JUAN JOSÉ VILLALBA CASAS, SECRETARIO GENERAL DE LA EXCMA. DIPUTACIÓN PROVINCIAL DE PALENCIA

CERTIFICO: Que el Pleno de esta Diputación, en sesión celebrada el 31 de marzo de 2022, adoptó, entre otros, el siguiente acuerdo:

NÚM. 21.- APROBACIÓN DE LA NUEVA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA DIPUTACIÓN DE PALENCIA.

La Política de Seguridad de la Información establece las directrices y principios para garantizar la protección de la información, así como el cumplimiento de los objetivos de seguridad definidos, asegurando la confidencialidad, integridad y disponibilidad de los sistemas de información y, por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables a esta Entidad.

La Diputación de Palencia aprobó en el año 2014 la Política de Seguridad de la Información, que figura publicada en el BOP de 18 de junio de ese año.

Siendo preciso actualizar este documento, atendiendo a las reformas normativas experimentadas a partir de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se ha elaborado un nuevo texto, por lo que el Pleno de la Corporación, con el dictamen favorable de la Comisión Informativa de Hacienda, Cuentas y Presidencia, por unanimidad, acuerda:

1º Aprobar la Política de Seguridad de la Información de la Diputación Provincial de Palencia, cuyo texto figura en anexo.

2º Dejar sin efecto la Política de Seguridad de la Información aprobada por acuerdo del Pleno de la Diputación de 24 de abril de 2014.

3º Dar publicidad a este acuerdo en el BOP, el portal web de la Diputación y portal del empleado.

ANEXO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA DIPUTACIÓN PROVINCIAL DE PALENCIA

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 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad 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 Palencia, 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, todas las áreas y servicios de la Diputación 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, 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 Real Decreto 3/2010, de 8 de enero.

MISIÓN DE LA DIPUTACIÓN PROVINCIAL DE PALENCIA

La Diputación 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, así como potenciando el uso de las nuevas tecnologías en la Diputación y en la propia ciudadanía.

Se persigue, entre otros objetivos, fomentar la relación electrónica de la ciudadanía con la Diputación, reduciendo así los tiempos de espera y de resolución de trámites solicitados por éstos.

ALCANCE

Esta Política se aplicará a los sistemas de información de la Diputación, 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.

Todos los miembros de la Diputación y sus empleados públicos, 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 Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

MARCO NORMATIVO

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

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, modificado por Real Decreto 951/2015, de 23 de octubre.
- 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.
- 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.
- 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.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en la materia.
- Real Decreto-ley 29/2020, de 29 de septiembre, de medidas urgentes en materia de teletrabajo en las Administraciones Públicas y de recursos humanos en el Sistema Nacional de Salud para hacer frente a la crisis sanitaria ocasionada por la COVID-19.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.
- Reglamento por el que se regula la prestación de servicios en la modalidad de teletrabajo en la Diputación de Palencia, aprobado por el Pleno de la Diputación de Palencia el 30 de septiembre de 2021.
- Resolución de la Sra. Presidenta de la Diputación de Palencia de 1 de julio de 2019 “Protocolo y Régimen de uso de sistema de identificación y firma electrónica de los cargos electos y empleados de la Diputación de Palencia”.
- Ordenanza reguladora de la Administración Electrónica de la Diputación Provincial de Palencia.

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

El mantenimiento del marco normativo será responsabilidad del Comité de Seguridad de la Información y se recogerá en un Anexo a este documento, incluidas las instrucciones técnicas de seguridad de obligado cumplimiento, aprobadas y publicadas por la Administración General del Estado, conforme a lo previsto en el artículo 29 del Real Decreto 3/2010, de 8 de enero.

Asimismo, el Comité de Seguridad será responsable de identificar las guías de seguridad del Centro Cristológico Nacional, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

MEDIDAS PARA EL CUMPLIMIENTO DE LAS NORMAS DE SEGURIDAD

La Diputación Provincial de Palencia, para lograr el cumplimiento de los preceptos del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, 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.

1. Seguridad como un proceso integral y seguridad por defecto.

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, conforme al artículo 6 del Real Decreto 3/2010, de 8 de enero. La aplicación del Esquema Nacional de Seguridad a la Diputación Provincial de Palencia estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Conforme al artículo 19 del Real Decreto 3/2010, de 8 de enero, los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

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

b) 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.

c) 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.

d) 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.

2. Reevaluación periódica e integridad y actualización del sistema.

La Diputación Provincial de Palencia ha implementado controles y evaluaciones regulares de la seguridad, incluyendo evaluaciones de los cambios de configuración de forma rutinaria, conforme al artículo 9 del Real Decreto 3/2010, de 8 de enero, 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.

Asimismo, solicitará la revisión periódica por terceros, con el fin de obtener una evaluación independiente.

3. Gestión de personal y profesionalidad.

De conformidad con el artículo 14 del Real Decreto 3/2010, de 8 de enero, todos los empleados de la Diputación Provincial de Palencia, 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 empleados, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo, según establece el artículo 15 del Real Decreto 3/2010, de 8 de enero. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

4. Gestión de la seguridad basada en los riesgos y análisis y gestión de riesgos.

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos, según lo previsto en los artículos 6 y 13 del Real Decreto 3/2010, de 8 de enero.

Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados 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 de ponerlas en conocimiento del Comité de Seguridad de la Información.

5. Prevención, reacción y recuperación. Incidentes de seguridad.

A fin de dar cumplimiento a lo previsto en los artículos 7 y 24 del Real Decreto 3/2010, de 8 de enero, la Diputación Provincial de Palencia ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren 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 Provincial de Palencia 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, así como los roles y

responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produzca 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.

La Diputación Provincial de Palencia 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, la Diputación Provincial de Palencia dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

6. Líneas de defensa y prevención ante otros sistemas interconectados.

De conformidad con lo previsto en el artículo 8 del Real Decreto 3/2010, de 8 de enero, la Diputación Provincial de Palencia 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 trata de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso, según establece el artículo 22 del Real Decreto 3/2010, de 8 de enero, 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. Función diferenciada y organización e implantación del proceso de seguridad.

La Diputación Provincial de Palencia ha organizado su seguridad comprometiendo a todos los empleados, tal como establece el artículo 12 del Real Decreto 3/2010, de 8 de enero, y ha designado diferentes roles de seguridad con responsabilidades claramente diferenciadas,

conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, como se recoge en el apartado 6 del presente documento.

8. Autorización y control de los accesos.

En cumplimiento del artículo 16 del Real Decreto 3/2010, de 8 de enero, la Diputación Provincial de Palencia ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

9. Protección de las instalaciones.

Atendiendo a lo dispuesto en el artículo 17 del Real Decreto 3/2010, de 8 de enero, la Diputación Provincial de Palencia ha implementado mecanismos 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.

10. Adquisición de productos de seguridad y contratación de servicios de seguridad.

Para la adquisición de productos, la Diputación Provincial de Palencia tendrá en cuenta que dichos productos 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, de conformidad con lo previsto en el artículo 18 del Real Decreto 3/2010, de 8 de enero.

11. Protección de la información almacenada y en tránsito y continuidad de la actividad.

A los efectos previstos en el artículo 21 del Real Decreto 3/2010, de 8 de enero, l objeto de La Diputación Provincial de Palencia ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tables, 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, de conformidad con el artículo 25 del Real Decreto 3/2010, de 8 de enero.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de la Diputación Provincial de Palencia. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

12. Registros de actividad.

De conformidad con el artículo 23 del Real Decreto 3/2010, de 8 de enero, la Diputación Provincial de Palencia 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 referido 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 de aplicación.

ORGANIZACIÓN DE LA SEGURIDAD

La Organización de la Seguridad de la Información en la Diputación Provincial de Palencia se estructura en la forma que se indica a continuación.

Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- **Delegado de Protección de Datos (DPD):** Letrado asesor
- **Responsable de los Servicios y Responsables de la Información:** Jefes de Servicio de la Diputación y directores de Organismos Autónomos.
- **Responsable de Seguridad:** Un técnico informático del Servicio de Informática.
- **Responsable del Sistema ENS:** Un técnico informático del Servicio de Informática.

Los Responsables de Seguridad y del Sistema, en función de la complejidad de la organización o del sistema, podrán proponer delegados de sus funciones por áreas o ámbitos diferenciados, los cuales serán designados por la Presidencia o Diputado delegado. Dichos delegados tendrán dependencia funcional directa y serán responsables en el ámbito asignado de las acciones que se hayan delegado en los mismos.

Comité de seguridad de la información.

La Diputación dispondrá de un Comité de Seguridad de la Información, compuesto por los siguientes miembros:

- **Presidente:** *Diputado de Hacienda y Administración General, por delegación de la Presidenta.*
- **Vocales:**
  - *Vicesecretaria*
  - *Delegado de Protección de Datos*
  - *Responsable de Seguridad*
  - *Jefa del Servicio de Informática*
- **Secretaria:** *Jefa del Servicio de Informática.*

El Responsable del Sistema asesorará al Comité en materia de seguridad de la información y asistirá a todas sus reuniones con voz, pero sin voto, para asegurar la independencia de la seguridad, tal y como establece el artículo 10 del Real Decreto 3/2010, de 8 de enero.

Los Responsables de la Información y de los Servicios podrán ser convocados a las reuniones del Comité para informar en los asuntos a tratar.

El Delegado de Protección de Datos se abstendrá de votar en las reuniones del Comité de seguridad de la información cuando se aborden cuestiones relacionadas con el tratamiento de datos de carácter personal. En todo caso, cuando un asunto se someta a votación se hará constar en acta la opinión del Delegado de Protección de Datos.

Podrán crearse grupos de trabajo especializados, de carácter interno, externo o mixto, para auxiliar al Comité en sus tareas.

El Comité de Seguridad de la Información celebrará sus reuniones en las dependencias de la Diputación Provincial de Palencia con periodicidad anual, previa convocatoria al efecto realizada por su Presidente.

Procedimiento de designación

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los responsables identificados en esta Política corresponde a la Presidencia de la Diputación Provincial de Palencia.
Los nombramientos de miembros del Comité, así como los roles de seguridad, serán revisados cada cuatro años o con ocasión de vacante.

Responsabilidades asociadas al Esquema Nacional de Seguridad

1. Funciones de los roles de Seguridad.

Son funciones y responsabilidades de los roles o perfiles de seguridad las siguientes:

- El **Responsable del Servicio** determina los requisitos de seguridad de los servicios prestados dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad ENS, y le corresponde aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
- El **Responsable de la Información** determina los requisitos de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad ENS, y le corresponde aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
- El **Responsable de Seguridad tiene como** funciones principales:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

¬ EL **Responsable del Sistema tiene como** funciones principales:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar 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.
- Prestar al Responsable de Seguridad de la Información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
  - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.

- La 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 los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- 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.
- Cuando la complejidad del sistema lo justifique, el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

2. Funciones del Comité de Seguridad de la Información

El Comité de Seguridad de la Información tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Institución, elevando a la Presidencia aquellos casos a la en los que no tenga suficiente autoridad para decidir.
- Promover la mejora continua del sistema de gestión de la seguridad de la información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar por que la Seguridad de la Información se tenga en cuenta en todos los proyectos 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.
- Realizar un seguimiento de riesgos residuales asumidos y proponer posibles actuaciones respecto de ellos.
- 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 Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación por el órgano competente.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

DATOS DE CARÁCTER PERSONAL

La Diputación Provincial de Palencia solo 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. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista de Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de

datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y su traslación al ordenamiento jurídico español con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas, tales como el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de Delegado de Protección de Datos.

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 seguridad de la Diputación en materia de protección de datos de carácter personal.

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

El Comité de Seguridad de la Información desarrollará, implementará, mantendrá y mejorará un sistema de gestión, conforme a estándares de seguridad internacionales que servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo mejoras de la misma, para su aprobación, en caso necesario, por el Pleno de la Diputación Provincial de Palencia.

TERCERAS PARTES

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

Cuando la Diputación 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, se requerirá un informe del Responsable de Seguridad ENS que precise los riesgos en que se incurre y la forma de tratarlos y la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información ha sido aprobada el día 31 de marzo de 2022 por el Pleno de la Diputación Provincial de Palencia y se publicará en el Boletín Oficial de la Provincia. Tendrá efectividad desde la fecha de aprobación y hasta su modificación o reemplazo por una nueva Política.

Y para que conste, expido la presente certificación con la salvedad a que se refiere el artículo 206 del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, con el Visto Bueno de la Sra. Presidenta.

Firmado electrónicamente por:

MARIA DE LOS ANGELES ARMISEN PEDREJON
Presidenta
05-04-2022

Diputación DE PALENCIA

Firmado electrónicamente por:

Secretario General
Juan José Villalba Casas
05-04-2022

Diputación DE PALENCIA