



La seguridad de los sistemas de información

DEBERÁ CONCEBIRSE COMO UNA ACTIVIDAD INTEGRAL, EN LA QUE NO CABEN ACTUACIONES PUNTUALES, DEBIDO A QUE LA DEBILIDAD DE UN SISTEMA LA DETERMINA SU PUNTO MÁS FRÁGIL



CCN-CERT
Centro Criptológico Nacional

El objeto del presente artículo es responder a diversas concepciones negativas en torno a la LAECSP con el beneficio de la perspectiva que dan el tiempo transcurrido y un punto de vista interno dentro de las Administraciones Públicas. Esto lleva además a reflexionar sobre posibles retos reales que surgen a la hora de su cumplimiento.

La Ley 11/2007 crea las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.

Para ello, en el artículo 4 se establecen unos principios generales que, en relación con la seguridad de los sistemas de información, son los siguientes:

- El respeto al derecho a la protección de datos de carácter personal en los términos establecidos

Administraciones Públicas, en cuya virtud se exigirá, al menos, el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa.

- Principio de proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones.

- Principio de responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones Públicas a través de medios electrónicos.

La utilidad y aplicación de la Ley 11/2007 descansa en gran medida en la confianza que genere en los ciudadanos la relación a través de medios electrónicos.

En el ámbito de las Administraciones Públicas, la consagración del derecho del ciudadano a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene como premisas la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda,

Se deberá prestar la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos

por la Ley Orgánica 15/1999, de Protección de los datos de carácter personal, en las demás Leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar.

- Principio de seguridad en la implantación y utilización de los medios electrónicos por las



incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

A ello pretende dar respuesta el artículo 42.2 de la Ley 11/2007, mediante la creación del Esquema Nacional de Seguridad, cuyo objeto es 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.

La finalidad del Esquema Nacional de Seguridad será, por tanto, la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Esquema Nacional de Seguridad perseguirá fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado

especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas. Se desarrollará y perfeccionará en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan.

En este contexto, se entiende por seguridad la capacidad de las redes o de los sistemas de información para

resistir, con un determinado nivel de confianza, los accidentes, acciones ilícitas o malintencionadas, que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad, de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen, o a través de los que se realiza el acceso.

Como no puede ser de otra manera, el Esquema Nacional de Seguridad tendrá presentes las recomendaciones de la Unión Europea (Decisión de la Comisión de 29 de noviembre de 2001, por la que se modifica su Reglamento interno -2001/844/CE, CECA, Euratom- y Decisión del Consejo de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo /2001/264/EC), la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos y, de forma complementaria, estándares de uso generalizado por los ciudadanos.

Los sistemas de información y comunicaciones de las Administraciones Públicas deberán satisfacer los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permitan una protección adecuada de la información y los servicios, lo que exige incluir el alcance y procedimiento para gestionar la seguridad de los sistemas que tratan información de las Administraciones Públicas en el ámbito de la Ley 11/2007.

El gran reto del Esquema Nacional de Seguridad será conjugar dichos principios y requisitos en un común denominador normativo que tenga en cuenta toda la normativa nacional sobre Administración Electrónica, Protección de Datos de Carácter Personal, Firma Electrónica y



Documento Nacional de Identidad Electrónico, Centro Criptológico Nacional, Sociedad de la Información, Reutilización de la Información en el Sector Público y Órganos Colegiados responsables de la Administración Electrónica; así como la regulación de diferentes Instrumentos y Servicios de la Administración, las Directrices y Guías de la OCDE y disposiciones nacionales e internacionales sobre normalización.

La seguridad de los sistemas de información y comunicaciones de las Administraciones Públicas deberá concebirse como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a

La finalidad del Esquema Nacional de Seguridad será la creación de confianza en el uso de los medios electrónicos

que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

Por ello, se deberá prestar 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 fuentes de riesgo para la seguridad.

Por otra parte, el análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

En resumen, la existencia de políticas y procedimientos de seguridad aplicados por personal con la necesaria concienciación y formación, utilizando productos y tecnologías de seguridad contrastada y por tanto certificada, serán los tres ejes en los que se ha de desarrollar lo contemplado en la Ley 11/2007 y su Esquema Nacional de Seguridad.

Todo ello está alineado con la actividad desarrollada por el Centro Criptológico Nacional desde su creación en 2004, en la que se ha promovido que todos los niveles de la Administración tomen conciencia de los riesgos asociados al uso de las tecnologías de la información, que el personal de cada nivel reciba la formación necesaria para tomar las medidas oportunas para gestionar el riesgo, que se establezcan y ejecuten procedimientos de seguridad y que existan productos de confianza certificada para satisfacer las necesidades de seguridad. ♦