POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA DIPUTACION PROVINCIAL Y ORGANISMOS DEPENDIENTES

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 Esquema Nacional de Seguridad (en adelante, ENS) tiene por objeto el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos, que permita la adecuada protección de la información. Es de aplicación a las administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados por dichos medios electrónicos.

Además, se pretende proporcionar las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de una serie de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos de manera que permita a los ciudadanos el ejercer sus derechos y a las Administraciones cumplir sus deberes a través de estos medios electrónicos.

Al objeto de dar cumplimiento al ENS, la Diputación Provincial de Valladolid, 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 Valladolid, así como los Organismos Dependientes, que se encuentran dentro del ámbito del ENS, tienen presente que la seguridad relacionada con las Tecnologías de la Información y la Comunicación (en adelante, 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 Valladolid, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y los niveles de prestación de servicio para analizar vulnerabilidades reportadas y detectar cualquier incidente, reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el ENS.

Por su parte 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 (RGPD) crea la figura del Delegado de Protección de Datos, obligatoria para las Administraciones Públicas.

CAPÍTULO I.
Disposiciones Generales

Artículo 1. Objeto

El objeto de este documento comprende los siguientes aspectos:

a. La regularización de la política de seguridad de la información de la Diputación Provincial de Valladolid y Organismos Dependientes.
b. Establecer el marco organizativo de aplicación para la protección de los accesos y servicios gestionados por medio de las tecnologías de la información y comunicación.
c. Garantizar la protección y calidad de la información, la prestación continuada del servicio mediante la supervisión diaria y la solución de los incidentes con la mayor rapidez posible.

Artículo 2. Marco Normativo

La presente política de seguridad se desarrolla en el marco normativo establecido por las siguientes normas y regulaciones:

a. Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de Régimen Jurídico del Sector Público, referenciando esta última, en su artículo 156, al ENS.
b. Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
c. 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 (RGPD).
d. Real Decreto-Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

Artículo 3. Ámbito de aplicación

Esta Política se aplicará a los sistemas de información de la Diputación Provincial de Valladolid y Organismos Dependientes, 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.

Artículo 4. Principios rectores

Las actuaciones y medidas que lleve a cabo la Diputación Provincial de Valladolid para desarrollar la Política de Seguridad cumplirán los siguientes principios rectores:

a. Principio de Confidencialidad: se deberá garantizar que la información sea accesible únicamente para aquellas personas expresamente autorizadas para ello.

b. Principio de Integridad: se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.
c. Principio de Disponibilidad: se garantizará la prestación continua de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada.
d. Principio de Autenticidad: se deberá garantizar que la información se intercambie con los interlocutores idóneos y que los servicios se acrediten correctamente.
e. Principio de Trazabilidad: se deberá garantizar el seguimiento de las operaciones efectuadas sobre la información y los servicios que lo requieran.
f. Principio de Gestión del Riesgo: Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.
g. Principio de mejora continua: se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados en la organización para aumentar la capacidad de adaptación a la constante evolución de los riesgos y del entorno tecnológico.
h. Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.
i. Principio de concienciación y formación: se articularán programas de formación, sensibilización y concienciación para las personas usuarias en materia de seguridad de la información.
j. Principio de cumplimiento normativo: todos los sistemas de información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquella relacionada con la intimidad y la protección de datos de carácter personal y con la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

Artículo 5. Desarrollo

La normativa sobre seguridad de la información es de obligado cumplimiento y se desarrollará en niveles, según el ámbito de aplicación y el nivel de detalle técnico. Dichos niveles de desarrollo son los siguientes:

a. Políticas de seguridad de la información. Este nivel está constituido por el presente documento y el manual de seguridad.
b. Procedimientos de seguridad. Son documentos que describen, explícitamente y paso a paso, cómo realizar una cierta actividad, por ejemplo, gestión de incidentes o copias de seguridad.
c. Instrucciones o procedimientos técnicos. Son propios del área de sistemas y especifican, por ejemplo, los distintos tratamientos asociados a tipologías de incidente.

CAPÍTULO II.
Estructura Organizativa

Artículo 6. Marco Organizativo

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. Los Responsables de Sistemas, Seguridad, Servicios e Información, roles con funciones asociadas a la implantación del Esquema Nacional de Seguridad.
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.

Artículo 7. Funciones y Obligaciones

Las funciones y responsabilidades de cada uno de estos roles se detallan en un documento 'Funciones y Responsabilidades en Seguridad y Privacidad' asociado a la presente política.

CAPÍTULO III.
Revisión y Vigencia

Artículo 8. Revisión de la Política de Seguridad

Será misión del Comité Operativo de Seguridad de la Información, la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Presidente y difundida para que la conozcan todas las partes afectadas.

En dicha revisión se deberán evaluar los siguientes aspectos:

a. La eficacia de la política, número e impacto de los incidentes de seguridad registrados.
b. Coste e impacto de los controles en la eficiencia del desarrollo de las actividades.
c. Los efectos de los cambios en la tecnología.

Artículo 9. Entrada en vigor y vigencia

La Política de Seguridad de la Información es efectiva desde la fecha de su aprobación y hasta que sea reemplazada por una nueva Política.