III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

4573 *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.*

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, de 8 de enero, 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 Auditoría de la Seguridad de los sistemas de información establece las condiciones para la realización de la preceptiva auditoría a la que deben someterse los sistemas de información del ámbito de aplicación del ENS, tal y como se regula en el artículo 34 y Anexo III de su norma reguladora.

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 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.

Esta Resolución se aprueba en aplicación de lo dispuesto en el Real Decreto 3/2010, de 8 de enero, en el artículo 29, apartado 2, en el capítulo V, Auditoría de la seguridad, artículo 34, así como en su Anexo III, modificado por Real Decreto 951/2015, de 23 octubre, a propuesta de la Comisión Sectorial de Administración Electrónica.

cve: BOE-A-2018-4573
Verificable en http://www.boe.es

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

Primero.

Aprobar la Instrucción Técnica de Seguridad «Auditoría de la Seguridad de los sistemas de información», cuyo texto se incluye a continuación.

Segundo.

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

La Instrucción Técnica de Seguridad de Auditoría de la 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, 27 de marzo de 2018.–La Secretaria de Estado de Función Pública, Elena Collado Martínez.

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE AUDITORÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

ÍNDICE

I. Objeto: La Instrucción Técnica de Seguridad de Auditoría de la Seguridad tiene por objeto establecer las condiciones para la realización de las auditorías, ordinarias o extraordinarias, previstas en el artículo 34 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.

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. Propósito de la Auditoría de la Seguridad, obligatoriedad y normativa reguladora:

III.1 La Auditoría de la Seguridad es un proceso sistemático, independiente y documentado, para la obtención de evidencias y su evaluación objetiva, con el fin de determinar el grado de conformidad con el ENS del sistema de información auditado. Debe permitir a sus responsables adoptar las medidas oportunas para subsanar las deficiencias y atender a las observaciones o recomendaciones que pudiera haber identificado el Equipo Auditor y, en su caso, posibilitar la obtención de la correspondiente Certificación de Conformidad, tal y como dispone la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, regulada por Resolución de 13 de octubre de 2016, del Secretario de Estado de Administraciones Públicas.

III.2 Para obtener la Certificación de Conformidad con el ENS, los sistemas de información de categorías MEDIA o ALTA precisarán superar una Auditoría de Seguridad, al menos cada dos años. Los sistemas de información de categoría BÁSICA solo requerirán

cve: BOE-A-2018-4573
Verificable en http://www.boe.es

de una autoevaluación que, de ser favorable, permitirá la exhibición de la Declaración de Conformidad, y cuyo resultado deberá estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior. Dicha autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.

III.3 Siendo obligatoria la Auditoría de Seguridad para los sistemas de categorías MEDIA o ALTA, nada impide que un sistema de categoría BÁSICA se someta asimismo a un proceso de Auditoría de Seguridad para la Certificación de la Conformidad, siendo siempre esta posibilidad la deseable.

III.4 El desarrollo de la Auditoría de la Seguridad se realizará con sujeción a la normativa contenida en la presente Instrucción Técnica de Seguridad y complementariamente, cuando corresponda, atendiendo a las normas nacionales e internacionales sobre auditoría de sistemas de información, entre ellas las guías CCN-STIC 802 Guía de auditoría, CCN-STIC 804 Guía de Implantación y CCN-STIC 808 Verificación del cumplimiento de las medidas en el ENS, y aquellas otras de ética y control de calidad interna de los auditores y entidades de auditoría, certificación y acreditación.

IV. Definición del alcance y objetivo de la Auditoría de la Seguridad:

IV.1 Los criterios metodológicos de auditoría utilizados, el alcance y objetivo de la Auditoría de la Seguridad deberán estar claramente definidos y documentados, conforme a lo dispuesto en el artículo 34 y en el Anexo III del ENS, debiendo aparecer en el Informe de Auditoría que se obtenga.

IV.2 Para asegurar la independencia objetiva de la Entidad Certificadora, las tareas de auditoría no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas actividades de consultoría o similares, tales como implantación o modificación de aplicaciones, relacionadas con el sistema auditado, redacción de documentos requeridos por el ENS o procedimientos de actuación, así como recomendaciones particulares sobre productos o soluciones concretas, entre otros.

V. Ejecución de la Auditoría de la Seguridad:

V.1 La entidad titular del sistema de información a auditar facilitará a la Entidad Certificadora cuanta información fuera pertinente para realizar los trabajos de auditoría, teniendo en cuenta su alcance y las eventuales limitaciones derivadas del ordenamiento jurídico.

V.2 El Equipo Auditor está obligado a requerir y obtener las evidencias pertinentes para verificar los criterios de auditoría, cuya evaluación constituirán los hallazgos en que se basarán las conclusiones recogidas en el Informe de Auditoría.

VI. El Informe de Auditoría:

VI.1 Atendiendo a la categoría del sistema auditado (BÁSICA, MEDIA o ALTA) el dictamen sobre la conformidad con el ENS se basará en el cumplimiento de los preceptos contenidos en el RD 3/2010, de 8 de enero, y de las medidas de seguridad del Anexo II del ENS que resulten de aplicación, así como de aquellos requisitos específicos que pudieran documentarse en guías CCN-STIC en función del contexto interno o externo del sistema de información, identificando, en su caso, las desviaciones que se observen, así como los registros, declaraciones de hechos o cualquier otra información pertinente y verificable en que se basen las conclusiones alcanzadas.

VI.2 Los hallazgos de no conformidad se clasificarán atendiendo a los siguientes grados:

– «No Conformidad Menor»: Se documentará una «No Conformidad Menor» ante la ausencia o el fallo en la implantación o mantenimiento de uno o más de los requisitos del ENS, incluyendo cualquier situación que pudiese, en base a una evidencia objetiva, sustentar una duda significativa sobre la conformidad del sistema de información con uno o más de tales requisitos.

cve: BOE-A-2018-4573
Verificable en http://www.boe.es

– «No Conformidad Mayor»: Se documentará una «No Conformidad Mayor» cuando se detecten «No Conformidades Menores» en relación con cualquiera de los preceptos contenidos en el RD 3/2010, de 8 de enero, o en el Marco organizativo, o en alguno de los subgrupos que integran el Marco operacional o las Medidas de protección (Planificación, Control de Accesos, Explotación, Servicios Externos, Continuidad del Servicio, Monitorización del Sistema, Protección de las Infraestructuras, Gestión del Personal, Protección de Equipos, Comunicaciones, Soportes de Información, Aplicaciones Informáticas, Información o Servicios) que, evaluadas en su conjunto, puedan implicar el incumplimiento del objetivo del Grupo o Subgrupo considerados.

Se documentará una Observación cuando se encuentren evidencias de una debilidad, una vulnerabilidad o una situación que, sin comprometer cualquier área del sistema de gestión definida en el ENS o por la organización, pueda, en la actualidad o en el futuro, derivar en un problema.

VI.3 El dictamen final de la Auditoría de la Seguridad será uno de los tres siguientes:

– «FAVORABLE»: Cuando no se evidencie ninguna «No Conformidad Mayor» o «No Conformidad Menor».

– «FAVORABLE CON NO CONFORMIDADES»: Cuando se evidencie cualquier no conformidad, mayor o menor. En este caso, la entidad titular responsable del sistema de información auditado deberá presentar, en el plazo máximo de un mes, un Plan de Acciones Correctivas sobre tales hallazgos de no conformidad a la entidad certificadora para su evaluación.

– «DESFAVORABLE»: Cuando, por el número o la transcendencia de las no conformidades detectadas, no sea posible decidir sobre su resolución a través de un Plan de Acciones Correctivas. En este caso se requerirá la realización de una auditoría extraordinaria que verifique la adopción de las medidas correctoras adecuadas.

La Guía CCN-STIC 824 Informe del Estado de Seguridad, que el Centro Criptológico Nacional mantendrá permanentemente actualizada, ofrecerá pautas de ayuda para el dictamen final de la Auditoría de la Seguridad.

VI.4 La Certificación de Conformidad con el ENS únicamente podrá expedirse si el dictamen fuera «FAVORABLE» o, si habiendo sido «FAVORABLE CON NO CONFORMIDADES», el Plan de Acciones Correctivas presentado por la entidad titular del sistema de información, trata y resuelve los hallazgos de no conformidad evidenciados, a criterio de la entidad certificadora.

VI.5 Ante un dictamen «DESFAVORABLE», la entidad titular del sistema de información auditado, en un plazo no superior a seis meses desde la fecha de emisión del Informe de Auditoría, deberá someterse a una Auditoría Extraordinaria, exclusivamente sobre los hallazgos de no conformidad evidenciados que, de resultar satisfactorio, permitirá la expedición del correspondiente Certificado de Conformidad con el ENS.

VI.6 En caso de un sistema certificado sobre el que se detecten No Conformidades Mayores, durante el período de resolución de las No Conformidades Mayores el Certificado de Conformidad quedará en suspenso. En caso de no cerrar las No Conformidades Mayores en un plazo de seis meses el Certificado de Conformidad quedaría revocado y la entidad auditada deberá eliminar el Distintivo de Conformidad de su sede hasta su próxima recertificación.

VI.7 El informe de Auditoría deberá contener la información adecuada y suficiente para facilitar y justificar la decisión de certificación, como mínimo:

– Las áreas organizativas, módulos o funciones del sistema de información cubiertas por la auditoría, incluyendo los requisitos de certificación y las ubicaciones que fueron auditadas, las pistas de auditoría seguidas y las metodologías de auditoría utilizadas.

– Los hallazgos identificados, tanto de conformidad como de no conformidad, incluyendo las Observaciones.

cve: BOE-A-2018-4573
Verificable en http://www.boe.es

– Los detalles de las no conformidades identificadas se justificarán mediante evidencias objetivas y su correspondencia con los requisitos del ENS u otros documentos requeridos para la Certificación.

– Comentarios sobre la conformidad del Sistema de Gestión de Seguridad de la Información del auditado con los requisitos de certificación, con una redacción clara de las no conformidades que hubieran podido evidenciarse, una referencia a la versión de la Declaración de Aplicabilidad, que incluya el nivel en cada dimensión para cada medida de seguridad del ENS aplicable, así como cualquier comparación útil con los resultados de Auditorías de la Seguridad previas.

– La Categoría del Sistema, con detalle del nivel de seguridad en cada una de las dimensiones recogidas en el ENS.

– El grado de confianza en las revisiones de la Dirección y auditorías internas del auditado.

– La conclusión o dictamen del Equipo de Auditoría sobre si el sistema de información del auditado debe ser certificado o no, con información que soporte esa conclusión.

VI.8 Los informes de auditoría podrán ser requeridos por el CCN-CERT, en los términos previstos en el artículo 37 del ENS.

VII. Entidades Auditoras del Sector Público: La presente Instrucción Técnica de Seguridad también será de aplicación a las actividades de auditoría y a la emisión de los correspondientes informes que se realicen por entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias se correspondan con el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.

VIII. Disposición adicional. Datos personales:

VIII.1 Cuando el sistema auditado tenga por objeto o incluya el tratamiento de datos personales se tendrá en cuenta lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

VIII.2 A partir del 25 de mayo de 2018, cuando el sistema auditado tenga por objeto o incluya el tratamiento de datos personales, se tendrá en cuenta el 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. A partir de dicha fecha en todo momento se informará al Delegado de Protección de Datos en calidad de responsable de la supervisión del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

cve: BOE-A-2018-4573
Verificable en http://www.boe.es