III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

5370 *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.*

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, ENS en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Dicho Real Decreto prevé, en su artículo 29, apartado 2, que el Ministerio de Hacienda y Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante resolución de la Secretaría de Estado de Función Pública, constituyendo elementos esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el ENS.

Así pues, tales instrucciones técnicas de seguridad, enumeradas en la Disposición Adicional cuarta del citado Real Decreto 3/2010, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; Notificación de Incidentes de Seguridad; Auditoría de la Seguridad; Conformidad con el Esquema Nacional de Seguridad; Adquisición de Productos de Seguridad; Criptología de empleo en el Esquema Nacional de Seguridad; Interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar la Comisión Sectorial de administración electrónica, según lo establecido en el citado artículo 29, en relación con lo dispuesto en la Disposición derogatoria única de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y Disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la instrucción técnica de seguridad de Notificación de Incidentes de Seguridad establece los criterios y procedimientos para la notificación por parte de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público al Centro Criptológico Nacional (CCN) de aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan en relación con la categoría del sistema, al objeto de poder dar adecuada respuesta al mandato del Capítulo VII, Respuesta a incidentes de seguridad, del Real Decreto 3/2010, de 8 de enero.

Por otra parte, de acuerdo con el Real Decreto 769/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Función Pública y se modifica el Real Decreto 424/2016, de 11 de noviembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales corresponde a la Secretaría de Estado de Función Pública el impulso, la programación y la supervisión de las actuaciones en ejecución de la política de Gobierno en materia de Administración

cve: BOE-A-2018-5370
Verificable en http://www.boe.es

Digital y del fomento de la administración electrónica, en especial lo referente al proceso de racionalización de las tecnologías de la información y de las comunicaciones, y la adopción de soluciones digitales que permitan la prestación eficiente de los servicios públicos incluyendo los servicios públicos esenciales. Además, dado que la resolución impone obligaciones no solo en el ámbito competencial de esta Secretaria de Estado sino también al Centro Criptológico Nacional (CCN) integrado en el CNI, organismo adscrito al Ministerio de la Presidencia y para las Administraciones Territoriales procede recabar el parecer del citado Departamento.

Esta Resolución se aprueba en aplicación de lo dispuesto en el artículo 29, apartado 2 del Real Decreto 3/2010, de 8 de enero, a propuesta de la Comisión Sectorial de Administración Electrónica y habiéndose solicitado informe al Ministerio de la Presidencia y para las Administraciones Territoriales.

En virtud de lo anterior, esta Secretaría de Estado resuelve:

Primero.

Aprobar la Instrucción Técnica de Seguridad «Notificación de incidentes de seguridad», cuyo texto se incluye a continuación.

Segundo.

Ordenar su publicación en el «Boletín Oficial del Estado».

La Instrucción Técnica de Seguridad de Notificación de incidentes de seguridad de los sistemas de información que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 13 de abril de 2018.–La Secretaria de Estado de Función Pública, Elena Collado Martínez.

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

ÍNDICE

I. Objeto

La Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad tiene por objeto, según lo dispuesto en el Capítulo VII del Real Decreto 3/2010, de 8 de enero, la notificación y gestión de incidentes de seguridad en los sistemas de información de las entidades del Sector Público del ámbito de aplicación de dicho cuerpo legal, cuando tales incidentes tengan un impacto significativo en la seguridad de la información que manejan o los servicios que prestan, en relación con la categoría del sistema y con independencia de los requerimientos adicionales que cada organismo o entidad implemente para adaptarlos a sus entornos singulares.

cve: BOE-A-2018-5370
Verificable en http://www.boe.es

II. Ámbito de aplicación

La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en los ámbitos subjetivo y objetivo de aplicación del Real Decreto 3/2010, de 8 de enero, según dispone el artículo 3 del mismo, así como al resto de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

III. Criterios de determinación del nivel de Impacto

Una vez detectado un incidente se utilizará la Guía CCN-STIC 817 Esquema Nacional de Seguridad - Gestión de Ciberincidentes, para clasificarlo de acuerdo con su tabla Criterios de determinación del nivel de impacto potencial. El nivel de impacto potencial de los ciberincidentes en la organización, será: Irrelevante, Bajo, Medio, Alto, Muy Alto y Crítico.

IV. Notificación obligatoria de los incidentes con nivel de impacto Alto, Muy alto y Crítico

IV.1 Las notificaciones efectuadas por las entidades del ámbito de aplicación de la presente Instrucción Técnica de Seguridad al Centro Criptológico Nacional (CCN), en el marco de la articulación de respuesta a los incidentes de seguridad y la prestación de servicios de respuesta por parte del Equipo de Respuesta a Incidentes de Seguridad del CCN-CERT, (Centro Criptológico Nacional - Computer Emergency Response Team) se realizará en los términos indicados en los artículos 36 y 37 del Real Decreto 3/2010, de 8 de enero.

IV.2 Para ello, se notificarán los incidentes de seguridad que tengan un impacto significativo en la seguridad de la información manejada o los servicios prestados en relación con la categoría del sistema, determinada de acuerdo con lo dispuesto en los artículos 43, 44 y Anexo I del Real Decreto 3/2010, de 8 de enero. Se dice que un incidente tiene impacto significativo cuando, por su magnitud o características, impide el tratamiento de la información o los servicios prestados. A estos efectos, se considerará que tienen un impacto significativo los niveles Alto, Muy Alto y Crítico recogidos en la tabla Criterios de Determinación del Nivel de Impacto de la Guía CCN-STIC 817.

IV.3 En todo caso, serán de obligatoria notificación al CCN en el momento en que se produzcan, los incidentes de seguridad que por su nivel de impacto potencial sean calificados con el nivel de CRÍTICO, MUY ALTO o ALTO, mediante el empleo de las herramientas desarrolladas al efecto de la notificación de incidentes.

V. Evidencias a entregar en el caso de incidentes nivel Alto, Muy alto y Crítico

V.1 Tras la detección de un incidente de seguridad y con carácter inmediato se recopilarán evidencias del incidente, que serán documentadas y custodiadas de forma que se pueda determinar el modo de obtención, se garantice la cadena de custodia, y respetando el ordenamiento jurídico que resulte de aplicación. En la recolección y custodia de evidencia se aplicarán las recomendaciones establecidas al efecto en la Guía CCN-STIC 817.

V.2 De acuerdo con lo dispuesto en el artículo 37 del Real Decreto 3/2010, de 8 de enero, el CCN podrá recabar éstas y cualesquiera otras informaciones que se consideren relevantes para el análisis del incidente, así como los soportes informáticos que se estimen necesarios para la investigación, sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y su normativa de desarrollo, así como la posible confidencialidad de datos de carácter institucional u organizativo.

cve: BOE-A-2018-5370
Verificable en http://www.boe.es

VI. Obligación de remisión de estadísticas de incidentes

De conformidad con lo dispuesto en el artículo 24.2 del Real Decreto 3/2010, de 8 de enero, el registro de todos los incidentes de seguridad que se produzcan y de las acciones de tratamiento que se sigan, será utilizado para la mejora continua de la seguridad del sistema, a cuyo fin las entidades del ámbito de aplicación de la presente Instrucción Técnica de Seguridad elaborarán estadísticas de incidentes de seguridad que, al menos, con carácter anual, remitirán al CCN, incluyendo el resto de la antedicha información relativa a los incidentes.

VII. Notificación de impactos recibidos

Una vez determinado el impacto del ciberincidente y calificado como de carácter significativo a los efectos de lo establecido en el artículo 36 del ENS, será notificado al CCN en los términos previsto en el artículo IV de la presente Instrucción Técnica de Seguridad.

VIII. Desarrollo de herramientas automatizadas para facilitar las notificaciones

El CCN ha desarrollado la herramienta LUCIA, Listado Unificado de Coordinación de Incidentes y Amenazas) con el propósito de automatizar los mecanismos de notificación, comunicación e intercambio de información sobre incidentes de seguridad, de acuerdo a lo establecido en la Guía CCN-STIC 817. Esta herramienta se mantendrá permanentemente actualizada para atender dicho propósito.

IX. Régimen legal de las notificaciones y comunicación de información

Para la articulación de respuesta a los incidentes de seguridad y gestión de ciberincidentes a los que se refiere la presente Resolución, el suministro de información por las entidades del ámbito de aplicación de la presente Instrucción Técnica de Seguridad al CCN, motu proprio o a su requerimiento, se realizará teniendo en cuenta lo siguiente:

a) La comunicación de información que tenga la consideración de datos de carácter personal se efectuará con pleno cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y su normativa de desarrollo, atendiendo a que la comunicación de datos se realiza para el cumplimiento de fines directamente relacionados con la función legítima de las entidades cedentes y del CCN como cesionario, sin que sea preciso el consentimiento del afectado toda vez que tales datos han sido recabados para el ejercicio de las funciones propias de unos y otro, en los términos previstos en el artículo 6.2 de la citada Ley Orgánica.

Tampoco resultará de aplicación lo dispuesto en los párrafos uno y dos del artículo 5 de la reiterada Ley Orgánica, en base a lo dispuesto en su artículo 24.1, por afectar a la Ciberseguridad, como ámbito de especial interés para la Seguridad Nacional.

b) La comunicación de información de datos de carácter institucional u organizativo a la que se refiere el artículo 37.1.a) último párrafo, del Real Decreto 3/2010, de 8 de enero, será suministrada y comunicada en función de su confidencialidad, atendiendo a lo dispuesto en el artículo 43 y anexo I, en relación con el citado artículo 37.1.a) del ENS.

X. Disposición adicional

X.1 Las referencias contenidas en la presente Instrucción a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo se entenderán hechas, a partir del 25 de mayo de 2018, al 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

cve: BOE-A-2018-5370
Verificable en http://www.boe.es

la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

X.2 Se añade un segundo párrafo al apartado VII de la Instrucción, con efectos a partir del 25 de mayo de 2018, con la siguiente redacción:

> «Cuando el incidente afecte a datos personales la notificación a la autoridad de control competente se realizará con independencia del nivel de impacto del incidente en el Esquema Nacional de Seguridad. En aquellos casos en los que el impacto de un incidente o violación de la seguridad afecte a datos personales, la notificación se realizará según lo previsto en el artículo 33 del Reglamento General de Protección de Datos.»

X.3 La referencia contenida en el apartado IX, letra a), primer párrafo, de la Instrucción, al artículo 6.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se entenderá realizada, a partir del 25 de mayo de 2018, al artículo 6.1.c) del Reglamento General de Protección de Datos.

X.4 La referencia contenida en el apartado IX, letra a), segundo párrafo, a «los párrafos uno y dos del artículo 5 de la reiterada Ley Orgánica, en base a lo dispuesto en su artículo 24.1», se entenderá sustituida, a partir del 25 de mayo de 2018, por «el capítulo III del Reglamento General de Protección de Datos, en base a lo dispuesto en el artículo 23.1.a) del mismo».

cve: BOE-A-2018-5370
Verificable en http://www.boe.es