



**GUÍA DE SEGURIDAD  
(CCN-STIC-802)**

**ESQUEMA NACIONAL DE SEGURIDAD  
GUÍA DE AUDITORÍA**

Edita:



© Editor y Centro Criptológico Nacional, 2010  
NIPO: 076-10-072-4

Tirada: 1000 ejemplares

Fecha de Edición: junio de 2010

Marina Touriño ha participado en la redacción de documento y Miguel Angel Amutio y José A. Mañas en su revisión.

#### **LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

#### **AVISO LEGAL**

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## 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, 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 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.

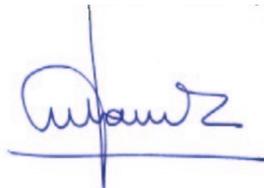
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad 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 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.

Junio de 2010



Félix Sanz Roldán  
Secretario de Estado  
Director del Centro Criptológico Nacional

**ÍNDICE**

<b>1. MARCO DE REFERENCIA.....</b>	<b>4</b>
<b>2. OBJETO DE LA AUDITORÍA.....</b>	<b>5</b>
<b>3. DESARROLLO Y EJECUCIÓN DE LA AUDITORÍA.....</b>	<b>5</b>
3.1. DEFINICIÓN DEL ALCANCE Y OBJETIVO DE LA AUDITORÍA.....	6
3.2. EQUIPO AUDITOR.....	7
3.3. PLANIFICACIÓN PRELIMINAR DE LA AUDITORÍA.....	8
3.4. PROGRAMA DE AUDITORÍA.....	10
3.5. REVISIONES Y PRUEBAS DE AUDITORÍA.....	13
3.6. ELABORACIÓN Y PRESENTACIÓN DE LOS RESULTADOS DE REVISIONES Y PRUEBAS DE AUDITORÍA.....	15
3.7. PRESENTACIÓN DEL INFORME DE AUDITORÍA.....	15
<b>ANEXO A. REQUISITOS PARA EL EQUIPO AUDITOR.....</b>	<b>18</b>
<b>ANEXO B. INCORPORACIÓN DE EXPERTOS AL EQUIPO DE AUDITORÍA.....</b>	<b>19</b>
<b>ANEXO C. CONCURRENCIA CON EL TÍTULO VIII DEL RD 1720/2007.....</b>	<b>20</b>
<b>ANEXO D. MODELO DE ACUERDO DE CONFIDENCIALIDAD.....</b>	<b>22</b>
<b>ANEXO E. GLOSARIO DE TERMINOS.....</b>	<b>24</b>
<b>ANEXO F. BIBLIOGRAFÍA DE REFERENCIA.....</b>	<b>29</b>

## 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 lo previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y específicamente 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 en el ámbito de la Administración Electrónica (RD 3/2010 en adelante).
3. 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.
4. Esta auditoría es requerida, de forma ordinaria, cada dos años para los sistemas de categoría media y alta, según el Anexo I del RD 3/2010, 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.
5. La trascendencia e importancia de los resultados de esta auditoría quedan reflejadas en el artículo 34, donde se establece que “En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas”.
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<sup>1</sup> que el auditor debe tener en cuenta (en la medida que no impliquen un nivel inferior de seguridad requerido por este RD 3/2010), o bien que prescriben la realización de auditorías de las medidas de seguridad pero con objetivos o bien alcances diferentes.
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 de auditores 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.

---

<sup>1</sup> Es el caso, por ejemplo, de que el sistema trate datos de carácter personal y haya que aplicar la normativa correspondiente.

## 2. OBJETO DE LA AUDITORÍA

8. Dar cumplimiento a lo establecido en el artículo 34 y en el Anexo III del RD 3/2010, y por lo tanto, verificar el cumplimiento de los requisitos establecidos por el RD 3/2010 en los capítulos II y III y en los Anexos I y II.
9. Emitir una opinión independiente y objetiva 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 para satisfacerse internamente, o bien frente a terceros que pudieran estar relacionados, sobre el nivel de seguridad implantado.
10. El objetivo final de la auditoría es sustentar la confianza que merece el sistema auditado en materia de seguridad; es decir, calibrar su capacidad 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 programa de auditoría, y a la ejecución de las pruebas que se consideren necesarias.
  - El establecimiento de un programa detallado de auditoría con las 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 OBJETIVO DE LA AUDITORÍA

14. El alcance y objetivo de la auditoría deben estar claramente definidos, documentados y consensuados entre el equipo auditor y el órgano de las Administraciones Públicas o entidades de derecho público vinculado o dependiente (en adelante, órgano de las AAPP) que haya solicitado la auditoría, y en sintonía con el artículo 34 del RD 3/2010.
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. 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 el límite hasta dónde se audita.
17. 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 éste:
  - Política de Seguridad.
  - Valoración de la información y los servicios, junto con la determinación de la categoría del sistema.
  - Política de Firma Electrónica y Certificados y servicios que utilizan estas técnicas.
  - Información, servicios y demás recursos sujetos a la auditoría.
  - Tipo de datos que se manejan así como la normativa que les sea de aplicación. Por ejemplo, datos de carácter personal.
  - Órgano de las AAPP responsable y personal afectado por la auditoría.
  - Conexiones externas con otros organismos públicos o privados.

- 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 a los auditores, y ni siquiera al Jefe del equipo de auditoría, 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.
  - Legislación que afecta al sistema de información auditado: si bien esta auditoría es requerida para las medidas de seguridad establecidas por el RD 3/2010, esta norma también menciona los datos de carácter personal y por lo tanto es necesario considerar la legislación aplicable a este tipo de datos.
  - Otra legislación que pueda ser aplicable, de acuerdo con lo establecido en la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado y Ley 50/1997, de 27 de noviembre, del Gobierno; los Estatutos de Autonomía, leyes autonómicas y normas de desarrollo; y la Ley 7/1985, de 2 de abril, reguladora de las bases del Régimen Local, respectivamente.
18. Para asegurar la independencia objetiva del equipo auditor, las tareas de auditoría no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas como responsabilidades de consultoría o similares (implantación o modificación de software relacionado con el sistema auditado, redacción de documentos requeridos por el RD 3/2010 o procedimientos de actuación, como tampoco posibles recomendaciones de productos concretos de software, entre otros).

### 3.2. EQUIPO AUDITOR

19. El equipo auditor deberá estar compuesto por un equipo de profesionales (Jefe del equipo de auditoría, auditores, y expertos) que garantice que se dispone de los conocimientos (de acuerdo al alcance establecido para la auditoría) suficientes para asegurar la adecuada y ajustada realización de la auditoría. En el Anexo A se establecen unos requisitos mínimos para los integrantes del equipo de auditoría.
20. 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 programa 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 protección 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 independientes, estos también deben firmar una cláusula de confidencialidad.
21. 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
22. 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.
23. El Jefe 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 la protección de datos de carácter personal.

### 3.3. PLANIFICACIÓN PRELIMINAR DE LA AUDITORÍA

24. 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 programa 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 de auditores y expertos.
- Si se realiza una auditoría conjunta con la requerida por el RD 1720/2007, en sus artículos 96 y 110, identificar qué medidas de seguridad entran en el alcance de esta última. El objetivo de eficiencia es que la revisión de una misma medida sea auditada una sola vez, teniendo en cuenta los objetivos relacionados con el RD 3/2010, y con los del RD 1720/2007.

25. 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, según se establece en el RD 3/2010, 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, según se contemplan en el RD 3/2010.
  - Descripción detallada del sistema de información a auditar (software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares).
  - Identificación de la categoría del sistema según el Anexo I del RD 3/2010.
  - Niveles de seguridad definidos.
  - 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 de análisis de riesgos.
  - La Declaración de Aplicabilidad.
  - Decisiones adaptadas para gestionar los riesgos.
  - Relación de las medidas de seguridad implantadas.
  - Relación de registros de actividad en lo relativo a las medidas de seguridad implantadas.
- 
- 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.
26. Según la disponibilidad de esta documentación, y de acuerdo con los responsables de la información, del servicio y del responsable de seguridad, el Jefe del equipo de auditoría 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.
27. 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.

### 3.4. PROGRAMA DE AUDITORÍA

28. 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, y c) establecer los recursos necesarios (del equipo de auditoría y de los servicios auditados).
29. 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 elementos de la seguridad que pueden auditarse mediante la revisión de documentación, observación, y/ o entrevistas.

En el caso concreto de realizar simultáneamente la auditoría requerida por el RD 1720/2007, es necesario identificar la documentación específica para esta auditoría, adicionalmente a la necesaria para la auditoría del RD 3/2010, como por ejemplo, el Documento de Seguridad aplicable.

- 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.

Dado que el RD 1720/2007 requiere, en ocasiones, determinadas medidas de seguridad, que es posible que no se contemplen en las medidas de seguridad adoptadas, como resultado del análisis de riesgos según los requisitos del RD 3/2010, estas medidas deben ser identificadas para verificar su cumplimiento, como por ejemplo la verificación mensual de los registros de acceso.

- 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.
- 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.

30. Los elementos a incluir en la planificación de la auditoría, como elementos mínimos a considerar son los siguientes, teniendo como referencia asimismo el Anexo II del RD 3/2010:

- Análisis y Gestión de riesgos.
  - Tipos de pruebas: sustentación metodológica del análisis de riesgos realizado, su coherencia y documentación, y verificación del inventario de activos. Para ello el equipo auditor puede basarse en la norma UNE 71504 - Metodología de análisis y gestión de riesgos de los sistemas de información. 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 (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 mecanismos de control para el acceso físico, etc.
  - 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.
    - Asimismo, si se realiza una auditoría simultánea según los requisitos del RD 1720/2007, es necesario que los auditores identifiquen las medidas establecidas para el cumplimiento específico de esta norma.
    - Tipos de pruebas: la revisión de los registros de actividad, su revisión y supervisión; fortaleza de las medidas de seguridad de las comunicaciones frente a ataques internos o externos, control de cambios en aplicaciones y sistemas, cumplimiento de contratos de propiedad intelectual, etc.
  - 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 y agenda de mejoras.
  - 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).
31. Para definir la tipología de pruebas a realizar (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 E se incluyen referencias de estas guías.
32. El Jefe del equipo auditor debe valorar qué información o documentación es necesaria solicitar al comienzo de la auditoría, para asegurar que se tiene una fotografía fiel de determinadas medidas de seguridad al comienzo de la misma, como pueden ser, entre otros posibles y según se considere aplicable:
- Lista del personal que ha dejado el organismo recientemente.
  - Copia del registro de incidencias

- Copia del registro de actividad de los usuarios
- Registros de formación del personal afectado por el sistema auditado.

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

34. 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.

### **3.5. REVISIONES Y PRUEBAS DE AUDITORÍA**

35. 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 esta no es suficiente.
- El equipo auditor no prejuzgará, a priori, en la existencia de determinadas medidas, ni será inflexible en su funcionalidad. Al evaluar las medidas existentes deberá siempre considerar, objetivamente, si se ajustan a lo previsto por el RD 3/2010 y si previenen 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.
- 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.
- Se ponderarán las respuestas de las entrevistas, pudiendo haber lugar a la realización de pruebas complementarias que no estaban previstas.

36. Para las evidencias de las pruebas el auditor tendrá en cuenta como normas generales, las siguientes:

- El Jefe del equipo auditor deberá supervisar todo el trabajo realizado y comprobar que se ha llevado a cabo el programa de auditoría previsto y aprobado, y que las desviaciones al programa, o sus modificaciones, están debidamente fundamentadas, y registradas.
- 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 incidencias a incluir en el informe, se sustente 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 revisión de documentación (incluyendo el análisis de riesgos) deberá documentarse con 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 ser plasmadas en actas comunicadas a las personas entrevistadas.
- Los correos electrónicos, en la medida que involucre a varias personas dentro del alcance de la auditoría, y se disponga del acuse de recibo, pueden servir, en determinados casos, también como prueba de auditoría.
- Las pruebas de observación (por ejemplo seguridad física) deberán estar documentadas ya sea a través de fotografías, documentación similar, o comunicaciones escritas puntuales<sup>2</sup> al Responsable de Seguridad.
- 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, deberan acogerse a la práctica habitual y en particular, si de trata de

---

<sup>2</sup> Cuando el auditor, en el curso de sus observaciones, descubre una irregularidad significativa de fácil resolución, puede informar inmediatamente al responsable de seguridad para que tome las medidas correctivas oportunas sin esperar al informe final de auditoría. Estas comunicaciones deben quedar documentadas e incorporarse al conjunto de evidencias que fundamentan las conclusiones de la auditoría.

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.

### **3.6. ELABORACIÓN Y PRESENTACIÓN DE LOS RESULTADOS DE REVISIONES Y PRUEBAS DE AUDITORÍA**

37. 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 aséptico, sin valoraciones subjetivas, ni aludiendo a la valoración de los resultados finales a plasmar en el informe, que es la opinión profesional del auditor.
38. 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.
39. Todos los resultados de pruebas, relacionados entre sí o que se refieran a una misma deficiencia o debilidad, serán agrupados para el informe, aún cuando se incluya un detalle de las deficiencias de forma individual, en un anexo al Informe de Auditoría.
40. En relación a los requisitos del Título VIII del RD 1720/2007, cuando haya una divergencia contrastable entre la aplicación de estos y los del RD 3/2010, resultando un incumplimiento del primero, se debe indicar con claridad esta situación, ya que los requisitos del RD 1720/2007 son prioritarios, como desarrollo de una ley orgánica (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).
41. Si bien el objetivo principal es la verificación del cumplimiento aceptable del RD 3/2010, el equipo auditor deberá tener en cuenta que estos requisitos son mínimos y por lo tanto, si observara alguna deficiencia que puede implicar riesgos en la protección de la información, deberá comunicarlo.

### **3.7. PRESENTACIÓN DEL INFORME DE AUDITORÍA**

42. Una vez confirmados los hechos y deficiencias resultados de las revisiones y pruebas de auditoría, este informe deberá presentarse al Responsable del Sistema y al Responsable de 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 medidas correctoras adecuadas.

43. 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.
44. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas exigidas por el RD 3/2010, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
45. El informe incluirá las no conformidades encontradas durante la realización de la auditoría
46. El informe incluirá una opinión sobre si:
  - La Política de Seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
  - Existen procedimientos para la resolución de conflictos entre dichos responsables.
  - Se han designado personas para dichos roles a la luz del principio de “separación de funciones”.
  - Existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.
  - Se ha realizado un análisis de riesgos, con revisión y aprobación regular, según lo establecido en las medidas aplicables del Anexo II del RD 3/2010.
  - 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.
  - Existe un sistema de gestión de mejora continua.
  - Si la auditoría se realizara conjuntamente con la requerida por el RD 1720/2007 en sus artículos 96 y 110, es necesario que el informe indique con claridad cuando una deficiencia de seguridad o incumplimiento, o una mejora recomendada está, individualmente, relacionada con ambas normas, o bien con una en concreto.
47. El Informe de Auditoría se puede presentar en formato audiovisual. No obstante, este informe siempre deberá entregarse en soporte papel y debidamente firmado, o bien en soporte electrónico con firma electrónica. El esquema del informe incluirá como mínimo:
  - Fecha de emisión del informe
  - Una sección de alcance, limitaciones al alcance, y objetivo de la auditoría, con la debida identificación del sistema auditado.
  - Breve descripción del proceso metodológico aplicado para realizar la auditoría.

- Identificación de la documentación revisada.
- Identificación de la tipología de pruebas realizadas.
- Las fechas (de comienzo y final del trabajo de campo, ya sean reuniones como revisiones técnicas) en que se ha realizado el trabajo de auditoría
- Indicación de si ha habido alguna limitación en la realización de las pruebas o revisiones, que impidan dar una opinión sobre determinados elementos de seguridad.
- Una sección de informe ejecutivo resumiendo los aspectos más relevantes o las áreas de acción más significativas, con un resumen general del grado de cumplimiento.
- Las recomendaciones en ningún caso deberán ser cerradas, sino sugerencias de las distintas alternativas posibles, cuando sea aplicable, a considerar por los responsables de 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 podrán 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 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 Jefe del equipo de auditoría, e indicar los participantes en el equipo de auditoría en un anexo o a continuación de la firma del Jefe del equipo.

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

## ANEXO A. REQUISITOS PARA EL EQUIPO AUDITOR

1. El equipo de auditores deberá estar dirigido y tutelado siempre por un Jefe del equipo de auditoría, cuyas funciones principales son las de supervisión de todo el proceso de auditoría, y responsable de la exactitud de los hechos y recomendaciones mencionados en el informe, y también de preservar las evidencias de la auditoría.
2. El Jefe del equipo de auditoría, responsable de gestionar las tareas 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 relativa a la protección de datos de carácter personal, y al acceso electrónico de los ciudadanos a los Servicios Públicos, y el RD 4/2010 de 8 de enero – Esquema Nacional de Interoperabilidad, entre otros.
3. El resto del equipo, puede no cumplir con los requisitos para el Jefe del equipo de auditoría, 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.
5. Todos los integrantes del equipo de auditoría, especialmente si son externos y los expertos, deberán haber firmado antes de comenzar la auditoría, un acuerdo de confidencialidad según el modelo del Anexo D.

## **ANEXO B. INCORPORACIÓN DE EXPERTOS AL EQUIPO DE AUDITORÍA**

1. En el desarrollo de las tareas de auditoría, los auditores tendrán 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 Jefe del equipo auditor considere necesaria la incorporación de expertos en determinadas materias.
2. Entre estos expertos 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 Jefe del equipo auditor, 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

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 por el artículo 96 del Título VIII del RD 1720/2007. Si el sistema de información auditado según el RD 3/2010, tratase datos de carácter personal, el equipo auditor podrá solicitar una copia de la auditoría preceptiva según el RD de protección de datos personales.
2. No obstante, si durante la realización de la auditoría a la que es aplicable esta guía, se identificase algún incumplimiento manifiesto del RD 1720/2007, es obligación del equipo auditor comunicarlo, e incluirlo en el informe de auditoría.
3. 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:
  - El Título VIII del RD 1720/2007 (medidas de seguridad en el tratamiento de datos de carácter personal) se aplica tanto a ficheros automatizados como no automatizados, y muchos de sus artículos son comunes a ambos tratamientos.
  - Los criterios para la categorización de los sistemas y el establecimiento de los niveles de seguridad en el RD 3/2010 (grado de perjuicio o impacto en el sistema o en personas), son diferentes de los criterios seguidos en el RD 1720/2007 (tipología de datos tratados, accedidos o almacenados, y con algunas excepciones según la finalidad de su tratamiento) para la determinación del nivel de medidas de seguridad aplicables. Por tanto el auditor deberá tener en cuenta unos y otros, en sus respectivos ámbitos de aplicación.<sup>3</sup>
  - Como buenas prácticas de seguridad, el RD 3/2010 y el RD 1720/2007 coinciden en que debe existir una Política de Seguridad (documento de seguridad según el Título VIII del RD 1720/2007), aprobado por la organización y comunicado a todo el personal afectado. En el espíritu del RD 1720/2007, subyace la condición de que las medidas exigidas para los ficheros son requisitos mínimos sin perjuicio de los requisitos de otras legislaciones o que se considere necesario para la protección de los datos.
  - La actividad también puede ser determinante en algunos casos, en la aplicación de las medidas de seguridad: el artículo 81 del RD 1720/2007, por ejemplo, indica que a los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de

<sup>3</sup> Es posible que un sistema de categoría básica según el Anexo I del RD 3/2010, puede procesar datos de carácter personal que requieran medidas de nivel medio o alto según el RD 1720/2007.

localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 (registro de accesos requeridos de forma expresa para el nivel alto).

- El RD 1720/2007 requiere determinadas medidas de seguridad (según el nivel aplicable), que pueden no derivarse necesariamente del preceptivo análisis de riesgos realizado según el RD 3/2010, y que por lo tanto, podrían no estar previstas como medidas a implantar siguiendo los requisitos de este último RD. A continuación se mencionan algunas de las medidas que podrían estar en esta situación:
    - Para los ficheros de cualquier nivel, se debe verificar semestralmente la fiabilidad de las copias de respaldo (artículo 94).
    - La recuperación de datos se considera una incidencia de seguridad (artículo 100, niveles medio y alto), requiriendo asimismo el registro de determinada información.
    - El registro de accesos (artículo 103, nivel alto) no puede ser desactivado ni deberá haber posibilidad de que sea manipulable, y se requiere una revisión mensual por el Responsable de Seguridad, que elaborará un informe sobre la revisión, y se mantendrá por dos años.
    - Si bien el cifrado en comunicaciones, solo se exige categóricamente para los ficheros que requieren medidas de nivel alto, su transmisión electrónica debe evitar su divulgación también para el nivel medio.
    - En relación al control de accesos el RD 1720/2007 (artículo 91) requiere la definición de perfiles de acceso.
    - La auditoría requerida por artículo 96 del RD 1720/2007, también implica la revisión de los contratos de proveedores externos referidos en el Documento de Seguridad, en cuanto a determinados contenidos, según las circunstancias de la prestación del servicio.
  - Se podrán emitir dos informes diferenciados, cada uno con su objetivo y alcance, o bien indicar qué deficiencias afectan al cumplimiento de una u otra norma.
4. Consecuentemente, dados estas dos normas son 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.

## 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, aunque estos servicios no se encuadren exactamente en la figura de “encargado del tratamiento” establecido en el artículo 3 de la Ley Orgánica 15/99 (pero sí dentro del artículo 83 del RD 1720/2007), pero, dado que en alguna circunstancia, se podría acceder a este tipo de datos, el equipo de auditoría XXXX se compromete, en cumplimiento de la Ley Orgánica 15/99 y del Reglamento, a tratar los datos conforme a las instrucciones del responsable de los datos de carácter personal (Responsable de Fichero) 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 DE TERMINOS

Para más información sobre términos y abreviaturas empleados en el Esquema Nacional de Seguridad se recomienda consultar la guía de seguridad **CCN-STIC-800** “ESQUEMA NACIONAL DE SEGURIDAD GLOSARIO DE TÉRMINOS Y ABREVIATURAS”.

### **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**

Elementos a los que comprende la revisión de auditoría: 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**

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.

**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.

**Criterios de auditoría**

- 1) Normas y procesos metodológicos propios de la función de auditoría.
- 2) Dentro de una auditoría, esta palabra se usa también para las razones o discernimientos de los auditores para la confección del plan de auditoría, o evaluar los resultados de las pruebas realizadas.

**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**

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 irrefutables en cuanto a los hechos a los que se refieren. La evaluación de estas evidencias corresponde al auditor para emitir su opinión.

**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.

**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.

**Observación**

Ver “pruebas de auditoría”.

**Opinión independiente y objetiva**

- 1) Independiente: (DRAE) que no tiene dependencia, que no depende de otro.
- 2) Objetiva: (DRAE) Pertenciente 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**

Ver “programa de 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. Asimismo 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.

**Programa 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 programa de la auditoría también se incluyen la asignación de tareas, fechas de realización de las tareas, y recursos necesarios para desarrollar la auditoría.

**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 la 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 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 las TIC - Inspección STIC - Centro Criptológico Nacional - CCN-STIC-303 v1.2
- Guía de seguridad de las TIC - (CCN-STIC-411) - Modelo de plan de verificación STIC - (ST&E PLAN) - CCN-STIC-411 v1.0
- Esquema de evaluación y certificación de la seguridad de las tecnologías de información - Auditorías internas – PO-001
- ISO 19011:2002 – Guidelines for quality and/or environmental management systems auditing  
UNE-EN ISO 19011:2002 – Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental
- ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems – Requirements  
UNE-ISO/IEC 27001:2007 – Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos
- ISO/IEC 27005:2008 - Information technology -- Security techniques -- Information security risk management.
- ISO/IEC 27006:2007 - 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.
- MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Consejo Superior de Administración Electrónica, 2006.

- Information Systems Audit and Control Association - [www.isaca.org](http://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](http://www.theiia.org) también tiene disponibles guías de auditoría para diversos sistemas, y de controles para sistemas de información.