GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 802

ENS. Guía de auditoría

Abril 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.06.02 09:11:54 +02'00'

NIPO: 785- 17- 031-X

Fecha de Edición: abril de 2017

El Sr. Carlos Galán y José Antonio Mañas han participado en la redacción de este documento y sus anexos mientras que AENOR, AUDERTIS, BDO y NUNSYS han colaborado en su revisión.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

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 que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Abril de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. MARCO DE REFERENCIA

1. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular.
2. Esta guía de auditoría del Esquema Nacional de Seguridad se encuadra dentro de los requisitos del artículo 34 (Auditoría de la seguridad), y del Anexo III (Auditoría de la Seguridad) del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, y su modificación mediante el Real Decreto 951/2015, de 23 de octubre según lo previsto en el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y la Instrucción Técnica de Seguridad de Auditoría de Seguridad de los Sistemas de Información[1].
3. Esta guía será de uso para los sistemas de información comprendidos en los ámbitos subjetivo y objetivo de aplicación según dispone el artículo 3 del Real Decreto 3/2010 de 8 de enero, del ENS, 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
4. Esta guía tiene el objetivo de encauzar de una forma homogénea la realización de las auditorías, ordinarias o extraordinarias, estableciendo unas premisas mínimas en su ejecución, sin que por lo tanto, ello implique una limitación en la aplicación de metodologías o esquemas de trabajo propios del equipo de auditoría y la correspondiente emisión de una opinión objetiva e independiente en el informe de auditoría, siempre que se desarrolle dentro de los objetivos y alcances requeridos por el artículo 34.
5. Los sistemas de información de categoría Alta o Media, incluidos aquellos de empresas del sector privado que presten servicios a las entidades públicas, cuando tales servicios se encuentren comprendidos en el ámbito de aplicación el ENS serán objeto de una auditoría regular ordinaria, al menos cada 2 años, que verifique el cumplimiento de los requerimientos de dicho Esquema.
6. El RD 3/2010 establece una serie de requisitos mínimos de medidas de seguridad pero, es posible, que también sean aplicables otros requisitos legales[2] que el auditor debe tener en cuenta (en la medida que no impliquen un nivel inferior de seguridad requerido por el RD 3/2010), o bien que prescriben la realización de auditorías de las medidas de seguridad pero con objetivos o bien alcances diferentes.

[1] Por Resolución del Secretario de Estado de Función Pública (pendiente de publicación)
[2] Es el caso, por ejemplo, de que el sistema trate datos de carácter personal y haya que aplicar la normativa correspondiente

7. Estos requisitos de auditoría adicionales no están dentro del objeto y alcance de la auditoría requerida por el RD 3/2010. Sin embargo, en determinadas situaciones, la necesidad de una mayor eficiencia en la aplicación de los recursos (tanto del equipo auditor como del personal involucrado en el sistema de información auditado) puede aconsejar la realización conjunta de estas auditorías. Aún en estos casos se deben aplicar las premisas mínimas de esta guía para la realización de estas auditorías.

2. OBJETO DE LA AUDITORÍA

8. Dar cumplimiento a lo establecido en el RD 3/2010, específicamente en el artículo 34 y en el Anexo III, y verificar el cumplimiento de los requisitos establecidos en los capítulos II y III y en los Anexos I y II del ENS.
9. Emitir una opinión independiente y objetiva, basada en los principios de integridad, presentación imparcial, debido cuidado profesional, confidencialidad, independencia y enfoque basado en la evidencia, sobre este cumplimiento de tal forma que permita a los responsables correspondientes, tomar las medidas oportunas para subsanar las deficiencias identificadas, si las hubiera, y atender a las observaciones 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..
10. El objetivo final de la auditoría es sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado; tanto internamente como frente a terceros, que pudieran estar relacionados, es decir, calibrar la capacidad del sistema para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

3. DESARROLLO Y EJECUCIÓN DE LA AUDITORÍA

11. Como toda auditoría de sistemas de las tecnologías de la información, que incluye normalmente, los aspectos de seguridad de los sistemas, ésta debe realizarse de una forma metodológica que permita identificar claramente:

    - El Alcance y Objetivo de la Auditoría.
    - Los recursos necesarios y apropiados para realizar la auditoría (equipo auditor), según lo establecido en los Anexos A y B de esta guía.
    - Las debidas comunicaciones con los responsables de la organización que soliciten la auditoría.
    - La planificación preliminar o requisitos de información previos al desarrollo del plan de auditoría, y a la ejecución de las pruebas que se consideren necesarias.

- El establecimiento de un plan de auditoría detallado con las actividades, revisiones y pruebas de auditoría previstas.
- La presentación, de los resultados individuales de las pruebas, a las personas involucradas con estos resultados, para su confirmación sin valoraciones con respecto a los resultados finales.
- La evaluación global de los resultados de la auditoría en relación al objetivo y alcance definidos y a los requisitos del RD 3/2010.
- La confección, presentación y emisión formal del Informe de Auditoría.

12. La metodología aplicada debe permitir comprobar, a través de los registros y evidencias de auditoría, la consecución de estos pasos, las limitaciones que se hayan podido producir en el desarrollo de las tareas, y las actividades realizadas.

13. Para una consecución eficaz de la auditoría, el equipo auditor verificará que las medidas de seguridad para el sistema auditado se ajustan a los principios básicos del RD 3/2010 (artículo 4), y satisfacen los requisitos mínimos de seguridad (artículo 11).

3.1 DEFINICIÓN DEL ALCANCE Y OBJETO DE LA AUDITORÍA

14. El objetivo y alcance de la auditoría deben estar claramente definidos, documentados y consensuados entre el equipo auditor y la entidad del sector público o proveedor de servicios privado al que le aplique el ENS de acuerdo con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público según se indica en la Guía de Seguridad CCN-STIC-830 sobre el ámbito de aplicación del Esquema Nacional de Seguridad.

15. Las auditorías podrán ser requeridas por los responsables de cada organización con competencias sobre la seguridad del sistema de información objeto de éstas. Por lo tanto, es necesario establecer con claridad antes de concretar la realización de la auditoría, el objetivo y el alcance de la misma.

16. Se aplicará el procedimiento de determinación de la conformidad que, con carácter ordinario, verifique el cumplimiento de los requerimientos contemplados en el ENS, atendiendo a lo dispuesto sobre auditoría en el artículo 34 y en el Anexo III del Real Decreto 3/2010 y en la resolución del 13 de octubre de 2016 del Secretario de Estado de Administraciones Públicas “Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad”, con las aclaraciones de la guía “CCN-STIC-809 de declaración y certificación de conformidad con el ENS y distintivos de cumplimiento” y la Instrucción Técnica de Seguridad de Auditoría de Seguridad de los Sistemas de Información . .

    - Los sistemas de categoría Básica:
        - Requerirán de una autoevaluación para su declaración de la conformidad que deberá realizarse al menos cada dos años o cuando se produzcan modificaciones sustanciales en el sistema.

- La autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.
- Un sistema de categoría Básica se puede someter igualmente a una auditoría formal de certificación de la conformidad, siendo esta posibilidad siempre la deseable.

- Los sistemas de categoría Media o Alta:
  - Precisarán de una auditoría formal para su certificación de la conformidad al menos cada dos años, y con carácter extraordinario, siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria.
  - Deberá desarrollarse con las garantías metodológicas y de independencia, profesionalidad y adecuación requeridas.

17. Considerando que las redes de comunicaciones y sistemas de la administración pública, tienen interconexiones con entidades públicas y privadas, la descripción detallada del alcance de la auditoría es esencial, es decir, establecer claramente la extensión y el límite hasta dónde se audita.

18. Las medidas de seguridad a auditar pueden abarcar medidas de naturaleza diversa (organizativa, física y lógica, entre otras). Por lo tanto, como parte de la definición del alcance de la auditoría, es necesario antes de comenzarla, identificar los elementos que entran dentro de ésta.

19. Es imprescindible que se defina, preliminarmente, si existe alguna información que, por indicación del Responsable del Sistema, del Servicio o del de Seguridad, no estará accesible al equipo auditor y ni siquiera al Auditor Jefe también llamado Líder del equipo auditor, debiendo éste evaluar si ésta es una limitación para realizar la auditoría de acuerdo a lo previsto en el artículo 34. Si es así, y se decide continuar con el proceso de auditoría, esta limitación debe reflejarse en el Informe de Auditoría.

20. Para asegurar la independencia objetiva del equipo de la entidad de certificación, las tareas de auditoría no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas como responsabilidades 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.

3.2 EQUIPO AUDITOR

21. El equipo auditor, que puede pertenecer o no a la entidad de certificación, deberá estar compuesto por profesionales (Auditor Jefe , auditores, y expertos

técnicos) que garantice que se dispone de los conocimientos suficientes, de acuerdo al alcance establecido, para asegurar la adecuada y ajustada realización de la auditoría y que forme parte de una entidad de certificación del ENS acreditada según se indica en la 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" y en la guía "CCN-STIC-809 de declaración y certificación de conformidad con el ENS y distintivos de cumplimiento". En el Anexo A se establecen unos requisitos mínimos para los integrantes del equipo de auditoría.

22. Este equipo podrá estar compuesto por auditores internos y/ o externos o una combinación de ambos, pero en todo caso, es necesario cumplir con los siguientes requisitos:

- Si el equipo de auditoría es interno, éste deberá ser totalmente independiente de la organización, sistemas o servicios que sean o puedan ser objeto de la auditoría. Por lo tanto, el equipo de auditoría debiera pertenecer al grupo de Auditoría / Control Interno / Intervención, o a un grupo con responsabilidades similares constituido como tal, que asegure su independencia y objetividad.
- Si participan auditores internos y externos, se debe establecer qué equipo es responsable de la supervisión y realización de la auditoría, y de la emisión del informe, y consecuentemente, de los resultados de la auditoría. El plan de auditoría debe establecer con claridad la responsabilidad y asignación de funciones a cada integrante del equipo auditor.
- Sean auditores externos o internos, o un equipo mixto, la propiedad de los documentos de trabajo y de las evidencias, así como la responsabilidad por la emisión del informe y su contenido deben ser siempre inequívocas tanto en la apertura de la auditoría, como en su informe final.
- Si la realización de la auditoría ha sido encargada a un equipo externo (organización privada o pública), los integrantes deberán firmar las preceptivas cláusulas de confidencialidad, incluyendo las cláusulas aplicables de la legislación de tratamiento de datos de carácter personal. En el Anexo D de esta guía se incluye un modelo aplicable.
- Si la auditoría es liderada por un equipo de Auditoría Interna, pero con la incorporación de expertos técnicos independientes, estos también deben firmar una cláusula de confidencialidad.

23. El equipo auditor, en el diseño de sus pruebas y revisiones, no debe limitarse a la revisión de documentos, ya que el objetivo de la auditoría es obtener evidencias eficaces para evaluar y sustentar si, en la práctica, las medidas de seguridad auditadas son adecuadas para proteger la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información tratada, almacenada o transmitida por el sistema auditado.

24. Los componentes del equipo de auditoría deberán tener una formación suficiente en auditoría de sistemas de información, y en seguridad, según se establece en los requisitos mínimos reflejados en el Anexo A de esta guía. Si se considera necesario por la complejidad tecnológica o dimensiones del entorno a auditar, se podrán incorporar expertos en determinadas materias según se establece en el Anexo B.

25. El Auditor Jefe o líder del equipo auditor deberá asegurar que:

- Dispone de los conocimientos técnicos necesarios para abordar la auditoría de una forma eficiente.
- Se realizan las acciones necesarias, en la etapa preliminar, para garantizar que todos los integrantes del equipo entienden y conocen la estructura organizativa y técnica del sistema a auditar, los servicios que presta, y el objetivo y el alcance de la auditoría.
- Todos los auditores conocen el RD 3/2010 y, en la medida de las tareas asignadas, los requisitos de seguridad de otra legislación aplicable, y en particular, la relativa a tratamiento de datos de carácter personal.
- Se ha llevado a cabo el plan de auditoría previsto y aprobado, y que las desviaciones al programa, o sus modificaciones, están debidamente fundamentadas y registradas

3.3 PLANIFICACIÓN DE LA AUDITORÍA

26. Para la realización de la auditoría es necesario realizar una planificación preliminar que, fundamentalmente, consiste en establecer los requisitos de información y documentación necesarios e imprescindibles para:

- Establecer y desarrollar el plan de auditoría.
- Concretar los conocimientos necesarios del equipo de auditoría.
- Definir la agenda de revisiones, reuniones y entrevistas.
- Definir las revisiones y pruebas a realizar.
- Adjudicar las tareas a los componentes del equipo auditor y expertos.
- Los criterios de auditoría y cualquier documento de referencia.

27. La documentación mínima a requerir para concretar la planificación en detalle de la auditoría del cumplimiento del RD 3/2010 es:

- Documentos firmados por el órgano superior correspondiente que muestren el conocimiento y la aprobación formal de las decisiones en materia de política de seguridad.
- Organigrama de los servicios o áreas afectadas, con descripción de funciones y responsabilidades.
- Identificación de los responsables: de la información, de los servicios, de la seguridad y del sistema.
- Descripción detallada del sistema de información a auditar (software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares).

- Categoría del sistema según el Anexo I del ENS, incluyendo los criterios de identificación y valor de los niveles de las dimensiones de seguridad que serán de aplicación al sistema.
- La Política de Seguridad.
- La Política de Firma Electrónica y Certificados (si se emplean estas tecnologías).
- La Normativa de Seguridad.
- Descripción detallada del sistema de gestión de la seguridad y la documentación que lo sustancia.
- Informes con el desarrollo y resultado de la apreciación del riesgo, incluyendo la identificación de escenarios de riesgo, su análisis y evaluación.
- La Declaración de Aplicabilidad.
- Decisiones adoptadas para tratar los riesgos.
- Relación de las medidas de seguridad implantadas por requisitos legales o como resultado de la apreciación del riesgo.
- Relación de registros de actividad en lo relativo a las medidas de seguridad implantadas y estado de implantación.
- Informes de otras auditorías previas de seguridad relacionados con los sistemas y servicios incluidos en el alcance de la auditoría, como podría ser el informe de la auditoría bienal de protección de datos de carácter personal, o de auditorías previas con el mismo objetivo y alcance que la auditoría a comenzar.
- Informes de seguimiento de deficiencias detectadas en auditorías previas de seguridad, y relacionadas con el sistema a auditar.
- Lista de proveedores externos cuyos servicios se ven afectados o entran dentro del alcance de la auditoría, y evidencias del control realizado sobre estos servicios.
- Sistemas de métricas con referencia a las guías CCN-STIC-815 “Sistema de Métricas e Indicadores”, CCN-STIC -824 “Informe Nacional del Estado de la Seguridad, teniendo en consideración lo indicado en la 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”.

28. Con el propósito de agilizar y acortar en lo posible los tiempos de auditoría presencial en la entidad auditada, es recomendable que ésta haga llegar al Auditor Jefe la documentación requerida en el apartado anterior con la antelación suficiente.

29. Según la disponibilidad de esta documentación, y de acuerdo con los Responsables de la Información, del Servicio, del Sistema y del Responsable de la Seguridad, el Auditor Jefe determinará si es necesario recibir una copia, o bien, según el caso, es suficiente con una presentación de esta documentación, por parte de estos responsables.

30. No obstante, es aconsejable para una planificación ajustada de las pruebas en detalle, que se pueda disponer de copias (en soporte papel o electrónico) de alguna de ellas como evidencia, o para facilitar la planificación de las pruebas y asignación de tareas a los integrantes del equipo auditor. En todos los casos el equipo auditor mantendrá una lista actualizada de la documentación solicitada y su situación en cuanto a si fue recibida una copia, o se permitió el acceso para su revisión.

31. Cada entorno a auditar será diferente y con sus propias configuraciones y estructura organizativa, por lo tanto, es necesario tenerlas en cuenta a la hora de:

    a) diseñar las revisiones y pruebas de auditoría,
    b) definir en qué consistirá cada una de ellas,
    c) y establecer los recursos necesarios (del equipo de auditoría y de los servicios auditados).

32. Para la planificación de la auditoría se tendrán en cuenta las siguientes premisas:

- Los criterios organizativos del órgano responsable del sistema auditado y la descripción de las funciones del personal afectados por este sistema.
- Los criterios que pueden auditarse mediante la revisión de documentación, observación, entrevistas, cuestionarios o muestreo.
- La selección de medidas de seguridad a verificar en cuanto a su cumplimiento tal y como han sido aprobadas.
- Las revisiones que deberían realizarse mediante la ejecución de pruebas técnicas (accesos, visualización de registros, edición de parámetros de seguridad, observación y fotografía, si es aplicable, de las medidas de seguridad física, etc.), estableciendo muestras de elementos a revisar. El objetivo, en este caso, es comprobar el cumplimiento y la observancia de determinadas normas de seguridad.
- Las pruebas podrán realizarse en base a muestras, pero el equipo auditor debe sustentar que la muestra de elementos seleccionada para una prueba determinada, es suficientemente representativa, para garantizar la solvencia de los resultados.
- Las evidencias que se espera obtener en cada prueba y cuáles son ineludibles para documentar la realización de la prueba, documentando aquellas que por restricciones de propiedad industrial o seguridad no sea factible su obtención, aunque sí su verificación por el auditor.
- Asignación de tareas a cada integrante del equipo de auditoría según su cualificación y experiencia, y asignación de tareas a los expertos. Deberá dejarse constancia de la supervisión de su trabajo.
- Si existen informes recientes de auditoría previas (internas o externas) que hayan incluido la revisión de elementos afectados por la presente

auditoría, estos podrán considerarse en la planificación y no repetir pruebas, siempre y cuando:

- De acuerdo a la información inicial recibida, no se hayan modificado las medidas de seguridad, y se pueda tener acceso a las evidencias de las pruebas realizadas en su momento. Si las medidas se han modificado, por cualquier circunstancia, ya sea por razones de mejora continua, o para solventar deficiencias identificadas en la auditoría anterior, la medida de seguridad se volverá a revisar.
- Estas auditorías previas hayan tenido el grado de independencia objetiva y cualificación, similar al requerido para la realización de la auditoría del RD 3/2010.

3.4 EVIDENCIAS DE LA AUDITORÍA

33. Las evidencias de auditoría pueden obtenerse a través de la inclusión de los siguientes métodos y procedimientos en el Plan de la auditoría, teniendo como referencia asimismo el RD 3/2010 y especialmente sus Anexos I y II:

- Gestión del Riesgo.

Tipos de pruebas: sustentación metodológica de la identificación de escenarios de riesgo, su análisis y evaluación, su coherencia y documentación, y verificación del inventario de activos. Para ello el equipo auditor puede basarse en la metodología MAGERIT[3] , la herramienta PILAR[4] del CCN, en la norma UNE 71504 - Metodología de análisis y gestión de riesgos de los sistemas de información o en otras metodologías de apreciación del riesgo reconocidas internacionalmente. En este apartado no es de aplicación la selección de muestras.

- El marco organizativo y la segregación de funciones.

Tipos de pruebas: documentación de las políticas y procedimientos (accesibilidad por el personal al que afecta y actualización); la comunicación de las normas, de las responsabilidades y de la concienciación del personal afectado sobre estas normas, políticas y procedimientos. Se recomienda que, a los efectos de una evaluación más representativa, se entreviste no solo a cargos jerárquicos, sino también a otro personal de forma aleatoria.

- El marco operacional (Planificación, Control de Accesos, Explotación, Servicios Externos, Continuidad del Servicio, y Monitorización del Sistema).

Tipos de pruebas: evaluación, entre otros, de las pruebas fehacientes de la continuidad del servicio, con inclusión o no de los servicios externos; las autorizaciones y solicitudes de acceso, el registro y seguimiento de los incidentes de seguridad; la adecuación de los derechos de acceso que consideren la segregación de funciones, evaluación del control de capacidad de los sistemas, los

[3] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
[4] Procedimiento Informático y Lógico de Análisis de Riesgos guías serie CCN-STIC-470 y siguientes

mecanismos de control para el acceso físico, la revisión de los registros de actividad, su revisión y supervisión; la fortaleza de las medidas de seguridad de las comunicaciones frente a ataques internos o externos; el control de cambios en aplicaciones y sistemas; el cumplimiento de contratos de propiedad intelectual, etc.

- Las medidas de protección (Protección de las instalaciones e infraestructuras, Gestión del personal, Protección de equipos, de las comunicaciones, de los soportes de información, de las aplicaciones informáticas, de la información, y de los servicios).

Tipos de pruebas: evaluación, entre otros, de las pruebas fehacientes de la protección de los elementos referenciados. La guía CCN-STIC-808 Verificación del cumplimiento del ENS describe las pruebas a realizar en el conjunto de las medidas de seguridad.

- La Declaración de Aplicabilidad que recoge las medidas de seguridad del Anexo II que son relevantes para el sistema de información sujeto a la auditoría.

Tipos de pruebas: evidencia documental de la Declaración de Aplicabilidad incluyendo todas las medidas de seguridad que son de aplicación globalmente o por sistema. En caso de utilizar medidas compensatorias se considerará lo indicado en el Artículo 27 – apartado 5 del ENS, donde la Declaración de Aplicabilidad indicará de forma detallada y documentada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de seguridad

- Los procesos de mejora continua de la seguridad.

Tipos de pruebas: evaluar el ciclo de madurez del sistema de gestión de la seguridad del sistema de información auditado, criterios para la revisión, no conformidades detectadas, derivadas o no de acciones, acciones correctivas y preventivas, y agenda de mejoras. Evolución de las métricas propuestas como clave para la supervisión del proceso de mejora continua.

- La aplicación de los modelos de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos correspondientes (según una muestra seleccionada de estos).

34. Para definir los métodos y procedimientos de auditoría (verificación de las medidas de seguridad), el equipo auditor puede utilizar guías y cuestionarios de auditoría disponibles en asociaciones y colectivos de auditores, y las guías STIC proporcionadas por el CCN que sean de aplicación al sistema auditado. Estas guías pueden ser una buena base para, dentro del alcance de la auditoría, diseñar pruebas adecuadas, manteniendo siempre un criterio analítico y de proporcionalidad. En el Anexo F se incluyen referencias de estas guías.

35. El Auditor Jefe debe valorar qué información o documentación complementaria es necesario solicitar al comienzo de la auditoría, para asegurar que se tiene un conocimiento fiel del estado de la seguridad al comienzo de la misma, como pueden ser, entre otros posibles y según se considere aplicable:

- Lista del personal que ha dejado la entidad recientemente.
- Copia del registro de incidencias.
- Copia del registro de actividad de los usuarios.
- Registros de formación del personal afectado por el sistema auditado.

36. Este tipo de evidencias pueden asistir al auditor en la evaluación de si determinadas medidas de seguridad se han realizado consistente y homogéneamente.

37. Durante la definición de las pruebas a realizar, se valorará si es necesario solicitar cuentas de acceso al sistema auditado para algunos integrantes del equipo auditor, aunque deberá minimizarse la necesidad de intervención directa por parte del equipo auditor en los sistemas del cliente, pudiendo en su caso requerir que la verificación técnica sea realizada por personal especializado de la organización auditada bajo supervisión del equipo auditor.

38. Para la realización de las pruebas de auditoría, el auditor tendrá en cuenta como normas generales, las siguientes premisas:

    - La planificación de las pruebas a realizar, especialmente las de observación y pruebas técnicas, es un elemento privativo del equipo auditor. Por lo tanto, éste no tiene obligación de anticiparlas al personal auditado, excepto en lo que concierne a la agenda o disponibilidad de elementos para la ejecución de la prueba.
    - En la realización de determinadas pruebas como la verificación documental de autorizaciones, aprobaciones o contratos, el auditor podrá requerir la revisión de los documentos. Estos documentos, bien en soporte electrónico o en papel, podrán ser originales o constituir alguno de los tipos de copia previstos en las Normas Técnicas de Interoperabilidad, en relación a la evidencia a la que deban servir a efectos de verificación (por ejemplo, en el caso en que, determinado documento, pueda servir como evidencia de una conclusión a incorporar en el informe de auditoría).
    - La muestra seleccionada de medidas o documentación debe ser suficiente y relevante para satisfacerse del cumplimiento objetivo de la prueba, dentro del alcance y objetivo de la auditoría. El Jefe del equipo de auditoría puede decidir que se amplíe la muestra si considera que el tamaño de ésta no es suficiente.
    - El equipo auditor al evaluar no prejuzgará las medidas existentes y deberá siempre considerar, objetivamente, si se ajustan a lo previsto en el 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 y si son efectivas para tratar realmente los riesgos identificados en el Análisis de Riesgos.
    - Ante la ausencia de determinada medida, se investigará y analizará si existen otras medidas compensatorias, y en su caso, se evaluará la

eficacia de estas últimas. Cuando se haya evaluado la implantación y efectividad de una medida de seguridad sin detectar no conformidades, se proseguirá con el plan de auditoría, asumiendo, por tanto, su conformidad.

- Las entrevistas no se plantearán de forma inductiva (conducir a una contestación concreta), sino abiertas (cómo se realiza determinada actividad o se concreta en la práctica determinada medida de seguridad). Es decir: no se deben realizar preguntas donde la respuesta, afirmativa o negativa según el caso, esté implícita en la pregunta, salvo para confirmar los hallazgos de conformidad o de no conformidad con los criterios de auditoría obtenidos a partir de las evidencias.
- Se ponderarán las respuestas de las entrevistas, pudiendo dar lugar a la realización de pruebas complementarias que no estaban previstas.

39. Para las evidencias el auditor tendrá en cuenta como normas generales, las siguientes:

- La evidencia recogida debe ser suficiente y relevante para que:
    - si no hay incidencias a comunicar, se acredite la realización adecuada de la prueba y sus resultados.
    - si hay hallazgos de no conformidad a incluir en el informe, se evidencie claramente el incumplimiento persistente o una indiscutible deficiencia de seguridad, y no aquellas situaciones excepcionales o puntuales, si están reportadas, controladas, y aprobadas, a menos que la excepcionalidad no debiera haber sido aprobada, por el riesgo que pudiera implicar, según el juicio objetivo y sustentado del auditor.
- La verificación de la documentación deberá fundamentarse en las conclusiones de la revisión, y las posibles aclaraciones recibidas posteriormente.
- Las conclusiones o información recogida en una entrevista, para poder ser consideradas como evidencias de auditoría, deberán corresponder a una declaración de hechos, de personal que intervenga directamente en el procedimiento.
- Los correos electrónicos, en la medida que involucre a varias personas dentro del alcance de la auditoría, pueden servir, en determinados casos, también como prueba de auditoría.
- Las pruebas de observación (por ejemplo, seguridad física) deberán estar documentadas detallando la fecha y lugar o activo observado.
- Las evidencias que se recojan deben evitar, en lo posible, contener datos de carácter personal, o si es necesario como evidencia, que los contengan, debe utilizarse algún mecanismo (supresión, tachado, etc.) que impida su divulgación.

- Las evidencias que haya que presentar a requerimiento de quien tenga competencias para solicitarlas, deberán acogerse a la práctica habitual y en particular, si se trata de evidencias electrónicas, deberán someterse a las Normas Técnicas de Interoperabilidad que resulten de aplicación.
- Los documentos de trabajo del auditor (planificación, documentación revisada, evidencias, actas de reuniones, listados, copias de pantallas, y evidencias similares del trabajo realizado, ya sean en soporte papel o electrónico) deberán mantenerse como mínimo durante los dos siguientes años, debidamente referenciados y archivados, así como custodiados y protegidos.
- Cuando el auditor, en el curso de sus observaciones, descubre una irregularidad significativa de fácil resolución, puede informar inmediatamente al Responsable de la Seguridad para que tome las medidas correctivas oportunas sin esperar al informe final de auditoría.

3.5 ELABORACIÓN Y PRESENTACIÓN DE LOS HALLAZGOS DE LA AUDITORÍA

40. El objetivo principal de la presentación de los resultados de las revisiones y pruebas, antes de la emisión del informe de auditoría, es confirmar los hechos y las situaciones detectadas o identificadas como resultado de las pruebas y revisiones realizadas. Esta presentación tendrá un carácter objetivo, sin valoraciones subjetivas, ni aludiendo a la valoración de los resultados finales a plasmar en el informe, que es la opinión profesional del auditor.

41. Esta presentación es fundamental para la eficacia del informe de auditoría posterior, al confirmar que los resultados, de las revisiones y las pruebas, son ciertos, y que no existe otra información, que por no haber sido considerada o no estar disponible en su momento, podría cambiar la evaluación del cumplimiento de determinado requisito de seguridad.

42. Todos los resultados de pruebas, relacionados entre sí o que se refieran a una misma no conformidad, serán agrupados en el informe, aun cuando se incluya un detalle de las deficiencias de forma individual, en un anexo al Informe de Auditoría.

3.6 PRESENTACIÓN DEL INFORME DE AUDITORÍA

43. Una vez confirmados los hechos y deficiencias resultantes de las revisiones y pruebas de auditoría, se recogerán en un informe que deberá presentarse al Responsable del Sistema y al Responsable de la Seguridad. Según el RD 3/2010 los informes de auditoría serán analizados por el Responsable de Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las acciones correctivas adecuadas.

44. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas exigidas por el RD 3/2010. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados.

45. Atendiendo a la categoría del sistema auditado (BÁSICA, MEDIA o ALTA) el informe de auditoría se basará en el cumplimiento alcanzado de lo prescrito en el ENS y en concreto en las medidas de seguridad del Anexo II 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, los hallazgos de conformidad, no conformidad y observaciones que se detecten, así como los registros, declaraciones de hechos o cualquier otra información pertinente y verificable en que se basen las conclusiones alcanzadas.

46. 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.
    - "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.

47. 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.

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

    - Existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.
    - La Política de Seguridad responde a la misión y objetivos de seguridad de la organización.
    - La organización define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de

información, detallando procedimientos para la resolución de conflictos entre dichos responsables cuando pueda darse dicho supuesto, y verificando que se han designado personas para dichos roles a la luz del principio de "separación de funciones".

- Se ha realizado una apreciación del riesgo, incluyendo la identificación de escenarios de riesgo, el análisis de las consecuencias y su probabilidad, y la evaluación de su aceptabilidad o inaceptabilidad para la organización, con revisión y aprobación regular, según lo establecido en las medidas aplicables del Anexo II del RD 3/2010.
- La Categoría del Sistema, con detalle del nivel de seguridad en cada una de las dimensiones recogidas en el ENS.
- Se cumplen las medidas de seguridad descritas en el Anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
- 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.
- Existe un proceso de mejora continua de la gestión de la seguridad.
- 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 detalles de las conformidades y no conformidades identificadas se justificarán mediante evidencias objetivas y su correspondencia con los requisitos del ENS u otros documentos requeridos para la Certificación.
- El dictamen del Equipo de Auditoría sobre si el sistema de información del auditado debe ser certificado o no, con información que soporte esa conclusión.

49. El informe de auditoría podrá ser requerido por el CCN-CERT, en los términos previstos en el artículo 37 del ENS.

50. El equipo auditor no entregará ni concederá acceso al informe de auditoría a terceros distintos de los indicados en el párrafo anterior, salvo por imperativo legal o mandato judicial.

51. El Informe de Auditoría se puede presentar en formato papel o electrónico y estar debidamente firmado El esquema del informe incluirá como mínimo:

    - Fecha de emisión del informe.
    - Una sección de alcance, detallando su extensión y limitaciones, e incluyendo el objetivo de la auditoría, con la debida identificación del sistema o sistemas auditados.
    - Breve descripción del proceso metodológico aplicado para realizar la auditoría.
    - Identificación de la documentación revisada.

- Indicación de si ha habido alguna limitación en la realización de la auditoría, que impidan al equipo auditor formarse una opinión sobre determinados criterios de la auditoría, incluidas medidas de seguridad.
- Una sección de informe ejecutivo resumiendo los puntos fuertes, las debilidades (resumen de las no conformidades y observaciones) y oportunidades de mejora, e incluyendo un resumen general del grado de cumplimiento.
- Las recomendaciones en ningún caso deberán ser cerradas, sino sugerencias generales de las distintas alternativas posibles, cuando sea aplicable, a considerar por los responsables de la seguridad.
- Las recomendaciones estarán siempre basadas en la existencia de un riesgo y sustentadas debidamente, o bien relacionadas con un incumplimiento fehaciente y preciso de los requisitos básicos y mínimos del RD 3/2010
- En anexos se podrá describir los detalles y resultados de las pruebas que permiten llegar a las conclusiones del informe ejecutivo, agrupándolos por los apartados del informe ejecutivo.
- El informe también podrá incluir como anexo las contestaciones del Responsable de la Seguridad a los comentarios vertidos en el informe, o las acciones que se tomarán para solucionar las deficiencias, si las hubiera.
- El Informe de Auditoría deberá ser firmado por el Auditor Jefe, e indicar los participantes en el equipo de auditoría en un anexo o a continuación de su firma.

52. En el informe ejecutivo no se incluirán términos o acrónimos técnicos, ya que el informe podrá ser leído por directores y gerentes, o terceros, que no tengan el conocimiento específico adecuado. Tampoco se deberán incluir nombres de personas concretas, solo funciones o puestos desempeñados.

3.7 DICTAMEN FINAL DEL INFORME DE AUDITORIA

53. El dictamen final del informe de Auditoría 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 evidencien "No Conformidades Menores". y/o "No Conformidades Mayores". 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 (PAC) sobre tales desviaciones a la entidad certificadora para su evaluación.
- "DESFAVORABLE": Cuando exista un número significativo de No Conformidades Mayores cuya solución no pueda evidenciarse a través de un Plan de Acciones Correctivas y requiere la comprobación in-situ de su correcta implantación a través de una auditoría extraordinaria.

54. 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 del informe de la Auditoría.

55. 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 las desviaciones evidenciadas, a criterio de la entidad certificadora.

56. 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 las desviaciones evidenciadas que, de resultar satisfactorio, permitirá la expedición del correspondiente Certificado de Conformidad con el ENS.

57. 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.

58. En el supuesto de que las conclusiones de la auditoría incluyan no conformidades, la organización auditada deberá remitir al equipo de auditoría para su aprobación un plan detallando las acciones correctivas que se implementarán para atacar la causa raíz de las no conformidades y evitar futuras ocurrencias. En el caso de auditorías de certificación, no podrá emitirse el Certificado de Conformidad hasta la recepción de los Planes de Acciones Correctivas de todas las No Conformidades detalladas en el informe y, opcionalmente, para las observaciones.

ANEXO A. REQUISITOS PARA EL EQUIPO AUDITOR

1. El equipo auditor deberá estar dirigido y tutelado siempre por un Auditor Jefe también llamado Líder del equipo auditor, cuyas funciones principales son la supervisión de todo el proceso de auditoría, y la exactitud de los hallazgos y recomendaciones mencionados en el informe, así como preservar las evidencias de la auditoría.
2. El Auditor Jefe, responsable de gestionar las actividades de auditoría, deberá probar como mínimo:
    - Acreditación de formación y experiencia en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional, o bien a través de experiencia verificable y evidenciada de al menos 4 años, en auditoría de tecnologías de la información.
    - Conocimientos de seguridad y gestión de riesgos de seguridad (certificación y experiencia probada de al menos 4 años en estos elementos).
    - Conocimiento de los requisitos del RD 3/2010.
    - Conocimientos de otra legislación aplicable cuando la auditoría incluya además otros requisitos o esquemas de seguridad, como puede ser la relativa a la protección de datos de carácter personal o el Esquema Nacional de Interoperabilidad, entre otros.
3. El resto del equipo puede no cumplir con los requisitos para el Auditor Jefe, no obstante, debe tener alguna preparación previa tanto en seguridad como en auditoría de los sistemas de información, dependiendo de, y en consonancia, con las responsabilidades asignadas. La responsabilidad por la asignación de tareas al resto del equipo, incluyendo a los expertos, corresponde a la organización (privada o pública) que aporte el equipo de auditoría.
4. En ningún caso los integrantes del equipo auditor, deben haber participado o detentado responsabilidades previas a la auditoría, al menos en los dos últimos años, en el sistema de información auditado, o bien haber sido consultores, para ese sistema, en el proceso de implantación de los requisitos del RD 3/2010.
5. Todos los integrantes del equipo auditor, especialmente los externos y los expertos técnicos, deberán haber firmado antes de comenzar la auditoría, un acuerdo de confidencialidad. En anexo D se propone un modelo.

ANEXO B. INCORPORACIÓN DE EXPERTOS TÉCNICOS AL EQUIPO DE AUDITORÍA

1. En el desarrollo de las actividades de auditoría, el equipo auditor tendrá que revisar temas tecnológicos diversos, como los relacionados con las transmisiones electrónicas, sistemas abiertos o propietarios, mecanismos de cifrado, firma electrónica, gestión de documentos electrónicos, planes de continuidad, seguridad de las comunicaciones, u otros de naturaleza análoga. Por esta razón, una vez analizada la complejidad tecnológica, es posible que el Auditor Jefe considere necesaria la incorporación de expertos técnicos en determinadas materias.

2. Entre estos expertos técnicos también es posible que sea necesario incluir profesionales con perfiles especializados tales como:

   - expertos con conocimientos jurídicos,
   - expertos en Procedimiento Administrativo,
   - expertos en Archivística, gestión documental y conservación a largo plazo,
   - expertos con conocimientos relativos a la gestión de documentos y archivos electrónicos,
   - y otros que se estimen pertinentes en función del sistema auditado.

3. Las necesidades de conocimiento de estos expertos dentro del equipo auditor, las establecerá el Auditor Jefe, en el momento de definir los recursos necesarios para la realización de la auditoría.

4. Estos expertos estarán sujetos a las mismas reglas de la auditoría que el resto del equipo auditor (planificación, evidencias de auditoría, supervisión por el Jefe del equipo de auditoría, y cláusulas de confidencialidad), pero no es necesario que detente las mismas cualificaciones requeridas para un auditor según el Anexo A.

5. En ningún caso estos expertos, deben haber participado o desempeñado responsabilidades previas a la auditoría, al menos en los dos últimos años, en el sistema de información auditado, o bien haber sido consultores, para ese sistema, en el proceso de implantación de los requisitos del RD 3/2010.

ANEXO C. CONCURRENCIA CON EL TÍTULO VIII DEL RD 1720/2007 O CON EL REGLAMENTO (UE) 2016/679 [5]

1. El alcance establecido para la auditoría en el artículo 34 del RD 3/2010, no tiene como objeto auditar o verificar el cumplimiento de las medidas de seguridad establecidas para el tratamiento de datos de carácter personal.

2. Cuando el sistema auditado tenga por objeto 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. A partir del 25 de mayo de 2018, cuando el sistema auditado tenga por objeto el tratamiento de datos personales, se tendrá en cuanta 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.

3. Si durante la realización de la auditoría a la que es aplicable esta guía, se identificase algún incumplimiento manifiesto de dicha legislación de protección o tratamiento de datos, es obligación del equipo auditor comunicarlo, e incluirlo en el informe de auditoría.

4. Asimismo, es posible que se establezca previamente la realización conjunta de ambas auditorías. En esta circunstancia, que ambas auditorías coincidan en el tiempo, y realizadas por el mismo equipo de auditoría, es necesario tener en cuenta, los aspectos comunes y diferenciados.

5. Se podrá emitir dos informes diferenciados, cada uno con su objetivo y alcance, o bien indicar en un mismo informe agrupado qué deficiencias afectan al cumplimiento de una u otra norma.

6. Consecuentemente, dado que estas las normas pueden ser concurrentes en una gran mayoría de las medidas de seguridad, pero diferentes en otras, el equipo auditor debe, si se realizan auditorías conjuntas, considerar y diferenciar en su planificación de la evaluación de las medidas de seguridad aplicables según la tipología de datos tratados y la finalidad de su tratamiento, por el sistema de información auditado, y determinar cuándo una revisión o prueba es válida para ambas auditorías.

[5] 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)

ANEXO D. MODELO DE ACUERDO DE CONFIDENCIALIDAD

Los contenidos de los modelos de confidencialidad que se incluyen en este Anexo, tendrán la consideración de requisitos mínimos. Las responsabilidades por su aplicación, en relación a sus respectivos equipos involucrados, en cualquier medida, en la auditoría, corresponden tanto a la organización responsable del equipo de auditoría, como a la del sistema de información auditado.

Datos de carácter personal

Las tareas de auditoría a realizar no conllevan, necesariamente en sí mismas, el tratamiento posterior ni simultáneo de datos de carácter personal. Pero, por la naturaleza de los servicios, es posible que se acceda a datos de carácter personal (por ejemplo, en alguna documentación revisada).

Por lo tanto, dado que en alguna circunstancia, se podría acceder a este tipo de datos, el equipo de auditoría XXXX se compromete, en cumplimiento de la legislación vigente en cuanto a tratamiento de datos de carácter personal, a tratar estos datos conforme a las instrucciones del responsable de los datos de carácter personal, a los que pudiera acceder, que no los aplicará o utilizará con fin distinto al que figure en este acuerdo y contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

XXXX declara conocer la legislación vigente en materia de protección de datos, y el equipo de auditoría está instruido en estos requisitos. Por lo tanto, en caso de tener lugar este acceso, como consecuencia de los servicios a prestar, se compromete a observar los requisitos establecidos en esta legislación.

De igual forma el organismo XXXX al cual pertenece el sistema auditado se compromete a no difundir ni utilizar para otros fines que los de la realización de la auditoría, cualquier dato de carácter personal del equipo de auditoría.

Información del sistema de información auditado

XXX se compromete a no difundir información alguna (procesos, sistemas, medidas de seguridad, y cualquier otra información relacionada o no con el sistema de información auditado, incluyendo el informe de auditoría) que se pueda conocer o a la que se tenga acceso durante la realización de la auditoría. En este sentido están instruidos todos los integrantes del equipo de auditoría, que han firmado sus respectivos acuerdos de confidencialidad.

Una copia de los documentos de trabajo que se elaboren para la realización de la presente auditoría será custodiada por XXXX, como evidencia del trabajo realizado.

Firmantes del acuerdo de confidencialidad

Los firmantes del acuerdo de confidencialidad serán todos y cada uno de los miembros del equipo auditor, incluyendo a expertos, con independencia del momento en el que se incorporen al mismo.

ANEXO E. GLOSARIO

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.

Las auditorías internas, denominadas en algunos casos auditorías de primera parte, se realizan por la propia organización, o en su nombre, para la revisión por dirección y para otros propósitos internos (por ejemplo, para confirmar la eficacia del sistema de gestión o para obtener información para la mejora del sistema de gestión). Las auditorías internas pueden formar la base para una autodeclaración de conformidad de una organización.

Las auditorías externas incluyen auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen interés en la organización. Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras independientes, tales como autoridades reglamentarias o aquellas que proporcionan la certificación.

Cuando dos o más sistemas de gestión de disciplinas diferentes se auditan juntos, se denomina auditoría combinada.

(Adaptado de la UNE-EN-ISO 19011:2012, definición 3.1).

Auditoría de sistemas de información

1) La Auditoría de sistemas de información es el proceso metodológico, realizado con independencia de los elementos auditados y con objetividad, de recoger, agrupar y evaluar evidencias para determinar si los sistemas o tecnologías de la información salvaguardan los activos, mantienen la integridad de los datos, contribuyen al logro de los fines de la organización y utilizan eficientemente los recursos.

2) La actividad de auditoría debe evaluar las exposiciones al riesgo referidas al gobierno, operaciones y sistema de información de la organización, con relación a la fiabilidad e integridad de la información, la eficacia y eficiencia de las operaciones, la protección de activos, y el cumplimiento de leyes, regulaciones y contratos.

Alcance de la auditoría

Extensión y límites de una auditoría. El alcance de una auditoría incluye generalmente una descripción de las ubicaciones, las unidades de la organización, las actividades y los procesos, así como el periodo de tiempo cubierto (adaptado de la UNE-EN-ISO 19011:2012, definición 3.14).

Elementos a los que comprende la auditoría del Esquema Nacional de Seguridad: los sistemas que estarán en revisión, el organismo responsable de estos sistemas, los elementos de la estructura tecnológica, personal vinculado a

los elementos anteriores, periodos de tiempo. Dentro del contexto de esta guía tiene una relación directa con la Declaración de Aplicabilidad.

Auditor

Persona que lleva a cabo una auditoría (adaptado de la UNE-EN-ISO 19011:2012, definición 3.8).

El profesional con formación y experiencia contrastable sobre las materias a auditar, que reúne las condiciones, además de las de conocimientos y competencia, de actuar de forma independiente. Realiza las tareas de auditoría.

Auditor interno

Pertenece a una unidad independiente dentro del organismo al que pertenecen los elementos objeto de la auditoría, con funciones y autoridad claramente definidas, que no tiene responsabilidades operativas, directivas o de gestión de los procesos, sistemas o áreas auditados. Para favorecer su independencia esta unidad debe reportar al nivel jerárquico más alto dentro del organismo.

Auditor externo

Es independiente laboralmente al organismo donde realizará la auditoría. Para mantener su independencia, a título individual o como entidad, no debe haber realizado funciones (asesoría, consultoría), para los sistemas o procesos dentro del alcance de la auditoría a realizar.

Comprobación

1) (DRAE) Verificar, confirmar la veracidad o exactitud de algo.

2) Dentro del contexto de esta guía, son verificaciones de la realización de controles, del establecimiento de medidas de seguridad, y de documentación de políticas, entre otros, dentro de los requerimientos establecidos por la norma de referencia en la auditoría.

Conformidad

Cumplimiento de un requisito (UNE-EN-ISO 19011:2012).

Control / Controles

1) (DRAE) Regulación, manual o automática, sobre un sistema.

2) Mecanismo o procedimiento que evita, previene, o detecta un riesgo.

3) En el contexto de una auditoría, estos pueden ser clasificados en preventivos, detectivos, y correctivos.

Criterio de auditoría

Conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cuál se compara la evidencia de auditoría (UNE-ISO/IEC 19011:2012)

Cumplimiento

Ver "prueba de cumplimiento".

Dictamen

(DRAE) Opinión y juicio que se forma o emite sobre algo.

Dictamen de auditoría

Ver "informe de auditoría".

Efectividad / Eficacia

(DRAE) Capacidad de lograr el efecto que se desea o se espera.

Evidencia de auditoría

Registros, declaraciones de hechos o cualquier otra información que es pertinente para los hallazgos de auditoría y que es verificable. La evidencia de auditoría puede ser cualitativa o cuantitativa (UNE-EN-ISO 19011:2012).

Las evidencias consisten, principalmente, en las demostraciones y testimonios (documentales, automatizadas, etc.) de los resultados de la aplicación de los procedimientos de auditoría (pruebas). Éstas deben ser suficientes para soportar las conclusiones del auditor. Para ello deben acreditar determinadas situaciones o hechos objetivos en cuanto a los hechos a los que se refieren. La evaluación de estas evidencias corresponde al auditor para documentar su hallazgo.

Experto técnico

Persona que aporta experiencia o conocimientos técnicos específicos al equipo auditor. El conocimiento o experiencia específicos son los relacionados con la organización, el proceso o la actividad a auditar, el idioma o la orientación cultural. Un experto técnico no actúa como un auditor en el equipo auditor.

Guía

Persona designada por el auditado para asistir al equipo auditor.

Hallazgo de auditoría

Resultados de la evaluación de la evidencia de auditoría frente a los criterios de auditoría. Los hallazgos de auditoría pueden indicar conformidad o no conformidad. Pueden conducir a la identificación de oportunidades de mejora o al registro de buenas prácticas. Si los requisitos de auditoría se seleccionan de entre los requisitos legales u otros requisitos, el hallazgo de auditoría se denomina "cumplimiento" o "no cumplimiento" (UNE-EN-ISO 19011:2012).

Informe de auditoría

Es el producto final de las tareas realizadas en una auditoría. En el informe el auditor comunica, a quien corresponda, los resultados de las tareas realizadas, con los resultados obtenidos.

Limitaciones al alcance

Son aquellos registros o documentos, o elementos del alcance de la auditoría, a los que, aunque previstos en las revisiones planificadas, para lograr los objetivos de la auditoría, el auditor no ha podido tener acceso, por distintas razones, y cuya restricción de acceso puede impactar en las conclusiones de la auditoría. Deben estar reflejadas en el informe de auditoría. Dentro del contexto de esta guía de auditoría, aunque podrían surgir en la definición del alcance, esta situación debería ser excepcional. Si las restricciones surgen en la fase inicial de delimitación del alcance, el auditor debe indicarlo, además de en el informe final, en la planificación. Asimismo, si surge en la fase inicial, debe indicarse el posible impacto en la realización de la auditoría, y la obtención de las conclusiones en relación al objetivo de la auditoría. Es conveniente que en todos los casos, el auditor requiera que se comunique por escrito, la restricción de acceso a registros, documentos o elementos auditables, y justificados por el objetivo de la auditoría.

No conformidad

Incumplimiento de un requisito (UNE-EN-ISO 19011:2012).

Objetividad

Ver “opinión independiente y objetiva”.

Objetivo de la auditoría

1) Las metas específicas que debe lograr la auditoría.

2) En el contexto de esta guía, llegar con concluir si se cumple con lo requeridos por las normas de referencia.

Observador

Persona que acompaña al equipo auditor pero que no audita. Un observador no es parte del equipo auditor, y no influye ni interfiere en la realización de la auditoría. Un observador puede designarse por el auditado, una autoridad reglamentaria u otra parte interesada que testifica la auditoría (adaptado de la UNE-EN-ISO 19011:2012, definición 3.11).

Observación

Ver “pruebas de auditoría”.

Opinión independiente y objetiva

1) Independiente: (DRAE) que no tiene dependencia, que no depende de otro.

2) Objetiva: (DRAE) Perteneciente o relativo al objeto en sí mismo, con independencia de la propia manera de pensar o de sentir.

3) La auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que está siendo auditada para permitir completar de manera objetiva la auditoría.

4) El auditor debe juzgar y opinar sobre los resultados de la auditoría, en función del objetivo y alcance de la misma, libre de toda parcialidad o sesgo que pueda afectar de forma negativa en los resultados de la auditoría, y que pueda conducir a una interpretación errónea de los hechos identificados.

Plan de auditoría

Descripción detallada (paso a paso) de los procedimientos de auditoría (documentación, pruebas, etc.) que se deben realizar durante la ejecución del trabajo de auditoría para alcanzar el objetivo de la misma. En el plan de la auditoría también se incluye la asignación de tareas, fechas de realización de las tareas, y recursos necesarios para desarrollar la auditoría.

Principios de segregación de funciones

1) (DRAE) Principio: Norma o idea fundamental que rige el pensamiento o la conducta.

2) La separación o segregación de funciones es una regla básica en los controles: evitar que una persona pueda dominar todo un proceso, de tal forma que errores u omisiones, o incumplimientos de controles no puedan ser identificados. Por lo tanto, el auditor debe identificar donde no se cumple con esta norma fundamental, para evaluar el impacto en la efectividad de los controles.

Procedimientos de auditoría

Comprenden el proceso de auditoría: habitualmente aluden a los procesos relacionados con la definición de las pruebas, su planificación y su ejecución. Las pruebas de auditoría pueden ser de cumplimiento o sustantivas, según su objetivo. Asi mismo, las técnicas de auditoría utilizadas en cualquier tipo de las pruebas mencionadas anteriormente pueden ser: observación de la realización de tareas, revisión de documentación, entrevistas, realización de pruebas técnicas, revisión de evidencias del cumplimiento de controles, etc. Entre estas últimas se pueden incluir los criterios para la selección de muestras de elementos a revisar en determinadas pruebas.

Pruebas de auditoría

1) Permiten obtener evidencia y verificar la consistencia de los controles existentes y también medir el riesgo por deficiencia de estos o por su ausencia.

2) Se diseñan y planifican para asegurar que los controles se diseñan adecuadamente y funcionan de forma efectiva y continuada.

Pruebas de cumplimiento

Permiten determinar si un control se está realizando de la forma prevista en las normas y políticas de seguridad establecidas por el organismo responsable del SI. Su objetivo principal es determinar si el control se realiza y si sus resultados son efectivos.

Pruebas sustantivas

Permiten confirmar la exactitud de determinadas situaciones o hechos, pero fundamentalmente permiten sustanciar el impacto y alcance de una deficiencia, o incidencia de seguridad (en el contexto de esta guía), con proyección sobre la integridad de determinada información o de un proceso. Ejemplo: en la revisión de un inventario de copias de respaldo, una prueba de cumplimiento puede determinar si los controles previstos se están cumpliendo o no, pero con una prueba sustantiva, se podría determinar cuántos, y /o cuáles elementos no están incluidos en el inventario.

Recomendaciones

Pueden ser parte del informe de auditoría, donde además de incluir las conclusiones de las tareas de auditoría realizadas, e identificar las deficiencias observadas, se pueden incluir sugerencias concretas para la solución de los fallos identificados.

Requisito

1) (DRAE) Circunstancia o condición necesaria para algo.

2) Dentro del contexto de esta guía, son las condiciones, en ocasiones mínimas, a cumplir por los auditores, o en cuanto a la aplicación de una norma.

3) En auditoría se suele indicar que existen “requisitos” o mandatos mínimos que debe cumplir el proceso de auditoría, tales como establecer el alcance y objetivo de la auditoría, realizar un programa de auditoría, y las pruebas relacionadas, así como la emisión de un informe, entre otros.

Responsabilidad

1) Obligación o deber de realizar alguna acción.

2) Dentro del contexto de una auditoría, se deben establecer, por ejemplo, responsabilidades mínimas para la función de auditoría interna,

responsabilidades del cumplimiento de la metodología de auditoría, y sus requisitos mínimos.

3) El auditor es responsable por la opinión y las conclusiones vertidas en el informe de auditoría.

Satisfacción de auditoría

1) (DRAE) Satisfacer: Cumplir, llenar ciertos requisitos o exigencias.

2) Dentro del contexto de la auditoría, se refiere a que el programa o plan de auditoría, debe cumplir con los objetivos de auditoría, y las tareas realizadas con éste.

Selección de muestras

Se pueden aplicar criterios de muestreo estadístico o no, para seleccionar elementos a revisar en una determinada prueba. La calidad de la muestra y de la selección de los elementos de la muestra puede facilitar el análisis de los resultados de una prueba y también la sustentación de una conclusión de auditoría. Se utiliza fundamentalmente cuando existe una población homogénea de elementos a seleccionar, por ejemplo: cuentas de usuarios.

Suficiencia de las evidencias

Las evidencias que soportan una conclusión deben ser suficientes (bastantes), y relevantes (significativos), para soportar las conclusiones y opinión del auditor.

Supervisión

1) (DRAE) Ejercer la inspección superior en trabajos realizados por otros.

2) Las tareas del equipo de auditoría deben ser supervisadas por el Jefe del equipo de auditoría para asegurar que se ha cumplido con el objetivo de la auditoría dentro del alcance previsto.

Verificación

Cualquiera de las acciones de auditoría encaminadas a la comprobación el cotejo, el contraste y el examen de evidencias, registros y documentos.

ANEXO F. BIBLIOGRAFÍA DE REFERENCIA

En la realización de esta auditoría se utilizarán, además de los mínimos requisitos de esta guía, los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a las auditorías.

A continuación, se incluyen referencias bibliográficas que pueden ayudar a los auditores en el desarrollo de su trabajo:

- Real Decreto 3/2010 del 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- 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 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
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Instrucción técnica de seguridad de Conformidad con el Esquema Nacional de Seguridad por Resolución de 13 de octubre de 2016, del Secretario de Estado de Administraciones Públicas
- Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad por Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas
- Instrucción técnica de seguridad de las TIC - Inspección STIC - Centro Criptológico Nacional - CCN-STIC-303
- Guía de seguridad de las TIC - (CCN-STIC-411) - Modelo de plan de verificación STIC - (ST&E PLAN) - CCN-STIC-411
- Guía de seguridad de las TIC - (CCN-STIC-808) - Verificación del cumplimiento de las medidas en el ENS
- Guía de seguridad de las TIC - (CCN-STIC-824) – Esquema Nacional De Seguridad. Informe del Estado de Seguridad.
- Guía de seguridad de las TIC - (CCN-STIC-830) - Ámbito de aplicación del Esquema Nacional de Seguridad
- Esquema de evaluación y certificación de la seguridad de las tecnologías de información - Auditorías internas – PO-001

- ISO/IEC 27001[6] - Information technology -- Security techniques -- Information security management systems – Requirements
- UNE-ISO/IEC 27001 – Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos
- ISO/IEC 27005 - Information technology -- Security techniques -- Information security risk management.
- ISO/IEC 27006 - Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.
- UNE 71504 – Metodología de análisis y gestión de riesgos para los sistemas de información.
- UNE-EN ISO/IEC 17065:2012 - Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
- MAGERIT – versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Consejo Superior de Administración Electrónica, 2012.
- Information Systems Audit and Control Association - www.isaca.org: en esta entidad se pone a disposición de los auditores de sistemas de información, distintos estándares, directrices y procedimientos de auditoría que pueden ser de utilidad para los auditores, ya que la mayoría de ellos tienen en cuenta los aspectos de seguridad, incluyendo algunos específicos sobre seguridad.
    - Las normas son de obligado cumplimiento para los auditores de sistemas tales como Independencia, Ética profesional, Planificación, aplicación de análisis de riesgos en la planificación, utilización del trabajo de expertos, emisión de informes, y similares.
    - Las directrices son una ampliación de los estándares, para facilitar la aplicación de estos últimos: requisitos de las evidencias de auditoría, utilización de herramientas de software de auditoría, externalización de servicios, documentación y registros de la auditoría, análisis forense, privacidad, revisión de la seguridad, y otras más, en algunos casos relacionadas con sistemas de información específicos.
    - Los procedimientos de auditoría proporcionan ejemplos concretos o modelos de programas y pruebas de auditoría: evaluación de sistemas de cifrado, de cortafuegos, firmas electrónicas, y similares.
- El Institute of Internal Auditors – ww.theiia.org también tiene disponibles guías de auditoría para diversos sistemas, y de controles para sistemas de información.

[6] Tanto los estándares ISO como UNE se entenderán referidos a su última versión vigente.