prevención ante otros sistemas interconectados (artículo 23)

Diputación de Huesca ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

7.6 Diferenciación de responsabilidades (artículo 11) y organización e implantación del proceso de seguridad (artículo 13)

Diputación de Huesca ha organizado su seguridad comprometiendo a todos los miembros de corporación, mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de “ORGANIZACIÓN DE LA SEGURIDAD” del presente documento.

7.7 Autorización y control de los accesos (artículo 17)

Diputación de Huesca ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

7.8 Protección de las instalaciones (artículo 18)

Diputación de Huesca ha implementado mecanismo de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante

perímetros de seguridad, controles físicos y protecciones generales en áreas.

7.9 Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 19)

Diputación de Huesca tendrá en cuenta, para la adquisición de productos 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 Seguridad.

7.10 Protección de la información almacenada y en tránsito (artículo 22) y continuidad de la actividad (artículo 26)

Diputación de Huesca ha implementado mecanismos para proteger la información almacenado o en tránsito especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

También ha desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de sus competencias. De igual modo, se han implementado mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren, para garantizar que toda información en soporte no electrónico relacionada estará protegida con el mismo grado de seguridad que la electrónica.

7.11 Registros de actividad (artículo 24)

Diputación de Huesca ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

Mejora continua del proceso de seguridad (artículo 27)

El Diputación de Huesca actualizará y mejorará de forma continua el proceso de seguridad integral implantado, aplicando los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de las tecnologías de la información.

8 RESPONSABILIDADES ASOCIADAS AL ESQUEMA NACIONAL DE SEGURIDAD

8.1 Funciones y responsabilidades de las figuras

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de las figuras.

Esta información se aprobó mediante los siguientes Decretos, accesibles y verificables como se indica:
Decreto N.º 2284, de fecha 23 de septiembre de 2019.
https://dphuesca.sedipualba.es/csv

Código seguro de verificación: PAMCLU-RTJK6JL3

Decreto N.º 3288 de 10 de diciembre de 2020 de Diputación Provincial de Huesca
https://dphuesca.sedipualba.es/csv

Código seguro de verificación: HHAAKYEUWTRNTV23T2KR

Decreto N.º 2333, de fecha 25 de julio de 2023
https://dphuesca.sedipualba.es/csv

Código seguro de verificación: HHAC DQVK WV3M 3DTE WQ3X

8.1.1 Funciones del Comité de Protección de Datos y Seguridad de la Información.

El Decreto n.º 2333, de fecha 25 de julio de 2023, establece:

Las funciones del Comité de Protección de Datos y Seguridad de la Información serán las siguientes:

- Atender las solicitudes de la Diputación y de las diferentes Áreas en materia de Seguridad de la Información, informando regularmente de su estado.
- Proponer medidas necesarias para el cumplimiento del ENS, de acuerdo con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como para el cumplimiento de la normativa de protección de datos personales.
- Asesorar al Presidente sobre los conflictos de responsabilidad que puedan aparecer en la materia entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Protección de Datos y Seguridad de la Información. Para ello se encargará de:
  - Coordinar los esfuerzos de las diferentes áreas en la materia, para evitar duplicidades.
  - Proponer planes de mejora y velar porque la protección de datos y la seguridad de la Información se tenga en cuenta en todos los proyectos desde su inicio hasta su ejecución.
  - Realizar un seguimiento de los principales riesgos residuales y recomendar posibles actuaciones respecto de ellos. En este sentido se incluye el análisis y, en su caso, aprobación de los análisis de riesgos y Evaluaciones de Impacto en materia de Protección de Datos Personales realizados.
  - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
  - Elaborar y revisar regularmente la Política de Protección de Datos y la de Seguridad de la Información para su aprobación por el Presidente, así como otros documentos relacionados.
- Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información y de protección de datos personales.
- Informar sobre la priorización de actuaciones en materia de seguridad cuando los recursos

sean limitados.

8.1.2 Funciones del Responsable de los Servicios (ENS) y Responsable de la Información (ENS)

El Anexo I del Decreto n.º 3288, de fecha 10 de diciembre de 2020, designa al Comité de Protección de Datos y Seguridad de la Información como Responsable de los Servicios (ENS) y Responsable de la Información (ENS), y le asigna las siguientes responsabilidades como tal:

- Identificar y aprobar formalmente los niveles de seguridad de la información, dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, previa propuesta del Responsable de Seguridad de la información.
- Determinar los requisitos de seguridad de los servicios prestados a partir de la información y los niveles de seguridad establecidos.
- Aceptar los niveles de riesgo residual que afectan al servicio y a la información.
- Poner en comunicación del Responsable de Seguridad ENS, cualquier variación respecto a la información y los servicios de los que es responsable, especialmente la incorporación de nuevos servicios o información a su cargo.
- Informar sobre los derechos de acceso al servicio y a la información

8.1.3 Funciones del Responsable de Seguridad (ENS)

- Decidir las medidas organizativas y técnicas exigibles para garantizar la protección de datos y la seguridad de la información, con base en los requisitos fijados por el responsable funcional del tratamiento y de la información.
- Mantener y verificar el nivel adecuado de seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Aprobar los cambios en el sistema de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución de la determinación de la categoría del sistema, del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad adicionales, determinar configuraciones necesarias de seguridad y elaborar documentación del sistema.
- Coordinar los análisis de riesgos y las evaluaciones de impacto, así como las medidas de seguridad necesarias para cada tratamiento.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Protección de Datos y Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y en los planes de continuidad, procediendo a su validación y seguimiento, así como de concienciación, formación y capacitación del personal.
- Gestionar las revisiones externas o internas del sistema, así como los procesos de certificación y validar los planes de continuidad.
- Elevar al Comité de Protección de Datos y Seguridad de la Información la aprobación de cambios y otros requisitos del sistema.
- Difundir en la Diputación las normas y procedimientos contenidos en la Política de Protección de Datos y Seguridad de la Información.
- Realizar auditorías internas, así como ordenar, supervisar y colaborar en las auditorías externas necesarias.

- Proponer, elaborar, actualizar y hacer seguimiento de las políticas y directrices concretas en materia de protección de datos y seguridad de la información, dentro de su ámbito de responsabilidad.
- Colaborar con la Unidad de Protección de Datos en todo lo que sea necesario para el buen desarrollo de sus funciones e informar sobre el estado de la protección de datos y seguridad de la información de la Diputación.
- Notificar a la autoridad de control las violaciones de seguridad y los incidentes que se produzcan cuando dicha comunicación sea obligatoria, en colaboración con el Delegado de Protección de Datos.
- Actuará como punto de contacto POC con objeto de centralizar las comunicaciones y que estas sean claras y se encuentre armonizadas con los requisitos para dar cumplimiento con el Real Decreto por el cual se regule el Esquema Nacional de Seguridad para la seguridad de la información tratada y su supervisión dentro de los servicios prestados por la Diputación.

8.1.4 Funciones del Responsable del Sistema (ENS)

- Paralizar o suspender al acceso a la información o prestación de servicio si conoce que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y la 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.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable de Seguridad y/o Comité de Protección de Datos y Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y en los planes de continuidad.
- Llevar a cabo las funciones de administrador de seguridad del sistema:
    - gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - aprobar cambios en la configuración del sistema de información.
    - asegurar que los controles de seguridad son cumplidos.
    - asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
    - 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.
    - monitorizar el estado de seguridad, proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

8.1.5 Funciones del Delegado de Protección de Datos

Esta información contenida en la Política de Protección de Datos, aprobada por Decreto n.º 2949, de fecha 20 de noviembre de 2020 - SEFYCU 2291708, páginas 12 y 13. La

información es accesible y verificable como se indica:

https://dphuesca.sedipualba.es/csv

Código seguro de verificación: HHAA HDLF MQUQ 3XUA 7QNQ

8.2 Composición del Comité de Protección de Datos y Seguridad de la Información

Procedimientos de designación

La Diputación Provincial de Huesca procede a realizar la constitución del Comité y de las distintas responsabilidades en el Decreto n.º 2997, de noviembre de 2013. Dicha composición sufre las siguientes modificaciones:

- Decreto 2284, de 23 de septiembre de 2019: se integra al DPD y a la Responsable de protección de datos, cambiando su denominación a CPDSI.
- Decreto 2525, de fecha 11 de octubre de 2019: se rectifica error en suplencia del Responsable de Seguridad.
- Decreto 2526, de fecha 11 de octubre de 2019: se actualizan roles y funciones.
- Decreto nº 3288, de fecha 10 de diciembre de 2020: se designa al CPDSI como Responsable de la información ENS y como Responsable de los servicios ENS.
- Decreto nº 363, de fecha 8 de febrero de 2021; actualización composición y funciones del Comité.
- Decreto n.º 995, de fecha 21 de abril de 2022: nueva actualización composición y funciones del Comité.
- Decreto n.º 2333, de 25 de julio de 2024: actualiza composición Comité por cambio de Corporación.

Composición vigente en el Decreto n.º 2333, de fecha 25 de julio de 2023

https://dphuesca.sedipualba.es/csv

Código seguro de verificación: HHAC DQVK WV3M 3DTE WQ3X

Los miembros y las funciones del Comité de Protección de Datos y Seguridad de la Información, se aprobaron en Decreto n.º 2333, de fecha 25 de julio de 2023. Su composición es la siguiente:

- Presidente del Comité: Vicepresidente primero de la Diputación Provincial como titular y Diputada-Delegada de Recursos Humanos y Servicios Sociales como suplente.
- Secretario/a: Jefe/a de la Sección de Régimen Interior como titular (RPT n.º 340) y Jefe/a de Negociado de la Sección de Régimen Interior y Bienestar Social como suplente (RPT n.º 9).
- Vocales:
  - Responsable jurídico: Secretario/a General como titular (RPT n.º 1), y Letrado/a Jefe/a del Servicio de Asesoría Jurídica como suplente (RPT n.º 28).
  - Responsable de Protección de Datos: Jefe/a Servicio de Secretaría como titular (RPT n.º 2), Secretario/a-Interventor/a con funciones de Letrado del Servicio de Asistencia a municipios como suplente (RPT n.º 298).

- Responsable de Seguridad de la Información ENS: el/la Jefe/a de los Servicios Informáticos como titular (RPT n.º 112), y el/la Técnico de Telecomunicaciones y Sistemas como suplente (RPT n.º 309).
- Delegado de Protección de Datos de la Diputación como titular (RPT n.º 543), y Secretario/a-Interventor/a del Servicio de Asistencia a municipios como suplente (RPT n.º 30).

8.2.1 Identificación de las personas que conforman el Comité

La vía para recopilar la información actualizada de la relación cargos del Comité – personas, pasa por consultar a los diversos departamentos involucrados, como se indica a continuación.

Tipo de cargo	Vía de consulta
Cargos políticos (Diputados)	Consultar a la Sección de Régimen Interior
Delegado de Protección de Datos	Consultar a la Sección de Contratación
Resto de funcionarios	Consultar a la Sección de Recursos Humanos

9 DATOS DE CARÁCTER PERSONAL

La Diputación Provincial de Huesca sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido, cumpliendo con los principios previstos en el RGPD. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos. En cumplimiento de lo anterior, por Decreto nº 2949, de fecha 20 de noviembre de 2020, se aprobó la Política de Protección de Datos de la Diputación y su normativa de desarrollo. La Diputación es consciente de que el tratamiento de carácter personal supone unos riesgos inherentes asociados y en consecuencia dispone de un análisis de riesgos dedicado especialmente a ello, así como evaluaciones de impacto en materia de protección de datos (EIPD) para los casos de tratamientos de alto riesgo.

10 OBLIGACIONES DEL PERSONAL

Todos los miembros del Diputación Provincial de Huesca, que se encuentran dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez cada al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Diputación Provincial de Huesca, en particular al de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11 PROFESIONALIDAD

Todos los miembros de la organización, que se encuentran dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, en particular al de nueva incorporación. Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la

necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El personal responsable de los sistemas de información será personal cualificado.

La Diputación exigirá, 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

12 GESTIÓN DE RIESGOS

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

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

El proceso de gestión de riesgos comprenderá las siguientes fases:

1. Categorización de los sistemas.
2. Análisis de riesgos.
3. El Comité de Seguridad procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos se utiliza la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

13 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (políticas, protocolos, procedimientos, instrucciones técnicas, etc.)

Del mismo modo, esta Política de Seguridad de la Información complementa las políticas de la Diputación Provincial de Huesca en materia de protección de datos de carácter personal.

La Normativa de Seguridad estará a disposición de todos los miembros de la Institución que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en la Intranet.

14 TERCERAS PARTES

Cuando la Diputación Provincial de Huesca preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Diputación Provincial de Huesca utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

15 DISPOSICIÓN DEROGATORIA

Esta Política de Seguridad de la Información deroga la Política de Seguridad de la Información de la Diputación aprobada por acuerdo de fecha 17 de enero de 2014 y publicada en el Boletín Oficial de la Provincia de Huesca n.º 37, de fecha 25 de febrero de 2014, así como la Política de Seguridad de la Información de la Diputación aprobada por Decreto n.º 1342, de fecha 16 de mayo de 2022.